Constacyclic Codes over Finite Commutative Chain Rings

by

Tania Sidana

Under the the guidance of

Dr. Anuradha Sharma

Indraprastha Institute of Information Technology, Delhi
New Delhi 110020, India

July 2020

Constacyclic Codes over Finite Commutative Chain Rings

by

Tania Sidana

submitted

in partial fulfillment of the requirements for the award of the degree of

Doctor of Philosophy

to the

Indraprastha Institute of Information Technology, Delhi

New Delhi, Delhi 110020, India

July 2020

Dedicated to my Family

CERTIFICATE

This is to certify that the thesis titled "**Constacyclic Codes over Finite Commutative Chain Rings**", being submitted by **Tania Sidana** to the Indraprastha Institute of Information Technology, Delhi, for the award of the degree of Doctor of Philosophy, is an original research work carried out by her under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree/diploma.

Supervisor

_____

Dr. Anuradha Sharma
Associate Professor
Department of Mathematics
Indraprastha Institute of Information Technology
New Delhi, Delhi 110020, India
Date:

CANDIDATE'S DECLARATION

The author hereby declares that the work presented in this thesis entitled "**Constacyclic Codes over Finite Commutative Chain Rings**", submitted as partial fulfillment for the degree of Doctor of Philosophy to Indraprastha Institute of Information Technology, Delhi, has been carried out under the supervision of Dr. Anuradha Sharma.

The work done in this thesis is original and has not been submitted earlier as a whole or in part for a degree or diploma at this or any other Institution or University.

_____

Signature of the candidate
(Tania Sidana)
Date:

ACKNOWLEDGEMENTS

I would like to offer my heartfelt thanks to all those people who have contributed to my academic journey either directly or indirectly.

At first, I would express my sincere gratitude to my advisor, Dr. Anuradha Sharma, for her consistent guidance, support and dedicated involvement in every step throughout the process. It is her immense encouragement and endless support that has enabled me to complete my research work in a productive manner. I sincerely thank her for giving me her time so generously.

I am extremely grateful to my doctoral committee members Dr. Samrith Ram, Dr. Sankha Basu and Dr. Pravesh Biyani for their valuable time and comments. My heartfelt thanks to Dr. Shanta Laishram (Indian Statistical Institute, New Delhi, India) who was the external examiner on the occasion of my comprehensive exam and fellowship enhancement seminar.

I would like to thank all my teachers who have taught me in various stages of my life. A special thanks to Dr. Tapas Chatterjee (IIT Ropar, India) for his guidance and encouragement. I want to express my heartfelt gratitude to Prof. Vanita Verma (Panjab University, Chandigarh, India) for her guidance and inspiring conversations. I would like to thank my yoga instructor Ajay Saxena for his consistent support and advice to keep myself physically and mentally fit. I am very grateful for the lab, mess, canteen, hostel, sports, etc. facilities provided by IIIT-Delhi to make my stay comfortable. A special thanks to all the staff members who are responsible for providing such facilities at IIIT-Delhi.

I convey my heartfelt thanks to all fellow researchers and friends, Anjali, Sarita, Divya, Kajal, Neelam, Anand, Anjali, Nidhi, Neetash, Kanika, Subhajit, Varsha and many more, for their valuable time and emotional support. I am also blessed to have a friend Radhika for providing me hopes during the hard times of my life.

I would also like to thank my thesis evaluation committee members Prof. Ferruh Özbudak (Middle East Technical University, Turkey), Dr. Nuh Aydin (Kenyon College, United States), and Dr. Santanu Sarkar (IIT Madras, India) for their insightful comments and suggestions that helped me in improving the overall presentation of the thesis. I gratefully acknowledge IIIT-Delhi and DST-SERB (grant no. EMR/2017/000662) for financial support to conduct this research at IIIT-Delhi.

I do not have enough words to thank my incredibly supportive family. I am blessed to have a family who stood to me at all the highs and lows of this academic journey. I would like to express my gratitude and respect to my parents, who made countless sacrifices to make me what I am today. My sister is one of the most supportive person, who can fight any challenge to fulfill my wishes. I am much indebted to her for all her contributions and sacrifices that she made for me. I thank my brother and my brother-in law who always mentored me. I am blessed to have niece Rose and nephew Arav, who has been a major source of cheerfulness during my visits at home.

Above all, I am grateful to Almighty for blessing me strength and wisdom.

ABSTRACT

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. Singleton [74] derived the upper bound (called the Singleton bound) on the size of an arbitrary block code with respect to the Hamming metric. Linear codes that attain the Singleton bound are called maximum distance separable (MDS) Hamming codes. 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 [70]; they also derived Singleton bound for codes with respect to the RT metric. Linear codes that attain the Singleton bound for the RT metric are called maximum distance separable (MDS) RT codes. Recently, Cassuto and Blaum [12, 13] established a new coding framework for channels whose outputs are overlapping pairs of symbols. Such channels are called symbol-pair read channels and the corresponding metric is called the symbol-pair metric. These channels are more suitable for high density data storage systems in which the spatial resolution of the reader is insufficient to isolate adjacent symbols. Chee et al. [15] derived a Singleton-type bound for codes with respect to the symbol-pair metric and constructed many maximum distance separable (MDS) symbol-pair codes, i.e., the codes attaining the Singleton-type bound with respect to the symbol-pair metric. Recently, Yaakobi et al. [82] extended the framework of symbol-pair read channels to b-symbol read channels, whose outputs are consecutive sequences of $b \geq 3$ symbols. The corresponding metric is called the b-symbol metric. In a recent work, Ding et al. [28] derived a Singleton-type bound for codes over finite fields with respect to the b-symbol metric. The codes that attain the Singleton-type bound with respect to the b-symbol metric are called MDS b-symbol codes. 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. Thus it is of great interest to study and find MDS codes with respect to various metrics.

The derivative is a well-known operator of sequences and is useful in investigating the linear complexity of sequences in game theory, communication theory and cryptography (see [6, 14, 33, 83]). Etzion [32] first applied the derivative operator on codewords of linear codes over finite fields, and defined the depth of a codeword in terms of the derivative operator. He showed that there are exactly k distinct non-zero depths attained by non-zero codewords of a k-dimensional linear code, and that any k non-zero codewords with distinct depths form a basis of the code. This shows that the depth distribution is an interesting parameter of linear codes.

In this thesis, we study algebraic structures of repeated-root constacyclic codes over finite commutative chain rings and their dual codes. We also explicitly determine Hamming distances, symbol-pair distances, b-symbol distances, RT distances, and RT weight distributions of several classes of repeated-root constacyclic codes over finite commutative chain rings. Using these results, we identify several isodual, MDS Hamming, MDS RT, MDS symbol-pair and MDS b-symbol codes within the family of repeated-root constacyclic codes over finite commutative chain rings. We also discuss a decoding algorithm for repeated-root constacyclic codes of prime power lengths over finite commutative chain rings with respect to Hamming, symbol-pair and RT metrics. We also study depths of codewords of a class of repeated-root constacyclic codes over finite commutative chain rings. As a consequence, we explicitly determine depth distributions of this particular class of constacyclic codes over finite commutative chain rings. We also introduce two new turn-based roulette games and discuss their winning strategies by applying our results on depths of codewords of repeated-root constacyclic codes over finite commutative chain rings. 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.

Contents

List of Tables

List of Figures

List of Notations

Symbol	Meaning
$\mathbb{N}$	The set of natural numbers
$\mathbb{F}_q$	The Finite field of order q
$\lvert A\rvert$	The cardinality of the set A
GR(p^e, m)	The Galois ring of characteristic p^e and cardinality p^{em}
$\lfloor\cdot\rfloor$	The Floor function
w_H	The Hamming weight
w_{RT}	The RT weight
w_{sp}	The symbol-pair weight
w_b	The b-symbol weight
d_H	The Hamming distance
d_{RT}	The RT distance
d_{sp}	The symbol-pair distance
d_b	The b-symbol distance
deg $f(x)$	The degree of a non-zero polynomial $f(x)$
$a\vert b$	a divides b
$a \nmid b$	a does not divide b
$\ell^r \vert\vert b$	r is the highest power of ℓ dividing b
$\mathcal{P}_k(\mathcal{S})$	The set consisting of the zero polynomial and all non-zero polynomials with coefficients from the set $\mathcal{S}$ of degree strictly less than k.

List of Publications

1. A. Sharma and T. Sidana, Repeated-root constacyclic codes of arbitrary lengths over the Galois ring GR(p^2, m), Discrete Math. Algorithm Appl. 10(3), DOI: 10.1142/S1793830918500362, 2018.

2. A. Sharma and T. Sidana, On the structure and distances of repeated-root constacyclic codes of prime power lengths over finite commutative chain rings, IEEE Trans. Inf. Theory 65(2), pp. 1072-1084, Feb. 2019.

3. A. Sharma and T. Sidana, On b-symbol distances of repeated-root constacyclic codes, IEEE Trans. Inf. Theory 65(12), pp. 7848-7867, Dec. 2019.

4. T. Sidana and A. Sharma, Repeated-root constacyclic codes over the chain ring $\mathbb{F}_{p^m}[u]/\langle u^3 \rangle$, IEEE Access 8, pp. 101320-101337, Jun. 2020.

5. T. Sidana and A. Sharma, Roulette games and depths of words over finite commutative rings, communicated for publication.

Chapter 1

Introduction

The object of this thesis is

- to establish algebraic structures of repeated-root constacyclic codes over finite commutative chain rings and to determine their dual codes.
- to determine Hamming distances, symbol-pair distances, b-symbol distances, Rosenbloom-Tsfasman distances, and Rosenbloom-Tsfasman weight distributions of repeated-root constacyclic codes over finite commutative chain rings.
- to identify optimal codes with respect to Hamming, symbol-pair, b-symbol and Rosenbloom-Tsfasman metrics within the family of repeated-root constacyclic codes over finite commutative chain rings.
- to discuss a decoding algorithm for repeated-root constacyclic codes of prime power lengths over finite commutative chain rings with respect to Hamming, symbol-pair and Rosenbloom-Tsfasman metrics.
- to determine depth distributions of a class of repeated-root constacyclic codes over finite commutative chain rings.
- to introduce two new turn-based two player roulette games and to discuss their positional winning strategies by studying depths of codewords of repeated-root constacyclic codes over finite commutative chain rings.

Now we proceed to describe the problems that we have explored in this thesis.

1.1 Structure and distances of constacyclic codes over finite commutative chain rings

One of the primary objectives of coding theory is to construct codes that are easy to encode and decode, can detect and correct many errors, and contain a sufficiently large number of codewords. In other words, the goal is to find codes with efficient encoding and decoding procedures, and with the largest possible value of distance for given code length, code size and cardinality of the code alphabet. To study error-detecting and error-correcting properties of a code with respect to various communication channels, several metrics (e.g. Hamming metric, Lee metric, symbol-pair metric, etc.) have been introduced and studied in coding theory. The most studied metric in coding theory is the Hamming metric, which is suitable for orthogonal modulated channels. Singleton [74] derived the following upper bound (called the Singleton bound) on the size M of an arbitrary block code with respect to the Hamming metric:

$$M \leq q^{n-d+1}, \tag{1.1.1}$$

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 (1.1.1) are called maximum distance separable (MDS) Hamming codes. Later, Rosenbloom and Tsfasman [70] introduced a non-Hamming metric, called the Rosenbloom-Tsfasman metric (or RT metric), which is motivated by a problem related to transmission over several parallel communication channels with some channels not available for transmission. This metric is also useful in case of interference between several consecutive communication channels. They also derived Singleton bound for the RT metric. Linear codes attaining the Singleton bound for the RT metric are called MDS RT codes. Recently, Cassuto and Blaum [12, 13] established a new coding framework for channels whose outputs are overlapping pairs of symbols. Such channels are called symbol-pair read channels and the corresponding metric is called the symbol-pair metric. These channels are more suitable for high density data storage systems in which the spatial resolution of the reader is insufficient to isolate adjacent symbols. They proved that for a cyclic code with dimension greater than 1 and Hamming distance d_H, the corresponding symbol-pair distance is at least $d_H + 2$. They showed that a code can correct

up to t symbol-pair errors if and only if its symbol-pair distance is at least $2t+1$. They further provided methods to construct symbol-pair codes from Hamming-metric codes, and derived some bounds on the parameters of symbol-pair codes. They provided an algorithm to decode symbol-pair codes obtained by interleaving the codewords of two Hamming-metric codes. Apart from this, they showed asymptotically that there exist symbol-pair codes whose rates are strictly higher than the best known Hamming-metric codes. Later, Chee et al. [15] derived a Singleton-type bound for symbol-pair codes and constructed many maximum distance separable (MDS) symbol-pair codes, i.e., the codes attaining the Singleton-type bound with respect to the symbol-pair metric. Hiromoto et al. [37] provided a syndrome decoding algorithm for symbol-pair codes within the symbol-pair error correcting capability of the code. Yaakobi et al. [82] showed that for a cyclic code with dimension greater than 1 and minimum distance d_H, the symbol-pair distance is at least $d_H + \lceil \frac{d_H}{2} \rceil$, which improves the lower bound on the symbol-pair distance obtained by Cassuto and Blaum [12, 13]. They also provided a decoding algorithm that can correct symbol-pair errors up to the decoding radius corresponding to this bound. They further extended the framework of symbol-pair read channels to b-symbol read channels, whose outputs are consecutive sequences of $b \geq 3$ symbols. The corresponding metric is called the b-symbol metric. They also extended some of the results obtained in Cassuto and Blaum [12, 13] to b-symbol read channels. This new paradigm is also very relevant to high density data storage systems with reading limitations. It also relates the symbol-pair problem with the sequence reconstruction problem, which was introduced and studied by Levenshtein [47]-[49]. To reconstruct sequences, the same codeword is transmitted over multiple channels, which are almost independent. All channel outputs are then received by the decoder, which provides an estimate of the transmitted codeword. In a recent work, Ding et al. [28] derived a Singleton-type bound for codes over finite fields with respect to the b-symbol metric. The codes attaining this bound are called MDS b-symbol codes. They also provided methods to construct MDS b-symbol codes using projective geometry. Besides this, they constructed an MDS b-symbol (simple-root) constacyclic code of length $\frac{q^{b+1}-1}{q-1}$ and b-symbol distance $2b+1$ over the finite field $\mathbb{F}_q$ of order q, where $b \geq 4$ and q is any prime power. Kai et al. [42] constructed some new MDS symbol-pair codes over finite fields with symbol-pair distance either 5 or 6 based upon simple-root constacyclic codes. Chen et al. [17] also obtained new MDS symbol-pair codes

over finite fields with symbol-pair distance either 5 or 6 or 7 or 8 through repeated-root cyclic codes of some special non prime power lengths and through a simple-root cyclic code of length n over $\mathbb{F}_q$ such that n $(\geq q+4)$ is a divisor of q^2-1. In a recent work, Kai et al. [43] constructed three new MDS symbol-pair codes over finite fields with symbol-pair distance either 6 or 7 through repeated-root constacyclic codes of some special non prime power lengths. Dinh et al. [24] and Sun et al. [77] simultaneously determined symbol-pair distances of all repeated-root constacyclic codes of prime power lengths over finite fields. Dinh et al. [24] also determined all MDS symbol-pair codes within this class of codes. Recently, Mostafanasab and Sevim [63] determined b-symbol distances of some cyclic codes of prime power lengths over finite fields. MDS codes are optimal codes in the sense that these codes have the highest possible error-detecting and error-correcting properties for given code length, code size and alphabet size. Thus it is of great interest to study and find MDS codes with respect to various metrics. In this thesis, we shall study and find MDS codes with respect to Hamming, RT, symbol-pair and b-symbol metrics within the family of repeated-root constacyclic codes over finite commutative chain rings.

Constacyclic codes over finite fields were introduced and studied by Berlekamp [5]. These codes have rich algebraic structures and are generalizations of cyclic and negacyclic codes. These codes can be effectively encoded and decoded using linear shift registers. In 1990's, Calderbank et al. [8], Hammons et al. [36] and Nechaev [64] related several binary non-linear codes to linear codes over the ring $\mathbb{Z}_4$ of integers modulo 4 with the help of a Gray map. This motivated many researchers to study linear codes over $\mathbb{Z}_4$ in particular and to study linear codes over finite commutative chain rings in general. This particular line of research further inspired many coding theorists to study constacyclic codes over finite commutative chain rings, which form an important class of linear codes. Despite all the efforts, the algebraic structure of constacyclic codes is known only for some special lengths and over certain special classes of finite commutative chain rings. Below we summarize some of the recent results known in this direction.

Abualrub and Oehmke [1] studied all cyclic codes of length 2^s over $\mathbb{Z}_4$, where s is a positive integer. Later, Dinh and L*ó*pez-Permouth [22] 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 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. Dinh [20] established algebraic structures of all negacyclic codes of length 2^s over the Galois ring $\mathrm{GR}(2^e, m)$ and their dual codes, where $s \geq 1$ and $e \geq 2$ are integers. Later, Kiah et al. [44] determined all cyclic codes of length p^s over the Galois ring $\mathrm{GR}(p^e, m)$, where p is a prime and e, s, m are positive integers. They further considered the case $e = 2$, and determined dual codes of all cyclic codes of length p^s over $\mathrm{GR}(p^2, m)$. They also listed all self-dual cyclic codes of length p^s over $\mathrm{GR}(p^2, m)$ when p is odd. Sobhani and Esmaeili [75] studied all repeated-root cyclic and negacyclic codes of arbitrary lengths over the Galois ring $\mathrm{GR}(p^2, m)$ and their dual codes.

In Chapter 3, we establish algebraic structures of all repeated-root constacyclic codes of arbitrary lengths over the Galois ring $\mathrm{GR}(p^2, m)$. As an application, we determine their dual codes and list some isodual constacyclic codes over $\mathrm{GR}(p^2, m)$.

In a related direction, many authors investigated algebraic structures of linear and cyclic codes over the quasi-Galois ring $\mathbb{F}_2[v]/\langle v^2 \rangle$ [2, 3, 7, 38, 78]. To describe some of the recent results in this direction, let p be a prime, s, m be positive integers, and let $\mathbb{F}_{p^m}$ be the finite field of order p^m. Dinh [21] 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. [16] and Liu et al. [56] 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 [16, 21, 56], Cao et al. [10] 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. [86] 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 related work, Sobhani [76] 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 $\mathbb{F}_{p^m}$. Recently, Cao et al. [11] established algebraic structures of all $(\alpha + \gamma u^2)$-constacyclic codes over

$\mathbb{F}_{2^m}[u]/\langle u^3\rangle$, where $\alpha, \gamma \in \mathbb{F}_{2^m} \setminus \{0\}$.

In Chapter 4, we determine all repeated-root constacyclic codes of arbitrary lengths over the quasi-Galois ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. We also determine their dual codes and the number of codewords in each repeated-root constacyclic code over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. With the help of their algebraic structures, we obtain Hamming distances, RT distances, RT weight distributions and ranks (i.e., cardinalities of minimal generating sets) of some repeated-root constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. Using these results, we identify several isodual and maximum distance separable (MDS) constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ with respect to Hamming and RT metrics.

In another related direction, Batoul et al. [4] proved that when λ is an nth power of a unit in a finite commutative chain ring $\mathcal{R}$, repeated-root λ-constacyclic codes of length n over $\mathcal{R}$ are equivalent to cyclic codes of the same length n over $\mathcal{R}$. Cao [9] established algebraic structures of all $(1 + a\gamma)$-constacyclic codes of arbitrary lengths over a finite commutative chain ring $\mathcal{R}$ with the maximal ideal as $\langle\gamma\rangle$, where a is a unit in $\mathcal{R}$. Later, Dinh et al. [25] studied repeated-root $(\alpha + a\gamma)$-constacyclic codes of length p^s over a finite commutative chain ring $\mathcal{R}$ with the maximal ideal as $\langle\gamma\rangle$, where p is a prime number, $s \geq 1$ is an integer, α is a non-zero element of the Teichmüller set of $\mathcal{R}$ and a is a unit in $\mathcal{R}$. The results obtained in Dinh et al. [25] can also be obtained from the work of Cao [9] with the help of the ring isomorphism from $\mathcal{R}[x]/\langle x^{p^s} - 1 - a\alpha^{-1}\gamma\rangle$ onto $\mathcal{R}[x]/\langle x^{p^s} - \alpha - a\gamma\rangle$, defined as $A(x) \mapsto A(\alpha_0^{-1}x)$ for each $A(x) \in \mathcal{R}[x]/\langle x^{p^s} - 1 - a\alpha^{-1}\gamma\rangle$, where $\alpha = \alpha_0^{p^s}$ (such an element α_0 always exists in the Teichmüller set of $\mathcal{R}$). The constraint that a is a unit in $\mathcal{R}$ restricts their study to only a few special classes of repeated-root constacyclic codes over $\mathcal{R}$. When a is a unit in $\mathcal{R}$, the codes belonging to these special classes are direct sums of (principal) ideals of certain finite commutative chain rings. However, when a is a non-unit in $\mathcal{R}$, there are repeated-root constacyclic codes over $\mathcal{R}$, which are direct sums of non-principal ideals. In a subsequent work, Dinh et al. [23] established algebraic structures of all $(4z - 1)$-constacyclic codes of length 2^s over $\mathrm{GR}(2^e, m)$ by showing that the quotient ring $GR(2^e, m)[x]/\langle x^{2^s} - 4z + 1\rangle$ is a chain ring, where $z \in \mathrm{GR}(2^e, m)$. They also determined their Hamming, Homogenous and Rosenbloom-Tsfasman distances, and their Rosenbloom-Tsfasman weight distributions. However, we noticed an error in

Proposition 6.5 of Dinh et al. [23] on Rosenbloom-Tsfasman weight distributions, which we shall illustrate in Example 5.5.2 and rectify in Theorem 5.5.3. Extending the work of Dinh et al. [23], Liu and Maouche [55] derived necessary and sufficient conditions for the quotient ring GR$(p^e, m)[x]/\langle x^{p^s} - \lambda\rangle$ to be a chain ring. They also determined Hamming and Homogenous distances of all λ-constacyclic codes of length p^s over GR(p^e, m) when $GR(p^e, m)[x]/\langle x^{p^s} - \lambda\rangle$ is a chain ring.

In Chapter 5, we establish algebraic structures of all repeated-root constacyclic codes of prime power lengths over finite commutative chain rings. Using their algebraic structures, we explicitly determine their Hamming distances, symbol-pair distances, RT distances, and RT weight distributions. As an application of these results, we identify all MDS Hamming, MDS symbol-pair and MDS RT codes within this particular class of constacyclic codes. We also present an algorithm to decode these codes with respect to Hamming, symbol-pair and RT metrics.

In Chapter 6, we obtain b-symbol distances of all repeated-root constacyclic codes of prime power lengths over finite fields. Using this result, we list all MDS b-symbol repeated-root constacyclic codes of prime power lengths over finite fields. Furthermore, we determine b-symbol distances of all repeated-root constacyclic codes of prime power lengths over finite commutative chain rings. Applying these results, we identify all MDS b-symbol repeated-root constacyclic codes of prime power lengths over finite commutative chain rings.

The results derived in Chapters 3-6 are useful in encoding and decoding these codes and in studying their error-detecting and error-correcting capabilities with respect to various communication channels.

1.2 Depth distributions of constacyclic codes over finite commutative chain rings and roulette games

The derivative is a well-known operator of sequences and is useful in studying the linear complexity of sequences in game theory, communication theory and cryptography (see

[6, 14, 33, 83]). Etzion [32] first defined the depth of a codeword by placing the derivative operator on codewords of linear codes over finite fields. He showed that non-zero codewords of a k-dimensional linear code over a finite field attain k distinct depth values, and such a code has a generator matrix whose rows are k non-zero codewords having distinct depths. This shows that the depth distribution is an interesting parameter of linear codes. He also proved that the depth of a binary sequence of an even prime power length as a non-cyclic word is equal to its linear complexity as a cyclic word. Later, Mitchell [62] explicitly determined depth spectra of all cyclic codes over arbitrary finite fields. Luo et al. [58] showed that depth distributions of linear codes over arbitrary finite fields are completely determined by their depth spectra. They also studied the enumeration problem of counting linear subcodes with a prescribed depth spectrum of a given linear code over a finite field. Using these results, they determined depth distributions of all rth order binary Reed-Muller codes.

Next let $\mathrm{Depth}(\mathcal{C})$ denote the depth spectrum of a linear code $\mathcal{C}$ over a finite field. Etzion [32] showed that if $\mathcal{C}$ is a binary linear code of length 2^r, then the depth spectrum of its dual code $\mathcal{C}^\perp$ is given by $\mathrm{Depth}(\mathcal{C}^\perp) = \{1, 2, \cdots, 2^r\} \setminus \{2^r + 1 - i : i \in \mathrm{Depth}(\mathcal{C})\}$. However, this result does not hold when the length n of the code $\mathcal{C}$ is not a power of 2. Recently, Deng [19] studied the intersection $\mathrm{Depth}(\mathcal{C}) \cap \mathrm{Depth}(\mathcal{C}^\perp)$ for a binary linear code $\mathcal{C}$ of length n (not necessarily an even prime power). In particular, he derived a necessary and sufficient condition for the intersection $\mathrm{Depth}(\mathcal{C}) \cap \mathrm{Depth}(\mathcal{C}^\perp)$ to be an empty set, and a sufficient condition under which $|\mathrm{Depth}(\mathcal{C}) \cap \mathrm{Depth}(\mathcal{C}^\perp)| = \lfloor \frac{n}{2} \rfloor$. Kong et al. [45] obtained depth spectra of all simple-root constacyclic codes over finite commutative chain rings. Later, Kai et al. [41] studied depth spectra of negacyclic codes of even lengths over $\mathbb{Z}_4$. Recently, Sidana [73] and Yuan et al. [84] independently determined depth spectra of some constacyclic codes over finite commutative chain rings.

In another related direction, Yehuda et al. [83] proposed and studied a turn-based two player rotating-table game and provided a winning strategy for the rotating-table game by defining the depth of a finite sequence in terms of the derivative operator on sequences. Motivated by the work of Yehuda et al. [83], we will propose two new turn-based two player roulette games and provide winning strategies for these games in terms of depths of words

over a finite commutative ring with unity R. Below we summarize some of the results known on turn-based two player mathematical games in this direction.

Martin Gardner published a monthly column titled "Mathematical Games" in Scientific American between the 1950s and the 1980s, in which he introduced many brain teasers and gave new twists to the old classical puzzles. In one of the columns, Gardner [34] presented a turn-based game for two players in which one of the players is the Blind Bartender and the other player is the adversary, and is nowadays called the Blind Bartender's problem or the rotating table problem. In this game, both the players are standing by a square table, which can rotate about its center by an angle a multiple of $90°$. The game starts when the adversary places 4 drinking glasses, either in the upright position or in the upside down position, on each of the 4 corners of the table in such a way that not all glasses have the same orientation (i.e., not all glasses on the table are either in the upright position or in the upside down position). The Bartender, being blind, cannot see the glasses. Each round of the game starts when the Bartender announces 2 positions of the glasses. Then the adversary rotates the table by an angle a multiple of $90°$, which leads to a permutation of the glasses occupying the 4 positions on the table. Now the Bartender touches two glasses on the positions that he declared and decides to invert these glasses in any way (that is, the Bartender may decide not to invert any of these two glasses or may decide to invert one glass or both the glasses). Thereafter, if all four glasses on the table have the same orientation, then a bell rings and the Bartender wins the game. Otherwise, the next round of the game starts and the game continues in this manner, unless all the 4 glasses on the table have the same orientation. In the same column, Gardner [34] asked if a 2-handed Blind Bartender can get all 4 glasses on the table either in the upright position or in the upside down position in a finite number of moves (or equivalently, if there exists a winning strategy for a 2-handed Blind Bartender in this game). In the next column [35], Gardner showed that a 2-handed Blind Bartender can win this game in at most 5 moves, and provided a positional winning strategy for the Bartender. In the same column [35], Gardner presented a generalization of this game suggested by Graham and Diaconis, where the Blind Bartender and the adversary are standing by a polygonal table with N edges. The polygonal table can rotate by an angle a multiple of $\frac{360°}{N}$. The game starts when the adversary places N drinking glasses, either in the upright position or in the upside down position, at each of the N corners of the table,

such that not all glasses on the table have the same orientation. Each round of the game starts when the Bartender announces K positions of the glasses on the table. Then the adversary rotates the table by an angle a multiple of $\frac{360^\circ}{N}$, which leads to a permutation of the glasses occupying the N positions on the table. Now the Bartender touches K glasses on the positions that he declared and decides to invert the glasses that he wishes to invert among these K glasses. Now if all N glasses on the table have the same orientation, then a bell rings and the Bartender wins the game. Otherwise, the next round of the game starts and the game continues in this manner, unless all the N glasses on the table are either in the upright position or in the upside down position. He also discussed the following result proved by Graham and Diaconis: An $(N-2)$-handed Blind Bartender can win this game if and only if N is a composite integer. One natural question is to determine the smallest value of K such that there exists a winning strategy for the K-handed Blind Bartender in this game. Laaser and Ramshaw [46] and Lewis and Williard [50] independently answered this question and showed that there exists a winning strategy for the K-handed Blind Bartender in this game if and only if the parameters K and N satisfy $K \geq (1-\frac{1}{p})N$, where p is the largest prime divisor of N. In fact, they provided a positional winning strategy for the $(1-\frac{1}{p})N$-handed Blind Bartender in this game.

Later, Ehrenborg and Skinner [31] studied the following generalization of the Blind Bartender's problem: Let S be a set of positions, and let G be a group acting transitively on the set S. A drinking glass either in the upright position or in the upside down position is standing on each element of the set S. Each round of the game starts when the Blind Bartender chooses a subset S' of S with $|S'| = K$ and the adversary applies an element $g \in G$ to the set S. The Bartender inverts some of the glasses standing on the image of the set S' under the action of $g \in G$. Now if all the glasses standing on the elements of S are either in the upright position or in the upside down position, then the Bartender wins the game. Otherwise, the next round of the game starts and the game continues in this manner, unless all the glasses standing on the elements of S are either in the upright position or in the upside down position. In the same work, they considered two versions of this game according as the Blind Bartender is wearing the boxing gloves or not, and they provided positional winning strategies for the Blind Bartender in both the versions of the game. They also determined the smallest K such that there exists a positional winning strategy for the

K-handed Blind Bartender in both the versions of the game. That is, they determined the minimum number of hands that the Blind Bartender needs to have a positional winning strategy in both the versions of the game. Note that the K-handed Blind Bartender Problem, studied by Graham and Diaconis [35], Laaser and Ramshaw [46] and Lewis and Williard [50], follows as a special case of the game studied by Ehrenborg and Skinner [31] when the Blind Bartender is not wearing the boxing gloves, $|S| = N$ and G is a group of cyclic permutations of the set S.

Yehuda et al. [83] presented a generalization of the rotating-table game in which roulettes are placed on the rotating table instead of drinking glasses. They studied two versions of the rotating-table game for two players, Player A (adversary) and Player B, according as Player B is blind or not. The version of the rotating-table game in which Player B is blind is a generalization of the Blind Bartender's problem. They derived necessary and sufficient conditions for Player B to have a positional winning strategy in both the versions of the rotating-table game. They also provided positional winning strategies for Player B in both the versions of the rotating-table game by defining the depth of a word in terms of the derivative operator on words.

In Chapter 7, we study depths of codewords of all repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over a finite commutative chain ring $\mathcal{R}$, where α is a non-zero element of the Teichmüller set of $\mathcal{R}$, γ is a generator of the maximal ideal of $\mathcal{R}$ and β is a unit in $\mathcal{R}$. As a consequence, we explicitly determine depth distributions of all repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$. Apart from this, we propose two new turn-based roulette games and provide winning strategies for these games in terms of depths of words over finite commutative rings with unity. We also discuss the feasibility of these winning strategies by applying our results on depths of codewords of repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$.

1.3 Conclusion and future work

In Chapter 8, we mention a brief conclusion and discuss some interesting open problems.

Chapter 2

Some preliminaries

In this chapter, we shall state some basic definitions and results that are needed to derive our main results. To begin with, let R be a finite commutative ring with unity, N be a positive integer, and let R^N be the R-module consisting of all N-tuples over R. Let $u = (u_0, u_1, \cdots, u_{N-1})$ and $v = (v_0, v_1, \cdots, v_{N-1})$ be vectors in R^N. Then the Hamming metric $d_H : R^N \times R^N \to \mathbb{N} \cup \{0\}$ is defined as

$$d_H(u, v) = |\{i : 0 \leq i \leq N-1, u_i \neq v_i\}|,$$

while the Rosenbloom-Tsfasman (RT) metric $d_{RT} : R^N \times R^N \to \mathbb{N} \cup \{0\}$ is defined as

$$d_{RT}(u, v) = \begin{cases} 1 + \max\{i : 0 \leq i \leq N-1, u_i \neq v_i\} & \text{if } u \neq v; \\ 0 & \text{if } u = v. \end{cases}$$

Further, the symbol-pair read vector of $u \in R^N$ is defined as

$$\pi_{sp}(u) = ((u_0, u_1), (u_1, u_2), \cdots, (u_{N-1}, u_0)) \in (R^2)^N,$$

and the symbol-pair metric $d_{sp} : R^N \times R^N \to \mathbb{N} \cup \{0\}$ is defined as

$$d_{sp}(u, v) = d_H(\pi_{sp}(u), \pi_{sp}(v)) = |\{i : 0 \leq i \leq N-1, (u_i, u_{i+1}) \neq (v_i, v_{i+1})\}|,$$

where the subscript $i + 1$ is taken modulo N. Furthermore, for an integer b satisfying $2 \leq b < N$, the b-symbol read vector of $u \in R^N$ is defined as

$$\pi_b(u) = ((u_0, u_1, \cdots, u_{b-1}), (u_1, u_2, \cdots, u_b), \cdots, (u_{N-1}, u_0, \cdots, u_{b-2})) \in (R^b)^N,$$

and the b-symbol metric $d_b : R^N \times R^N \to \mathbb{N} \cup \{0\}$ is defined as

$$\begin{aligned} d_b(u,v) &= d_H(\pi_b(u), \pi_b(v)) \\ &= |\{i : 0 \le i \le N-1, (u_i, u_{i+1}, \cdots, u_{i+b-1}) \neq (v_i, v_{i+1}, \cdots, v_{i+b-1})\}|, \end{aligned}$$

where the subscripts $i+1, i+2, \cdots, i+b-1$ are taken modulo N. In particular, when $b = 2$, the b-symbol metric coincides with the symbol-pair metric on R^N.

The Hamming weight $w_H(u)$ of the vector $u \in R^N$ is defined as the number of integers i satisfying $0 \le i \le N-1$ and $u_i \neq 0$.

The Rosenbloom-Tsfasman (RT) weight $w_{RT}(u)$ of u is defined as

$$w_{RT}(u) = \begin{cases} 1 + \max\{i : 0 \le i \le N-1, u_i \neq 0\} & \text{if } u \neq 0; \\ 0 & \text{if } u = 0. \end{cases}$$

The symbol-pair weight $w_{sp}(u)$ of the vector $u \in R^N$ is defined as the Hamming weight of the symbol-pair read vector $\pi_{sp}(u)$ over the alphabet R^2, which equals the number of integers i satisfying $0 \le i \le N-1$ and $(u_i, u_{i+1}) \neq (0,0)$, where the subscript $i+1$ is taken modulo N.

For an integer b satisfying $2 \le b < N$, the b-symbol weight $w_b(u)$ of the vector $u \in R^N$ is defined as the Hamming weight of the b-symbol read vector $\pi_b(u)$ over the alphabet R^b, which equals the number of integers i satisfying $0 \le i \le N-1$ and $(u_i, u_{i+1}, \cdots, u_{i+b-1}) \neq (0, 0, \cdots, 0)$, where the subscripts $i, i+1, \cdots, i+b-1$ are taken modulo N. In particular, when $b = 2$, the b-symbol weight $w_b(u)$ of the vector $u \in R^N$ is the same as the symbol-pair weight $w_{sp}(u)$ of the vector $u \in R^N$.

Note that $w_H(u) = d_H(u, 0)$, $w_{RT}(u) = d_{RT}(u, 0)$, $w_{sp}(u) = d_{sp}(u, 0)$ and $w_b(u) = d_b(u, 0)$ for each $u \in R^N$.

A linear code $\mathcal{C}$ of length N over R is defined as an R-submodule of R^N. The cardinality of the set $\mathcal{C}$ is called the size of the code $\mathcal{C}$. The Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is defined as $d_H(\mathcal{C}) = \min\{d_H(u,v) : u, v \in \mathcal{C} \text{ and } u \neq v\} = \min\{w_H(c) : c(\neq 0) \in \mathcal{C}\}$,

while the Rosenbloom-Tsfasman (RT) distance $d_{RT}(\mathcal{C})$ of the code $\mathcal{C}$ is defined as $d_{RT}(\mathcal{C}) = \min\{d_{RT}(u,v) : u,v \in \mathcal{C} \text{ and } u \neq v\} = \min\{w_{RT}(c) : c(\neq 0) \in \mathcal{C}\}$. Further, the symbol-pair distance of the code $\mathcal{C}$ is defined as $d_{sp}(\mathcal{C}) = \min\{d_{sp}(u,v) : u,v \in \mathcal{C} \text{ and } u \neq v\} = \min\{w_{sp}(c) : c(\neq 0) \in \mathcal{C}\}$. Furthermore, for an integer b satisfying $2 \leq b < N$, the b-symbol distance of the code $\mathcal{C}$ is defined as $d_b(\mathcal{C}) = \min\{d_b(u,v) : u,v \in \mathcal{C} \text{ and } u \neq v\} = \min\{w_b(c) : c(\neq 0) \in \mathcal{C}\}$. In particular, when $b = 2$, the b-symbol distance $d_b(\mathcal{C})$ of the code $\mathcal{C}$ is the same as the symbol-pair distance $d_{sp}(\mathcal{C})$ of the code $\mathcal{C}$.

One can easily see that an arbitrary R-submodule of R^N need not be a free module. 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 $0 \leq \rho \leq N$, $\mathcal{A}_\rho$ equals the number of codewords in $\mathcal{C}$ having the RT weight as ρ.

In the following theorem, we state Singleton bounds with respect to the Hamming, RT and symbol-pair metrics.

Theorem 2.0.1. [15, 70, 74] Let $\mathcal{C}$ be a code of length N over R.

(a) The Singleton bound with respect to the Hamming metric is as stated below.

$$|\mathcal{C}| \leq |R|^{N-d_H(\mathcal{C})+1}.$$

(b) The Singleton bound with respect to the RT metric is as stated below.

$$|\mathcal{C}| \leq |R|^{N-d_{RT}(\mathcal{C})+1}.$$

(c) The Singleton bound with respect to the symbol-pair metric is as stated below.

$$|\mathcal{C}| \leq |R|^{N-d_{sp}(\mathcal{C})+2}.$$

A code $\mathcal{C}$ of length N over R is called

(i) an MDS Hamming code if $|\mathcal{C}| = |R|^{N-d_H(\mathcal{C})+1}$.

(ii) an MDS symbol-pair code if $|\mathcal{C}| = |R|^{N-d_{sp}(\mathcal{C})+2}$.

(iii) an MDS RT code if $|\mathcal{C}| = |R|^{N-d_{RT}(\mathcal{C})+1}$.

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 $c = (c_0, c_1, \cdots, c_{N-1}) \in \mathcal{C}$. Two linear codes over R are said to be R-linearly equivalent if one code can be obtained from the other by a combination of operations of the following two types:

- permutation of coordinate positions of the code;
- multiplication of the symbols appearing in a fixed coordinate position by a unit in R.

The code $\mathcal{C}$ is said to be isodual if it is R-linearly equivalent to its dual code $\mathcal{C}^\perp$.

For a unit $\lambda \in R$, the linear code $\mathcal{C}$ is called a λ-constacyclic code if it satisfies the following: $(a_0, a_1, a_2, \cdots, a_{N-1}) \in \mathcal{C}$ implies that $(\lambda a_{N-1}, a_0, a_1, \cdots, a_{N-2}) \in \mathcal{C}$. It is easy to observe that the dual code $\mathcal{C}^\perp$ is a λ^{-1}-constacyclic code of length N over R. Under the standard R-module isomorphism from R^N onto $R[x]/\langle x^N - \lambda\rangle$, defined as $(a_0, a_1, \cdots, a_{N-1}) \mapsto a_0 + a_1x + \cdots + a_{N-1}x^{N-1} + \langle x^N - \lambda\rangle$ for each $(a_0, a_1, \cdots, a_{N-1}) \in R^N$, the code $\mathcal{C}$ can also be viewed as an ideal of the quotient 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 now on, all elements of the ring $R[x]/\langle x^N - \lambda\rangle$ shall be represented by their representatives in $R[x]$ of degree less than N, and their addition

and multiplication shall be performed modulo $x^N - \lambda$. In view of this, the Hamming weight $w_H(c(x))$ of $c(x) \in R[x]/\langle x^N - \lambda\rangle$ is defined as the number of non-zero coefficients of $c(x)$, while the RT weight $w_{RT}(c(x))$ of $c(x) \in R[x]/\langle x^N - \lambda\rangle$ is defined as

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

On the other hand, the b-symbol weight $w_b(c(x))$ of $c(x) = c_0 + c_1x + \cdots + c_{N-1}x^{N-1} \in R[x]/\langle x^N - \lambda\rangle$ is defined as the b-symbol weight of the vector $c = (c_0, c_1, \cdots, c_{N-1})$. 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 $\text{ann}(\mathcal{C})$ 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.

Theorem 2.0.2. [16] If $\mathcal{C} \subseteq R[x]/\langle x^N - \lambda\rangle$ is a λ-constacyclic code of length N over R, then we have

$$\mathcal{C}^\perp = \text{ann}(\mathcal{C})^*.$$

A finite commutative ring with unity is called

(i) a local ring if it has a unique maximal ideal.

(ii) a Galois ring if all its zero-divisors including 0 (or equivalently, all its non-units) form an ideal generated by some prime number p.

(iii) a chain ring if all its ideals form a chain with respect to the inclusion relation.

One can easily observe that the ring $\mathbb{Z}_{p^e}$ of integers modulo p^e is a Galois ring of characteristic p^e. Now let $^-$ be a canonical ring epimorphism from $\mathbb{Z}_{p^e}$ onto $\mathbb{Z}_{p^e}/\langle p\rangle \simeq \mathbb{F}_p$, defined as $r \mapsto \overline{r} = r + \langle p\rangle$ for each $r \in \mathbb{Z}_{p^e}$. The map $^-$ can be further extended to a ring epimorphism from $\mathbb{Z}_{p^e}[x]$ onto $\mathbb{F}_p[x]$ as follows:

$$f(x) \mapsto \overline{f(x)} = \sum_{i=0}^{k} \overline{b_i} x^i$$

for every $f(x) = \sum_{i=0}^{k} b_i x^i \in \mathbb{Z}_{p^e}[x]$. A polynomial $f(x) \in \mathbb{Z}_{p^e}[x]$ is said to be basic irreducible if the polynomial $\overline{f(x)}$ is irreducible over $\mathbb{F}_p$. A monic polynomial $f(x) \in \mathbb{F}_p[x]$ of degree k is called a primitive polynomial if $f(x)$ has a primitive element of $\mathbb{F}_{p^k}$ as one of its roots. A monic polynomial $f(x) \in \mathbb{Z}_{p^e}[x]$ is said to be basic primitive if $\overline{f(x)}$ is a primitive polynomial over $\mathbb{F}_p$. Then the following result is well-known.

Theorem 2.0.3. [79] Let R be a Galois ring. Suppose that the set of all zero-divisors of R including 0 form an ideal generated by a prime number p. Then the following hold.

(a) The characteristic of R is p^e for some positive integer e.

(b) The ring R is a chain ring with the maximal ideal $\langle p\rangle$.

(c) The residue field of R is given by $R/\langle p\rangle \simeq \mathbb{F}_{p^m}$ for some positive integer m. Furthermore, we have $|R| = p^{me}$, and the ring R is isomorphic to the quotient ring $\mathbb{Z}_{p^e}[x]/\langle h(x)\rangle$, where $h(x)$ is a monic basic irreducible polynomial of degree m over $\mathbb{Z}_{p^e}$.

(d) Any two Galois rings of the same characteristic and the same cardinality are isomorphic.

(e) There exists an element $\zeta \in \mathrm{GR}(p^e, m)$ having the multiplicative order as $p^m - 1$. Moreover, the cyclic subgroup generated by ζ is the only subgroup of the unit group of $\mathrm{GR}(p^e, m)$, which is isomorphic to $\mathbb{F}_{p^m} \setminus \{0\}$, (the set $\mathcal{T} = \{0, 1, \zeta, \cdots, \zeta^{p^m-2}\}$ is called the Teichmüller set of $\mathrm{GR}(p^e, m)$). As a consequence, for each non-zero $\theta \in \mathcal{T}$, there exists $\theta_0 \in \mathcal{T}$ satisfying $\theta_0^{p^s} = \theta$.

(f) Each element $r \in \mathrm{GR}(p^e, m)$ can be uniquely expressed as $r = r_0 + r_1 p + r_2 p^2 + \cdots + r_{e-1} p^{e-1}$, where $r_i \in \mathcal{T}$ for $0 \leq i \leq e-1$. Moreover, r is a unit in R if and only if $r_0 \neq 0$.

Now two polynomials $k_1(x), k_2(x) \in \mathrm{GR}(p^e, m)[x]$ are said to be coprime if $\langle k_1(x) \rangle + \langle k_2(x) \rangle = \mathrm{GR}(p^e, m)[x]$, i.e., if there exist polynomials $a_1(x), a_2(x) \in \mathrm{GR}(p^e, m)[x]$ such that $k_1(x)a_1(x) + k_2(x)a_2(x) = 1$ in $\mathrm{GR}(p^e, m)[x]$. In general, the polynomials $k_1(x), k_2(x), \cdots, k_r(x) \in \mathrm{GR}(p^e, m)[x]$ are said to be pairwise coprime in $\mathrm{GR}(p^e, m)[x]$ if for $1 \leq i, \ell \leq r$ with $i \neq \ell$, the polynomials $k_i(x)$ and $k_\ell(x)$ are coprime in $\mathrm{GR}(p^e, m)[x]$. In fact, we have the following:

Theorem 2.0.4. [67] The following hold.

(a) Let $k_1(x), k_2(x) \in \mathrm{GR}(p^e, m)[x]$. Then $k_1(x)$ and $k_2(x)$ are coprime in $\mathrm{GR}(p^e, m)[x]$ if and only if $\overline{k_1(x)}$ and $\overline{k_2(x)}$ are coprime in $\mathbb{F}_{p^m}[x]$.

(b) Let $f(x) \in \mathrm{GR}(p^e, m)[x]$ be a monic polynomial such that $\overline{f(x)}$ is square-free, i.e., $\overline{f(x)}$ is not divisible by the square of any irreducible polynomial over $\mathbb{F}_{p^m}$. Then the polynomial $f(x)$ factors uniquely as a product of monic basic irreducible pairwise coprime polynomials in $\mathrm{GR}(p^e, m)[x]$.

One can easily observe that Galois rings, finite fields and quasi-Galois rings $\mathbb{F}_q[u]/\langle u^e \rangle$ are examples of finite commutative chain rings. Further, we have the following well-known result.

Theorem 2.0.5. [22] For a finite commutative ring R with unity, the following statements are equivalent:

(a) R is a local ring and the (unique) maximal ideal $\mathcal{M}$ of R is principal, i.e., $\mathcal{M} = \langle \gamma \rangle$ for some $\gamma \in R$.

(b) R is a local principal ideal ring.

(c) R is a chain ring and all its ideals are given by $\{0\}, R, \langle \gamma \rangle, \langle \gamma^2 \rangle, \cdots, \langle \gamma^{e-1} \rangle$, where e is the nilpotency index of γ. Moreover, if $\overline{R} = R/\langle \gamma \rangle$, then $\overline{R}$ is a finite field (called the residue field of R) and $|\langle \gamma^\ell \rangle| = |\overline{R}|^{e-\ell}$ for $0 \leq \ell \leq e$.

From now on, let $\mathcal{R}$ be a finite commutative chain ring with unity 1, and let γ be a generator of the maximal ideal of $\mathcal{R}$. Further, let e be the nilpotency index of γ, and let $\overline{\mathcal{R}} = \mathcal{R}/\langle\gamma\rangle$ be the residue field of $\mathcal{R}$. As $\overline{\mathcal{R}}$ is a finite field, let us suppose that $\overline{\mathcal{R}} \simeq \mathbb{F}_{p^m}$ for some prime p and positive integer m, where $\mathbb{F}_{p^m}$ is the finite field of order p^m. Let $^- : \mathcal{R} \to \overline{\mathcal{R}}$ be the natural epimorphism from $\mathcal{R}$ onto $\overline{\mathcal{R}}$, which is given by $r \mapsto \overline{r} = r + \langle\gamma\rangle$ for each $r \in \mathcal{R}$. Then we have the following:

Theorem 2.0.6. [61, 65] The following hold.

(a) The characteristic of $\mathcal{R}$ is p^a, where $1 \leq a \leq e$. Moreover, we have $|\mathcal{R}| = |\overline{\mathcal{R}}|^e = p^{me}$.

(b) There exists an element $\zeta \in \mathcal{R}$ having the multiplicative order as $p^m - 1$. Moreover, the cyclic subgroup generated by ζ is the only subgroup of the unit group of $\mathcal{R}$, which is isomorphic to $\mathbb{F}_{p^m} \setminus \{0\}$, (the set $\mathcal{T} = \{0, 1, \zeta, \cdots, \zeta^{p^m-2}\}$ is called the Teichmüller set of $\mathcal{R}$). As a consequence, for each non-zero $\theta \in \mathcal{T}$, there exists $\theta_0 \in \mathcal{T}$ satisfying $\theta_0^{p^s} = \theta$.

(c) Each element $r \in \mathcal{R}$ can be uniquely expressed as $r = r_0 + r_1\gamma + r_2\gamma^2 + \cdots + r_{e-1}\gamma^{e-1}$, where $r_i \in \mathcal{T}$ for $0 \leq i \leq e-1$. Moreover, r is a unit in $\mathcal{R}$ if and only if $r_0 \neq 0$.

It is well-known that $\overline{\mathcal{R}} = \{0, \overline{1}, \overline{\zeta}, \cdots, \overline{\zeta}^{p^m-2}\}$, and hence the restriction of the map $^-$ to the Teichmüller set $\mathcal{T}$ is a bijection from $\mathcal{T}$ onto $\overline{\mathcal{R}}$. Furthermore, the map $^-$ can be extended to a ring epimorphism from $\mathcal{R}[x]$ onto $\overline{\mathcal{R}}[x]$ as follows: $f(x) = \sum_{i=0}^{k} a_i x^i \mapsto \overline{f(x)} = \sum_{i=0}^{k} \overline{a_i} x^i$ for each $f(x) \in \mathcal{R}[x]$. For a unit $\lambda \in \mathcal{R}$, the map $^-$ can be further extended to a map μ from $\mathcal{R}_\lambda = \mathcal{R}[x]/\langle x^N - \lambda\rangle$ into $\overline{\mathcal{R}}_\lambda = \overline{\mathcal{R}}[x]/\langle x^N - \overline{\lambda}\rangle$ as follows:

$$\sum_{i=0}^{N-1} a_i x^i \;\mapsto\; \sum_{i=0}^{N-1} \overline{a_i} x^i \quad \text{for each} \quad \sum_{i=0}^{N-1} a_i x^i \in \mathcal{R}_\lambda.$$

It is easy to observe that μ is a surjective ring homomorphism from $\mathcal{R}_\lambda$ onto $\overline{\mathcal{R}}_\lambda$.

Now let $\mathcal{C}$ be a linear code of length N over $\mathcal{R}$. For $0 \leq i \leq e-1$, the ith torsion code of $\mathcal{C}$ is defined as

$$\mathrm{Tor}_i(\mathcal{C}) \;=\; \{(\overline{a}_0, \overline{a}_1, \cdots, \overline{a}_{N-1}) \in \overline{\mathcal{R}}^N : \gamma^i(a_0, a_1, \cdots, a_{N-1}) \in \mathcal{C}\}.$$

Theorem 2.0.7. [66, 67] Let $\mathcal{C}$ be a linear code of length N over $\mathcal{R}$. Then we have the following:

(a) For $0 \leq i \leq e-1$, the ith torsion code $\text{Tor}_i(\mathcal{C})$ of $\mathcal{C}$ is a linear code of length N over $\overline{\mathcal{R}}$ and $|\text{Tor}_i(\mathcal{C})| = |\overline{\mathcal{R}}|^{\dim(\text{Tor}_i(\mathcal{C}))}$, where $\dim(\text{Tor}_i(\mathcal{C}))$ denotes the dimension of $\text{Tor}_i(\mathcal{C})$ over $\overline{\mathcal{R}}$.

(b) We have $\text{Tor}_0(\mathcal{C}) \subseteq \text{Tor}_1(\mathcal{C}) \subseteq \cdots \subseteq \text{Tor}_{e-1}(\mathcal{C})$.

(c) $|\mathcal{C}| = \prod_{i=0}^{e-1} |\text{Tor}_i(\mathcal{C})|$.

(d) The Hamming distance of the code $\mathcal{C}$ is equal to the Hamming distance of its $(e-1)$th Torsion code $\text{Tor}_{e-1}(\mathcal{C})$.

Now let $\mathcal{C}$ be a λ-constacyclic code of length N over $\mathcal{R}$, (i.e., an ideal of the ring $\mathcal{R}_\lambda$). For $0 \leq i \leq e-1$, the ith torsion code of $\mathcal{C}$ is given by

$$\text{Tor}_i(\mathcal{C}) \ = \ \{\mu(f(x)) \in \overline{\mathcal{R}}_\lambda : \gamma^i f(x) \in \mathcal{C}\}.$$

One can easily observe that for $0 \leq i \leq e-1$, the Torsion code $\text{Tor}_i(\mathcal{C})$ is a $\overline{\lambda}$-constacyclic code of length N over $\overline{\mathcal{R}}$.

Now the following theorem is useful in the determination of Hamming distances of some repeated-root constacyclic codes over $\mathcal{R}$ and is an extension of Theorem 3.4 of Dinh [21].

Theorem 2.0.8. 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, we have $|\mathcal{C}| = p^{mn(p^s - \nu)}$, and 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:

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

Proof. Working in a similar manner as in Theorem 3.4 of Dinh [21], the desired result follows. □

The following three divisibility results involving binomial coefficients are quite useful in determination of algebraic structures and distances of some repeated-root constacyclic codes over $\mathcal{R}$.

Theorem 2.0.9. (Kummer's Theorem) Let p be a prime number, and let $u \geq v \geq 0$ be integers. If t is the number of carries when adding $u - v$ and v in the base p, then $p^t || \binom{u}{v}$.

Theorem 2.0.10. (Lucas' Theorem) Let p be a prime number, t be a positive integer, and let u, v be integers satisfying $0 \leq u \leq v < p^t$. Let $v = v_0 + v_1 p + \cdots + v_{t-1}p^{t-1}$ and $u = u_0 + u_1 p + \cdots + u_{t-1}p^{t-1}$ be the p-adic representations of integers v and u, where $0 \leq v_i, u_i \leq p-1$ for $0 \leq i \leq t-1$. Then we have

$$\binom{v}{u} \equiv \prod_{i=1}^{t-1} \binom{v_i}{u_i} \pmod{p}.$$

Theorem 2.0.11. [25] Let p be a prime number, and let $a \geq 1$, $\ell \geq k \geq 0$ be integers. Then the following hold.

(a) If $p^\ell > a$ and $p^k || a$, then $p^{\ell-k} || \binom{p^\ell}{a}$.

(b) For each integer i satisfying $1 \leq i \leq p-1$, we have $p || \binom{p^\ell}{ip^{\ell-1}}$.

From now on, throughout this thesis, we shall follow the same notations as in Chapter 2.

Chapter 3

Repeated-root constacyclic codes over the Galois ring GR(p^2, m)

3.1 Introduction

In this chapter, we shall determine all repeated-root constacyclic codes of arbitrary lengths over the Galois ring GR(p^2, m), their sizes and their dual codes, where p is a prime and m is a positive integer. As an application, we shall list some isodual constacyclic codes over GR(p^2, m). To illustrate the results, we obtain all cyclic and negacyclic codes of length 10 over GR$(4, 3)$.

For this, throughout this chapter, let p be a prime, n, s be positive integers, and let λ be a unit in GR(p^2, m). This chapter is organized as follows: In Section 3.2, we determine all λ-constacyclic codes of length np^s over GR(p^2, m), their sizes and their dual codes. Besides this, we obtain some isodual constacyclic codes of arbitrary lengths over GR(p^2, m). In Section 3.3, we determine all cyclic and negacyclic codes of length 10 over GR$(4, 3)$.

3.2 Algebraic structures of repeated-root constacyclic codes over GR(p^2, m) and their dual codes

In this section, we shall determine all repeated-root constacyclic codes of length np^s over GR(p^2, m) and their dual codes. We shall also determine the number of codewords in each code and list some isodual constacyclic codes of length np^s over GR(p^2, m).

Towards this, we recall that for a unit $\lambda \in \text{GR}(p^2, m)$, a λ-constacyclic code of length np^s over GR(p^2, m) is an ideal of the quotient ring GR$(p^2, m)[x]/\langle x^{np^s} - \lambda\rangle$. By Theorem 2.0.3(f), the unit $\lambda \in \text{GR}(p^2, m)$ can be uniquely written as $\lambda = \alpha + p\beta$, where $\alpha, \beta \in \mathcal{T}$ and $\alpha \neq 0$. Further, by Theorem 2.0.3(e), we observe that there exists $\alpha_0 \in \mathcal{T} \setminus \{0\}$ such that ${\alpha_0}^{p^s} = \alpha$. This implies that $x^{np^s} - \lambda = x^{np^s} - {\alpha_0}^{p^s} - p\beta$. Now by Theorem 2.0.4(b), we can write $x^n - \alpha_0 = f_1(x)f_2(x)\cdots f_r(x)$, where $f_1(x), f_2(x), \cdots, f_r(x)$ are monic basic irreducible pairwise coprime polynomials in GR$(p^2, m)[x]$. Further, by applying Theorem 2.0.4(a), we observe that the polynomials $f_1(x)^{p^s}, f_2(x)^{p^s}, \cdots, f_r(x)^{p^s}$ are pairwise coprime in GR$(p^2, m)[x]$ and that the polynomials $f_j(x)$ and $F_j(x) = \frac{x^n - \alpha_0}{f_j(x)}$ are coprime in GR$(p^2, m)[x]$ for $1 \leq j \leq r$. Moreover, for $1 \leq u \leq r-1$, by Theorem 2.0.4(a) again, we see that the polynomials $f_u(x)^{p^s}$ and $f_{u+1}(x)^{p^s} f_{u+2}(x)^{p^s} \cdots f_r(x)^{p^s}$ are coprime in GR$(p^2, m)[x]$, which implies that there exist polynomials $v_u(x), w_u(x) \in \text{GR}(p^2, m)[x]$ satisfying deg $w_u(x) <$ deg $f_u(x)^{p^s}$ and $v_u(x)f_u(x)^{p^s} + w_u(x)f_{u+1}(x)^{p^s} f_{u+2}(x)^{p^s} \cdots f_r(x)^{p^s} = 1$. Further, by Theorem 2.0.11, we see that $p || \binom{p^s}{kp^{s-1}}$ for $1 \leq k \leq p-1$ and that $p^2 | \binom{p^s}{i}$ for each integer i satisfying $1 \leq i \leq p^s - 1$ and $p^{s-1} \nmid i$. So we can write $\binom{p^s}{kp^{s-1}} = pa_k$ with $p \nmid a_k$ for $1 \leq k \leq p-1$ and that $\binom{p^s}{i} = 0$ in GR(p^2, m) for each integer i satisfying $1 \leq i \leq p^s - 1$ and $p^{s-1} \nmid i$. Using this, we factorize the polynomial $x^{np^s} - \lambda$ into pairwise coprime polynomials in GR$(p^2, m)[x]$ in the following lemma.

Lemma 3.2.1. We have

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

where the polynomials $g_1(x), g_2(x), \cdots, g_r(x) \in \text{GR}(p^2, m)[x]$ satisfy the following for $1 \leq j \leq r$:

- $f_j(x)$ and $g_j(x)$ are coprime in GR$(p^2, m)[x]$ when $\beta \neq 0$.
- $g_j(x) = f_j(x)^{p^{s-1}} M_j(x)$ when $\beta = 0$, where

$$M_j(x) = F_j(x)^{p^{s-1}} \Big(\sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{(k-1)p^{s-1}} \alpha_0^{p^s - kp^{s-1}} \Big) w_j(x) \prod_{i=1}^{j-1} v_i(x)$$

  is coprime to $f_j(x)$ in GR$(p^2, m)[x]$.

Moreover, the polynomials $f_1(x)^{p^s} + pg_1(x), f_2(x)^{p^s} + pg_2(x), \cdots, f_r(x)^{p^s} + pg_r(x)$ are pairwise coprime in GR$(p^2, m)[x]$.

Proof. To prove the result, we note that $\binom{p^s}{kp^{s-1}} = pa_k$ with $p \nmid a_k$ for $1 \leq k \leq p-1$, and that $\binom{p^s}{i} = 0$ in GR(p^2, m) for each integer i satisfying $1 \leq i \leq p^s - 1$ and $p^{s-1} \nmid i$. Using this, we see that

$$\begin{aligned} x^{np^s} - \lambda &= (x^n - \alpha_0)^{p^s} + \sum_{k=1}^{p-1} \binom{p^s}{kp^{s-1}} (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}} - p\beta \\ &= f_1(x)^{p^s} f_2(x)^{p^s} \cdots f_r(x)^{p^s} - p\big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\big). \end{aligned}$$

As $v_1(x) f_1(x)^{p^s} + w_1(x) f_2(x)^{p^s} f_3(x)^{p^s} \cdots f_r(x)^{p^s} = 1$, we can write

$$\begin{aligned} x^{np^s} - \lambda = &\left\{ f_1(x)^{p^s} - p\Big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\Big) w_1(x) \right\} \\ &\times \left\{ f_2(x)^{p^s} f_3(x)^{p^s} \cdots f_r(x)^{p^s} - p\Big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\Big) v_1(x) \right\}. \end{aligned}$$

Further, since $v_2(x) f_2(x)^{p^s} + w_2(x) f_3(x)^{p^s} f_4(x)^{p^s} \cdots f_r(x)^{p^s} = 1$, we see that

$$\begin{aligned} &f_2(x)^{p^s} f_3(x)^{p^s} \cdots f_r(x)^{p^s} - p\big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\big) v_1(x) \\ &= \left\{ f_2(x)^{p^s} - p\big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\big) v_1(x) w_2(x) \right\} \\ &\quad \times \left\{ f_3(x)^{p^s} f_4(x)^{p^s} \cdots f_r(x)^{p^s} - p\big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\big) v_1(x) v_2(x) \right\}. \end{aligned}$$

Proceeding like this, we see that

$$x^{np^s} - \alpha - p\beta = \prod_{j=1}^{r} \Big(f_j(x)^{p^s} + pg_j(x) \Big),$$

where $g_1(x) = -\Big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\Big)$ when $r = 1$; and

$g_j(x) = -\Big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\Big) w_j(x) \prod_{i=1}^{j-1} v_i(x)$ for $1 \leq j \leq r-1$ and

$g_r(x) = -\Big(\beta - \sum_{k=1}^{p-1} a_k (x^n - \alpha_0)^{kp^{s-1}} {\alpha_0}^{p^s - kp^{s-1}}\Big) \prod_{i=1}^{r-1} v_i(x)$ when $r \geq 2$.

From this and by applying Theorem 2.0.4(a), the desired result follows immediately. □

Next for $1 \leq j \leq r$, let us define $k_j(x) = f_j(x)^{p^s} + pg_j(x)$. Further, let deg $f_j(x) = d_j$ for each j. By Lemma 3.2.1, we see that

$$x^{np^s} - \lambda = x^{np^s} - \alpha - p\beta = \prod_{j=1}^{r} k_j(x)$$

is a factorization of $x^{np^s} - \lambda$ into monic pairwise coprime polynomials in GR$(p^2, m)[x]$. Now by applying the Chinese Remainder Theorem, we get

$$\mathcal{R}_{\alpha,\beta} = \text{GR}(p^2, m)[x]/\langle x^{np^s} - \alpha - p\beta\rangle \simeq \bigoplus_{j=1}^{r} \text{GR}(p^2, m)[x]/\langle k_j(x)\rangle.$$

From this point on, let $\mathcal{K}_j = \text{GR}(p^2, m)[x]/\langle k_j(x)\rangle$ for $1 \leq j \leq r$. Then we have the following:

Proposition 3.2.1. (a) If $\mathcal{C}$ is an $(\alpha + p\beta)$-constacyclic code of length np^s over GR(p^2, m) (i.e., an ideal of the ring $\mathcal{R}_{\alpha,\beta}$), then we have

$$\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_r,$$

where $\mathcal{C}_j$ is an ideal of $\mathcal{K}_j$ for $1 \leq j \leq r$.

(b) Let I_j be 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 $\mathcal{R}_{\alpha,\beta}$, (i.e., I is an $(\alpha + p\beta)$-constacyclic code of length np^s over GR(p^2, m)). Furthermore, we have $|I| = |I_1||I_2| \cdots |I_r|$.

Proof. Its proof is straightforward. □

Now let $\mathcal{C}$ be an $(\alpha + p\beta)$-constacyclic code of length np^s over GR(p^2, m). Then its dual code $\mathcal{C}^\perp$ is an $(\alpha + p\beta)^{-1}$-constacyclic code of length np^s over GR(p^2, m). Further, we see that $(\alpha + p\beta)^{-1} = \alpha^{-1} - p\beta\alpha^{-2}$, which implies that $\mathcal{C}^\perp$ is an ideal of the ring $\widehat{\mathcal{R}_{\alpha,\beta}} = \text{GR}(p^2, m)[x]/\langle x^{np^s} - (\alpha + p\beta)^{-1}\rangle = \mathcal{R}_{\alpha^{-1},-\beta\alpha^{-2}}$. To determine the dual code $\mathcal{C}^\perp$, we see that

$$x^{np^s} - (\alpha + p\beta)^{-1} = -(\alpha + p\beta)^{-1} k_1^*(x) k_2^*(x) \cdots k_r^*(x).$$

By applying the Chinese Remainder Theorem again, we obtain

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

where $\widehat{\mathcal{K}_j} = \text{GR}(p^2, m)[x]/\langle k_j^*(x)\rangle$ for $1 \leq j \leq r$. Now we make the following observation.

Proposition 3.2.2. Let $\mathcal{C}$ be an $(\alpha + p\beta)$-constacyclic code of length np^s over GR(p^2, m), i.e., an ideal of the ring $\mathcal{R}_{\alpha,\beta}$. If $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_r$ with $\mathcal{C}_j$ an ideal of the quotient ring $\mathcal{K}_j$ 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. Moreover, $\mathcal{C}_j^\perp$ is an ideal of the quotient ring $\widehat{\mathcal{K}_j} = \text{GR}(p^2, m)[x]/\langle k_j^*(x)\rangle$ for each j.

Proof. Proof is trivial. □

In view of Propositions 3.2.1 and 3.2.2, we see that to determine all $(\alpha + p\beta)$-constacyclic codes of length np^s over GR(p^2, m), their sizes and their dual codes, we need to determine all ideals of the quotient ring $\mathcal{K}_j$, their cardinalities and their orthogonal complements in the quotient ring $\widehat{\mathcal{K}_j}$ for $1 \leq j \leq r$. For this, throughout this chapter, let $1 \leq j \leq r$ be fixed. From now on, we shall represent elements of the quotient rings $\mathcal{K}_j$ and $\widehat{\mathcal{K}_j}$ (resp. $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$) by their representatives in GR$(p^2, m)[x]$ (resp. $\mathbb{F}_{p^m}[x]$) of degree less than $d_j p^s$ (resp. $d_j p^s$), and we shall perform their addition and multiplication modulo $k_j(x)$ and $k_j^*(x)$ (resp. $\overline{f_j(x)}^{p^s}$), respectively. Now to determine all ideals of the quotient ring $\mathcal{K}_j$, their orthogonal complements and their sizes, we shall first prove the following lemma:

Lemma 3.2.2. Let $1 \leq j \leq r$ be fixed. In the ring $\mathcal{K}_j$, we have the following:

(a) Any non-zero polynomial $a(x) \in \text{GR}(p^2, m)[x]$ that is coprime to $f_j(x)$ is a unit in $\mathcal{K}_j$. As a consequence, any non-zero polynomial $b(x) \in \text{GR}(p^2, m)[x]$ satisfying deg $b(x) < d_j$ and $\overline{b(x)} \neq 0$ is a unit in $\mathcal{K}_j$.

(b) $f_j(x)$ is nilpotent in $\mathcal{K}_j$ and $\langle f_j(x)^{p^s}\rangle = \begin{cases} \langle p\rangle & \text{if } \beta \neq 0; \\ \langle p f_j(x)^{p^{s-1}}\rangle & \text{if } \beta = 0. \end{cases}$

(c) The nilpotency index $\mathfrak{N}$ of $f_j(x)$ is given by

$$\mathfrak{N} = \begin{cases} 2p^s & \text{if } \beta \neq 0; \\ 2p^s - p^{s-1} & \text{if } \beta = 0. \end{cases}$$

Proof. *(a)* As $a(x) \in \text{GR}(p^2, m)[x]$ is coprime to $f_j(x)$ and $f_j(x)$ is a basic irreducible polynomial in $\text{GR}(p^2, m)[x]$, by Theorem 2.0.4(a), we see that the polynomials $f_j(x)^{p^s}$ and $a(x)$ are coprime in $\text{GR}(p^2, m)[x]$, which implies that there exist polynomials $q(x), r(x) \in \text{GR}(p^2, m)[x]$ such that $q(x)a(x) + r(x)f_j(x)^{p^s} = 1$ in $\text{GR}(p^2, m)[x]$. This gives $q(x)a(x) = 1 + pr(x)g_j(x)$ in $\mathcal{K}_j$. From this and using the fact that $p^2 = 0$ in $\mathcal{K}_j$, we see that $a(x)$ is a unit in $\mathcal{K}_j$.

On the other hand, if $b(x) \in \text{GR}(p^2, m)[x]$ satisfies deg $b(x) < d_j$ and $\overline{b(x)} \neq 0$, then by applying Theorem 2.0.4(a), we see that $b(x)$ and $f_j(x)$ are coprime in $\text{GR}(p^2, m)[x]$, from which the desired result follows.

(b) In $\mathcal{K}_j$, we see that $f_j(x)^{p^s} = -pg_j(x) \in \langle p\rangle$, which implies that $f_j(x)$ is nilpotent in $\mathcal{K}_j$.

When $\beta \neq 0$, by Lemma 3.2.1, we see that $f_j(x)$ and $g_j(x)$ are coprime in $\text{GR}(p^2, m)[x]$. Now by part (a), we note that $g_j(x)$ is a unit in $\mathcal{K}_j$, which implies that $\langle f_j(x)^{p^s}\rangle = \langle p\rangle$. Finally, when $\beta = 0$, by Lemma 3.2.1, we have $g_j(x) = f_j(x)^{p^{s-1}} M_j(x)$, where $M_j(x)$ is coprime to $f_j(x)$ in $\text{GR}(p^2, m)[x]$. This implies that $f_j(x)^{p^s} = -pf_j(x)^{p^{s-1}} M_j(x)$. By part (a), we see that $M_j(x)$ is a unit in $\mathcal{K}_j$. From this, we obtain $\langle f_j(x)^{p^s}\rangle = \langle p f_j(x)^{p^{s-1}}\rangle$.

(c) When $\beta \neq 0$, by part (b), we have $\langle f_j(x)^{p^s}\rangle = \langle p\rangle$, which implies that the nilpotency index of $f_j(x)$ in $\mathcal{K}_j$ is $2p^s$. Next when $\beta = 0$, by part (b), we see that $\langle f_j(x)^{p^s}\rangle = \langle p f_j(x)^{p^{s-1}}\rangle$. This implies that $pf_j(x)^{p^s} = 0$. We further observe that $pf_j(x)^{p^s-1} \neq 0$ in $\mathcal{K}_j$. From this, it follows that the nilpotency index of $f_j(x)$ in $\mathcal{K}_j$ is $2p^s - p^{s-1}$.

□

For a positive integer k and a subset $\mathcal{S}$ of GR(p^2, m) with $0 \in \mathcal{S}$, let us recall that $\mathcal{P}_k(\mathcal{S}) = \{g(x) \in \mathcal{S}[x] : \text{ either } g(x) = 0 \text{ or deg } g(x) < k\}$. By repeatedly applying the division algorithm in GR$(p^2, m)[x]$, every element $A(x) \in \mathcal{K}_j$ can be uniquely written as

$$A(x) = \sum_{i=0}^{p^s-1} A_i(x) f_j(x)^i,$$

where $A_i(x) \in \mathcal{P}_{d_j}(\text{GR}(p^2, m))$ for $0 \leq i \leq p^s - 1$. Further, each $A_i(x) \in \mathcal{P}_{d_j}(\text{GR}(p^2, m))$ can be uniquely expressed as $A_i(x) = A_{i0}(x) + pA_{i1}(x)$, where $A_{i0}(x), A_{i1}(x) \in \mathcal{P}_{d_j}(\mathcal{T})$. In view of this, we see that every element $A(x) \in \mathcal{K}_j$ can be uniquely expressed as

$$A(x) = \sum_{i=0}^{p^s-1} A_{i0}(x) f_j(x)^i + p \sum_{i=0}^{p^s-1} A_{i1}(x) f_j(x)^i,$$

where $A_{i0}(x), A_{i1}(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for each i.

The following lemma is useful in the determination of cardinalities of ideals of $\mathcal{K}_j$.

Lemma 3.2.3. Let $1 \leq j \leq r$ be fixed, and let $\mathcal{I}$ be an ideal of $\mathcal{K}_j$. Then

$$\text{Tor}_0(\mathcal{I}) = \Big\{ \overline{a_0(x)} \in \mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle : a_0(x) + pa_1(x) \in \mathcal{I} \text{ for some } a_0(x), a_1(x) \in \mathcal{P}_{d_j p^s}(\mathcal{T}) \Big\}$$

and

$$\text{Tor}_1(\mathcal{I}) = \Big\{ \overline{a_1(x)} \in \mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle : pa_1(x) \in \mathcal{I} \text{ for some } a_1(x) \in \mathcal{P}_{d_j p^s}(\mathcal{T}) \Big\}$$

are ideals of $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$. Moreover, we have

$$|\mathcal{I}| = |\text{Tor}_0(\mathcal{I})||\text{Tor}_1(\mathcal{I})|.$$

Proof. One can easily show that $\text{Tor}_0(\mathcal{I})$ and $\text{Tor}_1(\mathcal{I})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$. To prove the second part, we shall view GR(p^2, m) as an $\mathbb{F}_{p^m}-$module with respect to the addition in GR(p^2, m) and the scalar product defined as $\overline{a}r = ar$ for each $a \in \mathcal{T}$ and $r \in \text{GR}(p^2, m)$. Further, we note that $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$ can be viewed as an $\mathbb{F}_{p^m}$-module. Thus the ideals $\text{Tor}_0(\mathcal{I})$ and $\text{Tor}_1(\mathcal{I})$ of $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$ can also be viewed as $\mathbb{F}_{p^m}$-modules.

Now define a map $\phi : \mathcal{I} \to \text{Tor}_0(\mathcal{I})$ as $\phi(a(x)) = \overline{a_0(x)}$ for each $a(x) = a_0(x)+pa_1(x) \in \mathcal{I}$ with $a_0(x), a_1(x) \in \mathcal{P}_{d_j p^s}(\mathcal{T})$. We see that ϕ is a surjective $\mathbb{F}_{p^m}$-module homomorphism and its kernel is given by

$$\ker \phi = \{a_0(x) + pa_1(x) \in \mathcal{I} : \overline{a_0(x)} = 0\} = \{pa_1(x) \in \mathcal{I} : a_1(x) \in \mathcal{P}_{d_j p^s}(\mathcal{T})\}.$$

This implies that $|\mathcal{I}| = |\text{Tor}_0(\mathcal{I})||\ker \phi|$. Further, one can easily see that $|\text{Tor}_1(\mathcal{I})| = |\ker \phi|$. From this, the desired result follows immediately. □

The following lemma is useful in the determination of orthogonal complements of all ideals of the ring $\mathcal{K}_j$.

Lemma 3.2.4. Let $1 \leq j \leq r$ be a fixed integer. Let $\mathcal{I}$ be an ideal of the ring $\mathcal{K}_j$, and let $\mathcal{I}^\perp$ be the orthogonal complement of $\mathcal{I}$ in $\widehat{\mathcal{K}_j}$. Then the following hold.

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

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

(c) If $\mathcal{I} = \langle f(x), pg(x)\rangle$, then $\mathcal{I}^* = \langle f^*(x), pg^*(x)\rangle$.

(d) For $f(x), g(x) \in \mathcal{K}_j$, let us define $(fg)(x) = f(x)g(x)$ and $(f+g)(x) = f(x)+g(x)$. If $f(x), g(x), (fg)(x)$ all are non-zero, then we have

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

If $f(x), g(x), (f+g)(x)$ all are non-zero, then we have

$$(f+g)^*(x) = \begin{cases} f^*(x) + x^{deg\, f(x)-deg\, g(x)}g^*(x) & \text{if deg } f(x) > \text{deg } g(x); \\ x^{\deg (f+g)(x)-\deg \text{f(x)}}(f^*(x) + g^*(x)) & \text{if deg } f(x) = \text{deg } g(x). \end{cases}$$

Proof. Its proof is straightforward. □

From now on, we shall distinguish the following two cases: $\beta \neq 0$ and $\beta = 0$.

In the following theorem, we determine all ideals of the ring $\mathcal{K}_j$, their sizes and their orthogonal complements in $\widehat{\mathcal{K}_j}$ when β is non-zero.

Theorem 3.2.1. When $\beta \neq 0$, the ring $\mathcal{K}_j$ is a finite commutative chain ring with unity whose ideals are given by

$$\{0\} \subset \langle f_j(x)^{2p^s-1} \rangle \subset \langle f_j(x)^{2p^s-2} \rangle \subset \cdots \subset \langle f_j(x)^2 \rangle \subset \langle f_j(x) \rangle \subset \mathcal{K}_j.$$

Moreover, for $0 \leq \nu \leq 2p^s$, the ideal $\langle f_j(x)^\nu \rangle$ has $p^{md_j(2p^s-\nu)}$ elements and the orthogonal complement of $\langle f_j(x)^\nu \rangle$ is given by $\langle f_j^*(x)^{2p^s-\nu} \rangle$.

Proof. To prove the result, we see that each element $A(x) \in \mathcal{K}_j$ can be uniquely expressed as

$$A(x) = \sum_{i=0}^{p^s-1} A_{i0}(x) f_j(x)^i + p \sum_{i=0}^{p^s-1} A_{i1}(x) f_j(x)^i,$$

where $A_{i0}(x), A_{i1}(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for each i. As $f_j(x)$ and p are nilpotent in $\mathcal{K}_j$, we see that $A(x)$ is a unit in $\mathcal{K}_j$ if and only if $A_{00}(x)$ is a unit in $\mathcal{K}_j$. Further, by Lemma 3.2.2(a), we observe that $A_{00}(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ is a unit in $\mathcal{K}_j$ if and only if $A_{00}(x) \neq 0$. In view of this and by applying Lemma 3.2.2(b), we see that $A(x)$ is a unit in $\mathcal{K}_j$ if and only if $A(x) \notin \langle f_j(x) \rangle$. This shows that all the non-units of $\mathcal{K}_j$ are given by $\langle f_j(x) \rangle$. Therefore $\mathcal{K}_j$ is a local ring with the unique maximal ideal as $\langle f_j(x) \rangle$. This, by Theorem 2.0.5 and Lemma 3.2.2(c), implies that $\mathcal{K}_j$ is a chain ring and all its ideals are given by $\langle f_j(x)^\nu \rangle$, where $0 \leq \nu \leq 2p^s$. Further, we observe that $|\overline{\mathcal{K}_j}| = |\mathcal{K}_j / \langle f_j(x) \rangle| = p^{md_j}$. Now by applying Theorem 2.0.5 and Lemma 3.2.2(c) again, we see that $|\langle f_j(x)^\nu \rangle| = p^{md_j(2p^s-\nu)}$ for $0 \leq \nu \leq 2p^s$. In order to determine their dual codes, let $\mathcal{I} = \langle f_j(x)^\nu \rangle$, where $0 \leq \nu \leq 2p^s$. Here it is easy to observe that $\text{ann}(\mathcal{I}) = \langle f_j(x)^{2p^s-\nu} \rangle$, which, by Lemma 3.2.4, gives $\mathcal{I}^\perp = \text{ann}(\mathcal{I})^* = \langle f_j^*(x)^{2p^s-\nu} \rangle$. This completes the proof of the theorem. □

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

Corollary 3.2.1. Let $\alpha = \alpha_0^{p^s} \in \mathcal{T} \setminus \{0\}$, where $\alpha_0 \in \mathcal{T}$ is such that $x^n - \alpha_0$ is basic irreducible over GR(p^2, m). When $\beta(\neq 0) \in \mathcal{T}$, the ideal $\langle (x^n - \alpha_0)^{p^s} \rangle = \langle p \rangle$ is the only isodual $(\alpha + p\beta)$-constacyclic code of length np^s over GR(p^2, m).

Proof. As $x^n - \alpha_0$ is basic irreducible over GR(p^2, m), by Theorem 3.2.1, we see that all $(\alpha + p\beta)$-constacyclic codes of length np^s over GR(p^2, m) are given by $\langle (x^n - \alpha_0)^\nu \rangle$, where $0 \leq \nu \leq 2p^s$. If $\mathcal{I} = \langle (x^n - \alpha_0)^\nu \rangle$, then by Theorem 3.2.1 again, we note that $|\mathcal{I}| = p^{mn(2p^s - \nu)}$ and $\mathcal{I}^\perp = \langle (x^n - \alpha_0^{-1})^{2p^s - \nu} \rangle$ for each ν. Working as in Theorem 3.2.1, we see that $|\mathcal{I}^\perp| = p^{mn\nu}$ for $0 \leq \nu \leq 2p^s$. Now if the code $\mathcal{I} = \langle (x^n - \alpha_0)^\nu \rangle$ is isodual, then we must have $|\mathcal{I}| = |\mathcal{I}^\perp|$, which implies that $\nu = p^s$. On the other hand, we see that the codes $\langle (x^n - \alpha_0)^{p^s} \rangle = \langle p \rangle (\subseteq \mathcal{R}_{\alpha,\beta})$ and $\langle (x^n - \alpha_0^{-1})^{p^s} \rangle = \langle p \rangle (\subseteq \widehat{\mathcal{R}_{\alpha,\beta}})$ are clearly GR(p^2, m)-linearly equivalent, which completes the proof. □

From this point on, throughout this chapter, we assume that $\beta = 0$.

In the following theorem, we determine all ideals of the ring $\mathcal{K}_j$ when $\beta = 0$.

Theorem 3.2.2. When $\beta = 0$, all the distinct ideals of the ring $\mathcal{K}_j$ are as listed below:

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

$$\{0\}, \ \mathcal{K}_j.$$

- **Type II:** (Principal ideals with non-monic polynomial generators)

$$\langle p f_j(x)^\tau \rangle, \text{ where } 0 \leq \tau < p^s.$$

- **Type III:** (Principal ideals with monic polynomial generators)

$$\langle f_j(x)^\omega + p f_j(x)^t G(x) \rangle,$$

where $0 < \omega < p^s$, $0 \leq t < \kappa$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{i=0}^{\kappa - t - 1} a_i(x) f_j(x)^i$ with $a_i(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for $0 \leq i \leq \kappa - t - 1$, with κ as the smallest integer satisfying $0 \leq \kappa \leq \omega$ and $p f_j(x)^\kappa \in \langle f_j(x)^\omega + p f_j(x)^t G(x) \rangle$.

- **Type IV:** (Non-principal ideals)

$$\langle f_j(x)^\omega + p f_j(x)^t G(x), p f_j(x)^\mu \rangle,$$

where $0 \leq \mu < \kappa \leq \omega < p^s$, $0 \leq t < \mu$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{i=0}^{\mu-t-1} a_i(x) f_j(x)^i$, $a_i(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for $0 \leq i \leq \mu - t - 1$, with κ as the smallest integer satisfying $p f_j(x)^\kappa \in \langle f_j(x)^\omega + p f_j(x)^t G(x) \rangle$.

Proof. Let $\mathcal{I}$ be a non-trivial ideal of $\mathcal{K}_j$. Now the following two cases arise: **(i)** $\mathcal{I} \subseteq \langle p \rangle$ and **(ii)** $\mathcal{I} \nsubseteq \langle p \rangle$.

(i) First suppose that $\mathcal{I} \subseteq \langle p \rangle$. In this case, each element $Q(x) \in \mathcal{I}$ can be uniquely written as

$$Q(x) = p \sum_{i=0}^{p^s-1} A_i^{(Q)}(x) f_j(x)^i,$$

where $A_i^{(Q)}(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for $0 \leq i \leq p^s - 1$. Further, for each $Q(x)(\neq 0) \in \mathcal{I}$, we observe that there exists a smallest integer k_Q satisfying $0 \leq k_Q \leq p^s - 1$ and $A_{k_Q}^{(Q)}(x) \neq 0$. Let

$$\tau = \min\{k_Q : Q(x) \in \mathcal{I} \setminus \{0\}\}.$$

We note that $0 \leq \tau \leq p^s - 1$ and that there exists $Q_0(x)(\neq 0) \in \mathcal{I}$ such that $k_{Q_0} = \tau$, i.e.,

$$Q_0(x) = p f_j(x)^\tau \sum_{i=\tau}^{p^s-1} A_i^{(Q_0)}(x) f_j(x)^{i-\tau}$$

with $A_\tau^{(Q_0)}(x) \neq 0$. By Lemma 3.2.2, we observe that $\sum_{i=\tau}^{p^s-1} A_i^{(Q_0)}(x) f_j(x)^{i-\tau}$ is a unit in $\mathcal{K}_j$, which implies that $\langle p f_j(x)^\tau \rangle = \langle Q_0(x) \rangle \subseteq \mathcal{I}$. Moreover, each element $Q(x) \in \mathcal{I}$ can be written as

$$Q(x) = p f_j(x)^\tau \sum_{i=k_Q}^{p^s-1} A_i^{(Q)}(x) f_j(x)^{i-\tau},$$

which implies that $\mathcal{I} \subseteq \langle p f_j(x)^\tau \rangle$. This gives $\mathcal{I} = \langle p f_j(x)^\tau \rangle$ with $0 \leq \tau \leq p^s - 1$, which is of Type II.

(ii) Next suppose that $\mathcal{I} \nsubseteq \langle p \rangle$. Here each element $Q(x) \in \mathcal{I}$ can be uniquely written as

$$Q(x) = \sum_{i=0}^{p^s-1} A_i^{(Q)}(x) f_j(x)^i + p \sum_{\ell=0}^{p^s-1} B_\ell^{(Q)}(x) f_j(x)^\ell,$$

where $A_i^{(Q)}(x), B_\ell^{(Q)}(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for each i and ℓ. Now let us define

$$\mathcal{I}_1 = \{Q(x) \in \mathcal{I} : A_i^{(Q)}(x) \neq 0 \text{ for some } i,\ 0 \leq i \leq p^s - 1\}$$

and

$$\mathcal{I}_2 = \{Q(x) \in \mathcal{I} : A_i^{(Q)}(x) = 0 \text{ for all } i,\ 0 \leq i \leq p^s - 1\}.$$

Since $\mathcal{I} \not\subseteq \langle p \rangle$, we see that $\mathcal{I}_1$ is a non-empty set and $0 \notin \mathcal{I}_1$. We also observe that $p\mathcal{I}_1 \subseteq \mathcal{I}_2$, which implies that $\mathcal{I}_2 \neq \{0\}$. Further, we note that $\mathcal{I}_2$ is a non-zero ideal of $\mathcal{K}_j$ and $\mathcal{I}_2 \subseteq \langle p \rangle$. This, by case (i), implies that $\mathcal{I}_2 = \langle p f_j(x)^\mu \rangle$ for some integer $\mu,\ 0 \leq \mu \leq p^s - 1$. Next for each $Q(x) \in \mathcal{I}_1$, there exists a smallest integer ω_Q satisfying $0 \leq \omega_Q \leq p^s - 1$ and $A_{\omega_Q}^{(Q)}(x) \neq 0$, i.e., each $Q(x) \in \mathcal{I}_1$ can be written as

$$Q(x) = f_j(x)^{\omega_Q} W_Q(x) + pM_Q(x),$$

where $W_Q(x) = \sum_{i=\omega_Q}^{p^s-1} A_i^{(Q)}(x) f_j(x)^{i-\omega_Q}$ and $M_Q(x) = \sum_{\ell=0}^{p^s-1} B_\ell^{(Q)}(x) f_j(x)^\ell$ in $\mathcal{K}_j$. By Lemma 3.2.2, we see that $W_Q(x)$ is a unit in $\mathcal{K}_j$. Now let

$$\omega = \min\{\omega_Q : Q(x) \in \mathcal{I}_1\}.$$

As $\mathcal{I} \neq \mathcal{K}_j$, we see that $1 \leq \omega \leq p^s - 1$. Also, there exists $Q_1(x) \in \mathcal{I}_1$ such that $\omega_{Q_1} = \omega$, i.e., $Q_1(x) = f_j(x)^\omega W_{Q_1}(x) + pM_{Q_1}(x)$, where $W_{Q_1}(x), M_{Q_1}(x) \in \mathcal{K}_j$. For each $Q(x) \in \mathcal{I}_1$, we observe that

$$\begin{aligned} Q(x) &= f_j(x)^{\omega_Q} W_Q(x) + pM_Q(x) \\ &= p\{M_Q(x) - M_{Q_1}(x) W_{Q_1}(x)^{-1} W_Q(x) f_j(x)^{\omega_Q - \omega}\} + \\ &\quad f_j(x)^{\omega_Q - \omega} W_Q(x) Q_1(x) W_{Q_1}(x)^{-1}. \end{aligned}$$

From this, we see that

$$p\left(M_Q(x) - M_{Q_1}(x) W_{Q_1}(x)^{-1} W_Q(x) f_j(x)^{\omega_Q - \omega}\right) \in \mathcal{I}_2 = \langle p f_j(x)^\mu \rangle$$

for every $Q(x) \in \mathcal{I}_1$. This implies that each $Q(x) \in \mathcal{I}_1$ can be written as $Q(x) = Q_1(x)U_Q(x) + pf_j(x)^\mu K_Q(x)$ for some $U_Q(x), K_Q(x) \in \mathcal{K}_j$. From this, we get

$$\mathcal{I} = \langle Q_1(x), pf_j(x)^\mu \rangle = \langle f_j(x)^\omega W_{Q_1}(x) + pM_{Q_1}(x), pf_j(x)^\mu \rangle.$$

As $W_{Q_1}(x)$ is a unit in $\mathcal{K}_j$, we obtain

$$\mathcal{I} = \langle f_j(x)^\omega + pM_{Q_1}(x)W_{Q_1}(x)^{-1}, pf_j(x)^\mu \rangle.$$

Let us write

$$pM_{Q_1}(x)W_{Q_1}(x)^{-1} = p\sum_{i=0}^{p^s-1} \mathcal{G}_i(x)f_j(x)^i,$$

where $\mathcal{G}_i(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for $0 \leq i \leq p^s - 1$. For all $i \geq \mu$, we note that $pf_j(x)^i \in \langle pf_j(x)^\mu \rangle (\subseteq \mathcal{I})$, which implies that

$$\mathcal{I} = \langle f_j(x)^\omega + p\sum_{i=0}^{\mu-1} \mathcal{G}_i(x)f_j(x)^i, pf_j(x)^\mu \rangle.$$

Let us denote $G_1(x) = \sum_{i=0}^{\mu-1} \mathcal{G}_i(x)f_j(x)^i$. When $G_1(x) \neq 0$, there exists a smallest integer t $(0 \leq t < \mu)$ satisfying $\mathcal{G}_t(x) \neq 0$ and we can write $G_1(x) = f_j(x)^t G(x)$, where $G(x) = \sum_{i=t}^{\mu-1} \mathcal{G}_i(x)f_j(x)^{i-t}$ is a unit in $\mathcal{K}_j$. When $G_1(x) = 0$, we choose $G(x) = 0$. From this, we have

$$\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^t G(x), pf_j(x)^\mu \rangle,$$

where $G(x)$ is either 0 or a unit in $\mathcal{K}_j$ of the form $\sum_{i=0}^{\mu-t-1} a_i(x)f_j(x)^i$ with $a_i(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for $0 \leq i \leq \mu - t - 1$. Since κ is the smallest non-negative integer satisfying $pf_j(x)^\kappa \in \langle f_j(x)^\omega + pf_j(x)^t G(x) \rangle$ and $pf_j(x)^\omega \in \langle f_j(x)^\omega + pf_j(x)^t G(x) \rangle$, we get $\kappa \leq \omega$. As $pf_j(x)^\kappa \in \mathcal{I}_2$, we must have $\mu \leq \kappa$. Moreover, when $\mu = \kappa$, we note that $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^t G(x) \rangle$, i.e., $\mathcal{I}$ is of Type III. In the view of this, we see that for $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^t G(x), pf_j(x)^\mu \rangle$ to be of Type IV, we must have $\mu < \kappa$.

This completes the proof of the theorem. □

By the above theorem, we see that κ is the smallest non-negative integer satisfying $pf_j(x)^\kappa \in \langle f_j(x)^\omega + pf_j(x)^t G(x)\rangle$. As $pf_j(x)^\omega \in \langle f_j(x)^\omega + pf_j(x)^t G(x)\rangle$, we have $\kappa \leq \omega$. Further, the element $pf_j(x)^\kappa$ can be written as

$$pf_j(x)^\kappa = \Big(f_j(x)^\omega + pf_j(x)^t G(x)\Big)\left(\sum_{i=0}^{p^s-1} A_i(x) f_j(x)^i + p\sum_{\ell=0}^{p^s-1} B_\ell(x) f_j(x)^\ell\right), \quad (3.2.1)$$

where $A_i(x), B_\ell(x) \in \mathcal{P}_{d_j}(\mathcal{T})$ for each i and ℓ.

In the following proposition, we determine the integer κ when $\beta = 0$.

Proposition 3.2.3. Let $\beta = 0$, and let us write $p(M_j(x) - G(x)) = pf_j(x)^\rho A_G(x)$, where $0 \leq \rho < p^s$ and $A_G(x)$ is either 0 or a unit in $\mathcal{K}_j$. Then we have

$$\kappa = \begin{cases} \min\{\omega, p^{s-1}\} & \text{if } G(x) = 0; \\ \min\{\omega, p^s - \omega + t, p^{s-1}\} & \text{if } G(x) \neq 0 \text{ and } \omega \neq p^s - p^{s-1} + t; \\ \min\{\omega, p^{s-1} + \rho\} & \text{if } G(x) \neq 0, \omega = p^s - p^{s-1} + t, A_G(x) \neq 0 \text{ and} \\ & \rho < p^s - p^{s-1}; \\ \omega & \text{if } G(x) \neq 0, \omega = p^s - p^{s-1} + t \text{ with either } A_G(x) = 0 \text{ or} \\ & A_G(x) \neq 0 \text{ and } \rho \geq p^s - p^{s-1}. \end{cases}$$

Proof. Since $f_j(x)^{p^s} = -pf_j(x)^{p^{s-1}} M_j(x)$, equation (3.2.1) can be rewritten as

$$\begin{aligned} pf_j(x)^\kappa = \sum_{i=0}^{p^s-\omega-1} A_i(x) f_j(x)^{i+\omega} - p\sum_{i=p^s-\omega}^{p^s-1} A_i(x) f_j(x)^{i+\omega-p^s+p^{s-1}} M_j(x) \\ + p\sum_{i=0}^{p^s-1} A_i(x) f_j(x)^{i+t} G(x) + p\sum_{\ell=0}^{p^s-1} B_\ell(x) f_j(x)^{\ell+\omega}. \end{aligned}$$

This gives $\sum_{i=0}^{p^s-\omega-1} \overline{A_i(x)}\ \overline{f_j(x)}^{i+\omega} = 0$ in $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s}\rangle$. This implies that $\overline{A_i(x)} = 0$, which further implies that $A_i(x) = 0$ for $0 \leq i \leq p^s - \omega - 1$. From this, we obtain

$$\begin{aligned} pf_j(x)^\kappa = -p\sum_{i=p^s-\omega}^{p^s-1} A_i(x) f_j(x)^{i+\omega-p^s+p^{s-1}} M_j(x) + p\sum_{i=p^s-\omega}^{p^s-1} A_i(x) f_j(x)^{i+t} G(x) \\ + p\sum_{\ell=0}^{p^s-1} B_\ell(x) f_j(x)^{\ell+\omega}. \end{aligned} \quad (3.2.2)$$

When $G(x) = 0$, by (3.2.2), we get $\kappa \geq \min\{\omega, p^{s-1}\}$. Further, as $pf_j(x)^{p^{s-1}} M_j(x) = -f_j(x)^{p^s}$ and $\kappa \leq \omega$, we get $\kappa = \min\{\omega, p^{s-1}\}$.

From now on, throughout the proof, we assume that $G(x)$ is a unit in $\mathcal{K}_j$. Here we shall consider the following two cases separately: $p^s - p^{s-1} + t - \omega \neq 0$ and $p^s - p^{s-1} + t - \omega = 0$.

First let $p^s - p^{s-1} + t - \omega \neq 0$. In this case, we note that

$$\begin{aligned} p(-f_j(x)^{p^{s-1}} M_j(x) + f_j(x)^{p^s-\omega+t} G(x)) &= f_j(x)^{p^s} + pf_j(x)^{p^s-\omega+t} G(x) \\ &= f_j(x)^{p^s-\omega}\{f_j(x)^{\omega} + pf_j(x)^t G(x)\}. \end{aligned}$$

From this and using the fact that $p^s - p^{s-1} - \omega + t \neq 0$, we get

$$\kappa \leq \min\{p^s - \omega + t, p^{s-1}\}.$$

Now by (3.2.2), we obtain $\kappa = \min\{\omega, p^s - \omega + t, p^{s-1}\}$.

Next suppose that $\omega = p^s - p^{s-1} + t$. In this case, (3.2.2) can be rewritten as

$$pf_j(x)^{\kappa} = -p \sum_{i=p^s-\omega}^{p^s-1} A_i(x) f_j(x)^{i+\omega-p^s+p^{s-1}+\rho} A_G(x) + p \sum_{\ell=0}^{p^s-1} B_\ell(x) f_j(x)^{\ell+\omega}. \quad (3.2.3)$$

By (3.2.3), we see that $\kappa = \omega$ when $A_G(x) = 0$.

Further, let $A_G(x)$ be a unit in $\mathcal{K}_j$. When $\rho \geq p^s - p^{s-1}$, (3.2.3) becomes

$$pf_j(x)^{\kappa} = p \sum_{\ell=0}^{p^s-1} B_\ell(x) f_j(x)^{\ell+\omega},$$

which gives $\kappa = \omega$. On the other hand, we see that

$$pf_j(x)^{p^{s-1}+\rho} A_G(x) = pf_j(x)^{p^{s-1}}(M_j(x) - G(x)) = -f_j(x)^{p^s-\omega}\{f_j(x)^{\omega} + pf_j(x)^t G(x)\},$$

which gives $\kappa \leq p^{s-1} + \rho$ when $\rho < p^s - p^{s-1}$. From this and using (3.2.3), we get $\kappa = \min\{\omega, p^{s-1} + \rho\}$ when $\rho < p^s - p^{s-1}$. □

In the following theorem, we determine cardinalities of all ideals of $\mathcal{K}_j$ when $\beta = 0$.

Theorem 3.2.3. Suppose that $\beta = 0$. Let $\mathcal{I}$ be an ideal of $\mathcal{K}_j$ (as determined in Theorem 3.2.2).

(a) If $\mathcal{I} = \{0\}$, then $|\mathcal{I}| = 1$.

(b) If $\mathcal{I} = \mathcal{K}_j$, then $|\mathcal{I}| = p^{2md_jp^s}$.

(c) If $\mathcal{I} = \langle pf_j(x)^\tau \rangle$ is of Type II, then $|\mathcal{I}| = p^{md_j(p^s-\tau)}$.

(d) Let $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^tG(x) \rangle$ be of Type III. Let us write $p(M_j(x) - G(x)) = pf_j(x)^\rho A_G(x)$, where $0 \leq \rho < p^s$ and $A_G(x)$ is either 0 or a unit in $\mathcal{K}_j$. Then

$$|\mathcal{I}| = \begin{cases} p^{2md_j(p^s-\omega)} & \text{if either } G(x) = 0, \omega \leq p^{s-1} \text{ or } G(x) \neq 0, p^s - 2\omega \\ & +t \geq 0, \omega \leq p^{s-1}, \omega \neq p^s - p^{s-1} + t \text{ or } G(x) \neq 0, A_G(x) = 0, \\ & \omega = p^s - p^{s-1} + t \text{ or } G(x) \neq 0, A_G(x) \neq 0, \omega = p^s - p^{s-1} + t, \\ & \rho \geq p^s - p^{s-1} \text{ or } G(x) \neq 0, A_G(x) \neq 0, \omega = p^s - p^{s-1} + t \leq \\ & p^{s-1} + \rho; \\ p^{md_j(p^s-t)} & \text{if } G(x) \neq 0, p^s - 2\omega + t \leq 0, p^s - p^{s-1} - \omega + t < 0; \\ p^{md_j(2p^s-\omega-p^{s-1})} & \text{if } G(x) = 0, \omega > p^{s-1} \text{ or } G(x) \neq 0, \omega \geq p^{s-1}, \\ & p^s - p^{s-1} - \omega + t > 0; \\ p^{md_j(2p^s-\omega-p^{s-1}-\rho)} & \text{if } G(x) \neq 0, A_G(x) \neq 0, \omega = p^s - p^{s-1} + t, \omega > p^{s-1} + \rho. \end{cases}$$

(e) If $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^tG(x), pf_j(x)^\mu \rangle$ is of Type IV, then $|\mathcal{I}| = p^{md_j(2p^s-\mu-\omega)}$.

Proof. To prove the result, we see, by Lemma 3.2.3, that

$$|\mathcal{I}| = |\text{Tor}_0(\mathcal{I})||\text{Tor}_1(\mathcal{I})|.$$

So we need to determine cardinalities of $\text{Tor}_0(\mathcal{I})$ and $\text{Tor}_1(\mathcal{I})$, which are ideals of the quotient ring $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$. To do this, we first note that the nilpotency index of $\overline{f_j(x)}$ in $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$ is p^s. Further, by Theorem 2.0.5, we observe that $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$ is a finite commutative chain ring with unity and all its ideals are given by $\langle \overline{f_j(x)}^i \rangle$, where $0 \leq i \leq p^s$. We also observe that the residue field of $\mathbb{F}_{p^m}[x]/\langle \overline{f_j(x)}^{p^s} \rangle$ is of order p^{md_j}. This,

by Theorem 2.0.5 again, implies that

$$|\langle\overline{f_j(x)}^i\rangle| = p^{md_j(p^s-i)} \text{ for } 0 \leq i \leq p^s. \tag{3.2.4}$$

(a) If $\mathcal{I} = \{0\}$, then $\text{Tor}_0(\mathcal{I}) = \text{Tor}_1(\mathcal{I}) = \{0\}$, which gives $|\mathcal{I}| = 1$.

(b) If $\mathcal{I} = \mathcal{K}_j$, then $\text{Tor}_0(\mathcal{I}) = \text{Tor}_1(\mathcal{I}) = \langle 1\rangle = \mathbb{F}_{p^m}[x]/\langle\overline{f_j(x)}^{p^s}\rangle$. From this and using (3.2.4), we get $|\mathcal{I}| = p^{2md_jp^s}$.

(c) If $\mathcal{I} = \langle pf_j(x)^\tau\rangle$ is of Type II, then $\text{Tor}_0(\mathcal{I}) = \{0\}$ and $\text{Tor}_1(\mathcal{I}) = \langle\overline{f_j(x)}^\tau\rangle$. From this and using (3.2.4), we obtain $|\mathcal{I}| = p^{md_j(p^s-\tau)}$.

(d) If $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^tG(x)\rangle$ is of Type III, then it is easy to see that $\text{Tor}_0(\mathcal{I}) = \langle\overline{f_j(x)}^\omega\rangle$ and $\text{Tor}_1(\mathcal{I}) = \langle\overline{f_j(x)}^\kappa\rangle$. Now by applying Proposition 3.2.3 and using (3.2.4), part (d) follows.

(e) If $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^tG(x), pf_j(x)^\mu\rangle$ is of Type IV, then $\text{Tor}_0(\mathcal{I}) = \langle\overline{f_j(x)}^\omega\rangle$ and $\text{Tor}_1(\mathcal{I}) = \langle\overline{f_j(x)}^\mu\rangle$. From this and using (3.2.4), we get $|\mathcal{I}| = p^{md_j(2p^s-\mu-\omega)}$.

□

In the following theorem, we determine the orthogonal complement of each ideal of $\mathcal{K}_j$ when $\beta = 0$.

Theorem 3.2.4. Suppose that $\beta = 0$. Let $\mathcal{I}$ be an ideal of $\mathcal{K}_j$ (as determined in Theorem 3.2.2).

(a) If $\mathcal{I} = \{0\}$, then $\mathcal{I}^\perp = \widehat{\mathcal{K}_j} = \text{GR}(p^2, m)[x]/\langle k_j^*(x)\rangle$.

(b) If $\mathcal{I} = \mathcal{K}_j$, then $\mathcal{I}^\perp = \{0\}$.

(c) If $\mathcal{I} = \langle pf_j(x)^\tau\rangle$ is of Type II, then $\mathcal{I}^\perp = \langle f_j^*(x)^{p^s-\tau}, p\rangle$.

(d) Let $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^tG(x)\rangle$ be of Type III. Let us write $p(M_j(x) - G(x)) = pf_j(x)^\rho A_G(x)$, where $0 \leq \rho < p^s$ and $A_G(x)$ is either 0 or a unit in $\mathcal{K}_j$. When $G(x) \neq 0, t = \omega - p^s + p^{s-1}$ with either $A_G(x) = 0$ or $A_G(x) \neq 0$ and $\rho \geq p^s - p^{s-1}$, we have $\mathcal{I} = \langle f_j(x)^\omega + pf_j(x)^{\omega-p^s+p^{s-1}}M_j(x)\rangle$. Furthermore, we have

$$\mathcal{I}^{\perp} = \begin{cases} \langle f_j^*(x)^{p^s-\omega} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}-\omega} M_j^*(x) \rangle \text{ if } G(x) = 0 \text{ and} \\ \omega \leq p^{s-1}; \\ \langle f_j^*(x)^{p^s-p^{s-1}} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} M_j^*(x), pf_j^*(x)^{p^s-\omega} \rangle \text{ if } G(x) = 0 \\ \text{and } \omega > p^{s-1}; \\ \langle f_j^*(x)^{p^s-p^{s-1}} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} M_j^*(x) - px^{d_j\omega - d_j t - \deg G(x)} \\ f_j^*(x)^{p^s+t-\omega-p^{s-1}} G^*(x), pf_j^*(x)^{p^s-\omega} \rangle \text{ if } G(x) \neq 0, p^s - p^{s-1} + t - \omega > 0 \\ \text{and } \omega > p^{s-1}; \\ \langle f_j^*(x)^{p^s-\omega} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}-\omega} M_j^*(x) - px^{d_j\omega - d_j t - \deg G(x)} \\ f_j^*(x)^{p^s+t-2\omega} G^*(x) \rangle \text{ if } G(x) \neq 0, p^s - p^{s-1} + t - \omega > 0 \text{ and } \omega \leq p^{s-1}; \\ \langle f_j^*(x)^{p^s-\omega} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}-\omega} M_j^*(x) - px^{d_j\omega - d_j t - \deg G(x)} \\ f_j^*(x)^{p^s+t-2\omega} G^*(x) \rangle \text{ if } G(x) \neq 0, p^s - p^{s-1} + t - \omega < 0 \text{ and } p^s - 2\omega + t \geq 0; \\ \langle f_j^*(x)^{\omega-t} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}+\omega-t-p^s} M_j^*(x) \\ -px^{d_j\omega - d_j t - \deg G(x)} G^*(x), pf_j^*(x)^{p^s-\omega} \rangle \text{ if } G(x) \neq 0, p^s - p^{s-1} + t - \omega < 0 \\ \text{and } p^s - 2\omega + t < 0; \\ \langle f_j^*(x)^{p^s-\omega} \rangle \text{ if } G(x) \neq 0, \omega = p^s - p^{s-1} + t \text{ with either } A_G(x) = 0 \text{ or } A_G(x) \\ \neq 0, \rho \geq p^s - p^{s-1}; \\ \langle f_j^*(x)^{p^s-\omega} + px^{d_j p^s - d_j p^{s-1} - d_j\rho - \deg A_G(x)} f_j^*(x)^{p^{s-1}-\omega+\rho} A_G^*(x) \rangle \text{ if } G(x) \neq 0, \\ t = \omega - p^s + p^{s-1}, A_G(x) \neq 0 \text{ and } \omega - p^{s-1} \leq \rho < p^s - p^{s-1}; \\ \langle f_j^*(x)^{p^s-p^{s-1}-\rho} + px^{d_j p^s - d_j p^{s-1} - d_j\rho - \deg A_G(x)} A_G^*(x), pf_j^*(x)^{p^s-\omega} \rangle \text{ if } G(x) \\ \neq 0, t = \omega - p^s + p^{s-1}, A_G(x) \neq 0 \text{ and } \rho < \omega - p^{s-1}. \end{cases}$$

(e) Let $\mathcal{I} = \langle f_j(x)^{\omega} + pf_j(x)^t G(x), pf_j(x)^{\mu} \rangle$ be of Type IV. Let us write $p(M_j(x) - G(x)) = pf_j(x)^{\rho} A_G(x)$, where $0 \leq \rho < p^s$ and $A_G(x)$ is either 0 or a unit in $\mathcal{K}_j$. When $G(x) \neq 0$, $t = \omega - p^s + p^{s-1}$ with either $A_G(x) = 0$ or $A_G(x) \neq 0$ and $\rho \geq p^s - p^{s-1}$, we have $\mathcal{I} = \langle f_j(x)^{\omega} + pf_j(x)^{\omega - p^s + p^{s-1}} M_j(x), pf_j(x)^{\mu} \rangle$. Furthermore, we have

$$\mathcal{I}^{\perp} = \begin{cases} \langle f_j^*(x)^{p^s-\mu}, pf_j^*(x)^{p^s-\omega}\rangle \text{ if } G(x) = 0 \text{ and } p^s - p^{s-1} - \omega + \mu \leq 0; \\ \langle f_j^*(x)^{p^s-\mu} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}-\mu} M_j^*(x), pf_j^*(x)^{p^s-\omega}\rangle \text{ if } G(x) \\ = 0 \text{ and } p^s - p^{s-1} - \omega + \mu > 0; \\ \langle f_j^*(x)^{p^s-\mu} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}-\mu} M_j^*(x) - px^{d_j\omega - d_j t - \deg G(x)} \\ f_j^*(x)^{p^s-\mu+t-\omega} G^*(x), pf_j^*(x)^{p^s-\omega}\rangle \text{ if } G(x) \neq 0 \text{ and } p^s - p^{s-1} + t - \omega \neq 0; \\ \langle f_j^*(x)^{p^s-\mu}, pf_j^*(x)^{p^s-\omega}\rangle \text{ if } G(x) \neq 0, t = \omega - p^s + p^{s-1} \text{ with either } A_G(x) \\ = 0 \text{ or } A_G(x) \neq 0, \rho \geq p^s - p^{s-1}; \\ \langle f_j^*(x)^{p^s-\mu} + px^{d_j p^s - d_j p^{s-1} - d_j\rho - \deg A_G(x)} f_j^*(x)^{p^{s-1}-\mu+\rho} A_G^*(x), pf_j^*(x)^{p^s-\omega}\rangle \\ \text{if } G(x) \neq 0, t = \omega - p^s + p^{s-1}, A_G(x) \neq 0 \text{ and } \rho < p^s - p^{s-1}. \end{cases}$$

Proof. It is easy to see that $\mathcal{I}^{\perp} = \mathcal{K}_j$ when $\mathcal{I} = \{0\}$ and that $\mathcal{I}^{\perp} = \{0\}$ when $\mathcal{I} = \mathcal{K}_j$. As the proofs of parts (d) and (e) are almost similar, we will prove parts (c) and (e) only. For this, we see, by Lemma 3.2.2(c), that the nilpotency index $\mathfrak{N}$ of $f_j(x)$ in $\mathcal{K}_j$ is given by $\mathfrak{N} = 2p^s - p^{s-1}$. We also note that $f_j(x)^{p^s} = -pf_j(x)^{p^{s-1}} M_j(x)$, $pf_j(x)^{p^s} = 0$ and $pf_j(x)^{p^s-1} \neq 0$ in $\mathcal{K}_j$.

To prove (c), suppose that $\mathcal{I} = \langle pf_j(x)^{\tau}\rangle$ is of Type II. Here we see that ann$(\mathcal{I}) = \langle f_j(x)^{p^s-\tau}, p\rangle$. From this and by applying Lemma 3.2.4, we obtain $\mathcal{I}^{\perp} = \langle f_j^*(x)^{p^s-\tau}, p\rangle$.

To prove (e), let $\mathcal{I} = \langle f_j(x)^{\omega} + pf_j(x)^t G(x), pf_j(x)^{\mu}\rangle$ be of Type IV.

When $G(x) = 0$, we have $\mathcal{I} = \langle f_j(x)^{\omega}, pf_j(x)^{\mu}\rangle$. As ann$(\mathcal{I})$ is an ideal of $\mathcal{K}_j$, by Theorem 3.2.2, we can write ann$(\mathcal{I}) = \langle f_j(x)^a + pf_j(x)^b H(x), pf_j(x)^c\rangle$, where $H(x)$ is either 0 or a unit in $\mathcal{K}_j$. This implies that

$$pf_j(x)^{a+\mu} = 0, pf_j(x)^{c+\omega} = 0 \text{ and } f_j(x)^{a+\omega} + pf_j(x)^{b+\omega} H(x) = 0. \tag{3.2.5}$$

By Theorem 3.2.2 and Proposition 3.2.3, we see that $\mu < \kappa$ and $\kappa = \min\{\omega, p^{s-1}\}$, which implies that $\mu < \omega$ and $\mu < p^{s-1}$. Using this and by (3.2.5), we get $a \geq p^s - \mu$, $c \geq p^s - \omega$ and $-pf_j(x)^{a+\omega-p^s+p^{s-1}} M_j(x) + pf_j(x)^{b+\omega} H(x) = 0$, which holds only if $a \geq \max\{p^s - \mu, p^s - p^{s-1}\} = p^s - \mu$, $b = a - p^s + p^{s-1}$ and $pH(x) = pM_j(x)$. This implies that ann$(\mathcal{I}) = \langle f_j(x)^{p^s-\mu}, pf_j(x)^{p^s-\omega}\rangle$ when $p^s - p^{s-1} - \omega + \mu \leq 0$, while ann$(\mathcal{I}) =$

$\langle f_j(x)^{p^s-\mu} + pf_j(x)^{p^{s-1}-\mu}M_j(x), pf_j(x)^{p^s-\omega}\rangle$ when $p^s - p^{s-1} - \omega + \mu > 0$. From this and by applying Lemma 3.2.4, we get $\mathcal{I}^\perp = \langle f_j^*(x)^{p^s-\mu}, pf_j^*(x)^{p^s-\omega}\rangle$ when $p^s - p^{s-1} - \omega + \mu \leq 0$, while $\mathcal{I}^\perp = \langle f_j^*(x)^{p^s-\mu} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}-\mu} M_j^*(x), pf_j^*(x)^{p^s-\omega}\rangle$ when $p^s - p^{s-1} - \omega + \mu > 0$.

Next assume that $G(x)$ is a unit in $\mathcal{K}_j$. As ann$(\mathcal{I})$ is an ideal of $\mathcal{K}_j$, by Theorem 3.2.2, we can write ann$(\mathcal{I}) = \langle f_j(x)^a + pf_j(x)^b H(x), pf_j(x)^c\rangle$, where $H(x)$ is either 0 or a unit in $\mathcal{K}_j$. This implies that

$$pf_j(x)^{a+\mu} = 0, pf_j(x)^{c+\omega} = 0 \text{ and } f_j(x)^{a+\omega} + p(f_j(x)^{a+t}G(x) + f_j(x)^{b+\omega}H(x)) = 0. \tag{3.2.6}$$

By (3.2.6), we get $a \geq p^s - \mu$, $c \geq p^s - \omega$ and

$$p(-f_j(x)^{a+\omega-p^s+p^{s-1}}M_j(x) + f_j(x)^{a+t}G(x) + f_j(x)^{b+\omega}H(x)) = 0. \tag{3.2.7}$$

Here we consider the following two cases separately: $p^s - p^{s-1} + t - \omega \neq 0$ and $p^s - p^{s-1} + t - \omega = 0$.

When $p^s - p^{s-1} + t - \omega \neq 0$, by Proposition 3.2.3, we note that $p^s - \omega + t - \mu \geq 0$ and $\mu \leq p^{s-1}$. In this case, we see that (3.2.7) holds for $a = p^s - \mu$, which implies that ann$(\mathcal{I}) = \langle f_j(x)^{p^s-\mu} + pf_j(x)^{p^{s-1}-\mu}M_j(x) - pf_j(x)^{p^s-\mu+t-\omega}G(x), pf_j(x)^{p^s-\omega}\rangle$. From this and using Lemma 3.2.4, we get

$$\begin{aligned}\mathcal{I}^\perp = \langle & f_j^*(x)^{p^s-\mu} + px^{d_j p^s - d_j p^{s-1} - \deg M_j(x)} f_j^*(x)^{p^{s-1}-\mu} M_j^*(x) \\ & - px^{d_j\omega - d_j t - \deg G(x)} f_j^*(x)^{p^s-\mu+t-\omega} G^*(x), pf_j^*(x)^{p^s-\omega}\rangle.\end{aligned}$$

Next suppose that $p^s - p^{s-1} + t - \omega = 0$. In this case, (3.2.7) can be rewritten as

$$pf_j(x)^{b+\omega}H(x) = pf_j(x)^{a+\omega-p^s+p^{s-1}}(M_j(x) - G(x)) = pf_j(x)^{a+\omega-p^s+p^{s-1}+\rho}A_G(x). \tag{3.2.8}$$

When $A_G(x) = 0$, we see that (3.2.8) holds for all $b \geq p^s - \omega$, which implies that ann$(\mathcal{I}) = \langle f_j(x)^{p^s-\mu}, pf_j(x)^{p^s-\omega}\rangle$. From this and using Lemma 3.2.4, we obtain $\mathcal{I}^\perp = \langle f_j^*(x)^{p^s-\mu}, pf_j^*(x)^{p^s-\omega}\rangle$.

Next let $A_G(x)$ be a unit in $\mathcal{K}_j$. Here by Proposition 3.2.3, we see that $p^{s-1} + \rho \geq \mu$. When $\rho \geq p^s - p^{s-1}$, we see that $pf_j(x)^{\omega+\rho-p^s+p^{s-1}} \in \mathcal{I}$, which implies that

$$\begin{aligned}\mathcal{I} &= \langle f_j(x)^\omega + pf_j(x)^{\omega-p^s+p^{s-1}} M_j(x) - pf_j(x)^{\omega+\rho-p^s+p^{s-1}} A_G(x), pf_j(x)^\mu \rangle \\ &= \langle f_j(x)^\omega + pf_j(x)^{\omega-p^s+p^{s-1}} M_j(x), pf_j(x)^\mu \rangle.\end{aligned}$$

Now when $\rho \geq p^s - p^{s-1}$, we see that (3.2.8) holds for all $b \geq p^s - \omega$, which implies that ann$(\mathcal{I}) = \langle f_j(x)^{p^s-\mu}, pf_j(x)^{p^s-\omega} \rangle$. From this and using Lemma 3.2.4, we get $\mathcal{I}^\perp = \langle f_j^*(x)^{p^s-\mu}, pf_j^*(x)^{p^s-\omega} \rangle$. Moreover, when $\rho < p^s - p^{s-1}$, we observe that (3.2.8) holds for all $a \geq p^s - \mu$, $b = a + p^{s-1} - p^s + \rho$ and $H(x) = A_G(x)$. This implies that ann$(\mathcal{I}) = \langle f_j(x)^{p^s-\mu} + pf_j(x)^{p^{s-1}-\mu+\rho} A_G(x), pf_j(x)^{p^s-\omega} \rangle$, which, by Lemma 3.2.4, further implies that

$$\mathcal{I}^\perp = \langle f_j^*(x)^{p^s-\mu} + px^{d_j p^s - d_j p^{s-1} - d_j \rho - \deg A_G(x)} f_j^*(x)^{p^{s-1}-\mu+\rho} A_G^*(x), pf_j^*(x)^{p^s-\omega} \rangle.$$

This completes the proof of the theorem. □

As a consequence of the above results, we obtain some isodual α-constacyclic codes of length np^s over GR(p^2, m).

Corollary 3.2.2. Suppose that $\beta = 0$. Let $\alpha = \alpha_0^{p^s} \in \mathcal{T} \setminus \{0\}$, where $\alpha_0 \in \mathcal{T}$ is such that $x^n - \alpha_0$ is basic irreducible over GR(p^2, m). Following the same notations as in Theorem 3.2.2, we have the following:

(a) The code $\langle p \rangle$ is the only isodual α-constacyclic code of Type II over GR(p^2, m).

(b) When $p = 2$, the codes $\langle (x^n - \alpha_0)^{2^{s-1}} \rangle$ and $\langle (x^n - \alpha_0)^{2^{s-1}} + 2(x^n - \alpha_0)^t G(x) \rangle$ are isodual α-constacyclic codes of Type III over GR$(4, m)$ for each $G(x) \neq 0$ and for each integer $t \geq 1$.

(c) The α-constacyclic codes $\langle (x^n - \alpha_0)^\omega, p(x^n - \alpha_0)^{p^s-\omega} \rangle$, $\frac{2p^s-p^{s-1}}{2} \leq \omega < p^s$, are isodual codes of Type IV over GR(p^2, m).

Proof. Let $\mathcal{C}$ be an α-constacyclic code of length np^s over GR(p^2, m). For $\mathcal{C}$ to be isodual, we must have $|\mathcal{C}| = |\mathcal{C}^\perp|$.

(a) Let $\mathcal{C}$ be of Type II, i.e., $\mathcal{C} = \langle p(x^n - \alpha_0)^\tau \rangle$ for some τ, $0 \leq \tau < p^s$. By Theorems 3.2.3 and 3.2.4, we observe that $\mathcal{C}^\perp = \langle (x^n - \alpha_0^{-1})^{p^s-\tau}, p \rangle$, $|\mathcal{C}| = p^{mn(p^s-\tau)}$ and $|\mathcal{C}^\perp| = p^{mn(p^s+\tau)}$. Now if the code $\mathcal{C} = \langle p(x^n - \alpha_0)^\tau \rangle$ is isodual, then we must have $|\mathcal{C}| = |\mathcal{C}^\perp|$, which gives $\tau = 0$. On the other hand, when $\tau = 0$, we see that the codes $\mathcal{C} = \langle p \rangle$ and $\mathcal{C}^\perp = \langle p \rangle$ are GR(p^2, m)-linearly equivalent. From this, it follows that $\langle p \rangle$ is the only isodual α-constacyclic code of Type II over GR(p^2, m).

(b) If $\mathcal{C}$ is of Type III, then $\mathcal{C} = \langle (x^n - \alpha_0)^\omega + p(x^n - \alpha_0)^t G(x) \rangle$, where $0 < \omega < p^s$, $G(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha,0}$ and $0 \leq t < \omega$ if $G(x) \neq 0$.

When $G(x) = 0$ and $\omega \leq p^{s-1}$, by Theorems 3.2.3 and 3.2.4, we have $|\mathcal{C}| = p^{2mn(p^s-\omega)}$, $\mathcal{C}^\perp = \langle (-\alpha_0)^{p^s-\omega}(x^n - \alpha_0^{-1})^{p^s-\omega} + px^{np^s-np^{s-1}-\deg M_j(x)}(-\alpha_0)^{p^{s-1}-\omega}(x^n - \alpha_0^{-1})^{p^{s-1}-\omega} M_j^*(x) \rangle$ and $|\mathcal{C}^\perp| = p^{2mn\omega}$. Now for the code $\mathcal{C}$ to be isodual, we must have $|\mathcal{C}| = |\mathcal{C}^\perp|$, which gives $p = 2$ and $\omega = 2^{s-1}$. Further, when $p = 2$ and $\omega = 2^{s-1}$, we note that $M_j(x) = a_1 \alpha_0^{2^{s-1}} \in$ GR$(4, m)$, which implies that $\mathcal{C}^\perp = \langle (-\alpha_0)^{2^{s-1}}(x^n - \alpha_0^{-1})^{2^{s-1}} + px^{n2^{s-1}} z a_1 \alpha_0^{2^{s-1}} \rangle$. It is easy to observe that $\mathcal{C}^\perp$ is GR$(4, m)$-linearly equivalent to the α-constacyclic code $\mathcal{D} = \langle (x^n - \alpha_0)^{2^{s-1}} + 2a_1 \alpha_0^{2^{s-1}} \rangle$ of length $n2^s$ over GR$(4, m)$. In view of this, we see that the codes $\mathcal{C}$ and $\mathcal{C}^\perp$ are GR$(4, m)$-linearly equivalent if and only if $\mathcal{C}$ and $\mathcal{D}$ are GR$(4, m)$-linearly equivalent. For $s = 1$, we see that $\mathcal{C} = \langle x^n - \alpha_0 \rangle$ and $\mathcal{D} = \langle x^n - \alpha_0 + 2a_1 \rangle$, which are trivially GR$(4, m)$-linearly equivalent. For $s \geq 2$, by Theorem 2.0.11, we note that $2 || \binom{2^{s-1}}{2^{s-2}}$ and that $\binom{2^{s-1}}{i} = 0$ for each i satisfying $1 \leq i \leq 2^{s-1} - 1$ and $i \neq 2^{s-2}$. From this, we get $\mathcal{C} = \langle x^{n2^{s-1}} + \binom{2^{s-1}}{2^{s-2}} x^{n2^{s-2}} (-\alpha_0)^{2^{s-2}} + \alpha_0^{2^{s-1}} \rangle$ and $\mathcal{D} = \langle x^{n2^{s-1}} + \binom{2^{s-1}}{2^{s-2}} x^{n2^{s-2}} (-\alpha_0)^{2^{s-2}} + \alpha_0^{2^{s-1}}(1+2a_1) \rangle$. It is easy to observe that the codes $\mathcal{C}(\subseteq \mathcal{R}_{\alpha,0})$ and $\mathcal{D}(\subseteq \mathcal{R}_{\alpha,0})$ are GR$(4, m)$-linearly equivalent.

Next when $G(x) \neq 0$, $p^s - p^{s-1} + t - \omega > 0$ and $\omega \leq p^{s-1}$, by Theorems 3.2.3 and 3.2.4, we have $|\mathcal{C}| = p^{2mn(p^s-\omega)}$,

$$\mathcal{C}^\perp = \langle (-\alpha_0)^{p^s-\omega}(x^n - \alpha_0^{-1})^{p^s-\omega} + px^{np^s-np^{s-1}-\deg M_j(x)} M_j^*(x)(-\alpha_0)^{p^{s-1}-\omega}$$
$$(x^n - \alpha_0^{-1})^{p^{s-1}-\omega} - px^{n\omega-nt-\deg G(x)}(-\alpha_0)^{p^s-2\omega+t}(x^n - \alpha_0^{-1})^{p^s-2\omega+t} G^*(x)\rangle$$

and $|\mathcal{C}^\perp| = p^{2mn\omega}$. Here for the code $\mathcal{C}$ to be isodual, we must have $|\mathcal{C}| = |\mathcal{C}^\perp|$, which gives $p = 2$ and $\omega = 2^{s-1}$. On the other hand, when $p = 2$ and $\omega = 2^{s-1}$, we see that $\mathcal{C}^\perp = \langle (-\alpha_0)^{2^{s-1}}(x^n - \alpha_0^{-1})^{2^{s-1}} - 2(-\alpha_0)^t x^{n2^{s-1}-nt-\deg G(x)}(x^n - \alpha_0^{-1})^t G^*(x) + 2a_1\alpha_0^{2^{s-1}} x^{n2^{s-1}}\rangle$, which is GR$(4, m)$-linearly equivalent to the α-constacyclic code $\mathcal{D}_1 = \langle (x^n - \alpha_0)^{2^{s-1}} - 2(x^n - \alpha_0)^t G(x) + 2a_1\alpha_0^{2^{s-1}}\rangle$ of length $n2^s$ over GR$(4, m)$. Further, one can easily observe that the codes $\mathcal{C}(\subseteq \mathcal{R}_{\alpha,0})$ and $\mathcal{D}_1(\subseteq \mathcal{R}_{\alpha,0})$ are GR$(4, m)$-linearly equivalent, which implies that the codes $\mathcal{C}(\subseteq \mathcal{R}_{\alpha,0})$ and $\mathcal{C}^\perp(\subseteq \widehat{\mathcal{R}_{\alpha,0}})$ are GR$(4, m)$-linearly equivalent.

When $p^s - p^{s-1} + t = \omega$ and $pM_j(x) = pG(x)$, by Theorems 3.2.3 and 3.2.4, we have $|\mathcal{C}| = p^{2mn(p^s-\omega)}$, $\mathcal{C}^\perp = \langle (x^n - \alpha_0^{-1})^{p^s-\omega}\rangle$ and $|\mathcal{C}^\perp| = p^{2mn\omega}$. Now for the code $\mathcal{C}$ to be isodual, we must have $p = 2$ and $\omega = 2^{s-1}$. On the other hand, when $p = 2$ and $\omega = 2^{s-1}$, it is easy to see that the codes $\mathcal{C}(\subseteq \mathcal{R}_{\alpha,0})$ and $\mathcal{C}^\perp(\subseteq \widehat{\mathcal{R}_{\alpha,0}})$ are GR$(4, m)$-linearly equivalent.

(c) If $\mathcal{C}$ is of Type IV, then $\mathcal{C} = \langle (x^n - \alpha_0)^\omega + p(x^n - \alpha_0)^t G(x), p(x^n - \alpha_0)^\mu\rangle$, where $0 < \mu < \omega < p^s$, $G(x)$ is either 0 or a unit in $\mathcal{R}_{\alpha,0}$ and $0 \leq t < \mu$ if $G(x) \neq 0$. Here by Theorems 3.2.3 and 3.2.4, we have $|\mathcal{C}| = p^{mn(2p^s-\omega-\mu)}$ and $|\mathcal{C}^\perp| = p^{mn(\omega+\mu)}$. Now if the code $\mathcal{C}$ is isodual, then $2p^s - \omega - \mu = \omega + \mu$, which gives $\mu = p^s - \omega$.

Now let $\mu = p^s - \omega$. Then we have $\mathcal{C} = \langle (x^n - \alpha_0)^\omega + p(x^n - \alpha_0)^t G(x), p(x^n - \alpha_0)^{p^s-\omega}\rangle$. When $G(x) = 0$ and $\omega \geq \frac{2p^s - p^{s-1}}{2}$, by Theorem 3.2.4, we see that $\mathcal{C}^\perp = \langle (x^n - \alpha_0^{-1})^\omega, p(x^n - \alpha_0^{-1})^{p^s-\omega}\rangle$, which is clearly GR$(p^2, m)$-linearly equivalent to the code $\mathcal{C}$.

This completes the proof of the theorem. □

3.3 Some examples

To illustrate our results, we determine all cyclic and negacyclic codes of length 10 over the Galois ring GR$(4, 3)$ as follows:

Example 3.3.1. In order to write down all negacyclic codes of length 10 over GR$(4, 3)$, we observe that the factorization of $x^5 - 1$ into monic pairwise coprime basic irreducible polynomials over GR$(4, 3)$ is given by $x^5-1 = (x+3)(x^4+x^3+x^2+x+1)$. Further, working as in the proof of Lemma 3.2.1, we see that $x^{10} + 1 = \{(x + 3)^2 + 2(x^5 - 2)\}\{(x^4 + x^3 + x^2 + x + 1)^2 + 2(x^5 - 2)(3x^6 + 2x^4 + x^2 + 2x)\}$ is a factorization of $x^{10} + 1$ into coprime polynomials over GR$(4, 3)$. Now by applying the Chinese Remainder Theorem, we get $\mathcal{R}_{1,1} = \text{GR}(4, 3)[x]/\langle x^{10} + 1\rangle \simeq \mathcal{K}_1 \oplus \mathcal{K}_2$, where $\mathcal{K}_1 = \text{GR}(4, 3)[x]/\langle (x + 3)^2 + 2(x^5 - 2)\rangle$ and $\mathcal{K}_2 = \text{GR}(4, 3)[x]/\langle (x^4 + x^3 + x^2 + x + 1)^2 + 2(x^5 - 2)(3x^6 + 2x^4 + x^2 + 2x)\rangle$. By Theorem 3.2.1, we note that all the ideals of $\mathcal{K}_1$ are given by $\langle (x + 3)^i\rangle$, $0 \leq i \leq 4$ and all the ideals of $\mathcal{K}_2$ are given by $\langle (x^4 + x^3 + x^2 + x + 1)^\ell\rangle$, $0 \leq \ell \leq 4$. From this and by applying Proposition 3.2.1, we see that all negacyclic codes of length 10 over GR$(4, 3)$ are given by $\langle (x + 3)^i\rangle \oplus \langle (x^4 + x^3 + x^2 + x + 1)^\ell\rangle$, where $0 \leq i, \ell \leq 4$. By Corollary 3.2.1, we see that the code $\langle 2\rangle$ is a self-dual negacyclic code of length 10 over GR$(4, 3)$.

Example 3.3.2. Next we proceed to write down all cyclic codes of length 10 over GR$(4, 3)$, which are ideals of the ring $\mathcal{R}_{1,0} = \text{GR}(4, 3)[x]/\langle x^{10} - 1\rangle$. To do this, working as in the proof of Lemma 3.2.1, we see that $x^{10}-1 = \{(x+3)^2+2(x^5-1)\}\{(x^4+x^3+x^2+x+1)^2+2(x^5-1)(3x^6+2x^4+x^2+2x)\}$ is a factorization of $x^{10} - 1$ into coprime polynomials over GR$(4, 3)$. Now by applying the Chinese Remainder Theorem, we obtain $\mathcal{R}_{1,0} \simeq \mathcal{K}_1 \oplus \mathcal{K}_2$, where $\mathcal{K}_1 = \text{GR}(4, 3)[x]/\langle (x + 3)^2 + 2(x^5 - 1)\rangle$ and $\mathcal{K}_2 = \text{GR}(4, 3)[x]/\langle (x^4 + x^3 + x^2 + x+1)^2 + 2(x^5 - 1)(3x^6 + 2x^4 + x^2 + 2x)\rangle$. Further, by applying Proposition 3.2.1, all cyclic codes of length 10 over GR$(4, 3)$ are given by $\mathcal{I}_1 \oplus \mathcal{I}_2$, where $\mathcal{I}_1$ is an ideal of $\mathcal{K}_1$ and $\mathcal{I}_2$ is an ideal of $\mathcal{K}_2$.

Trivial ideals	Principal ideals	Non-principal ideals
$\{0\}$, $\mathcal{K}_1$	$\langle 2\rangle$, $\langle x + 3\rangle$, $\langle 2x + 2\rangle$, $\langle x + 1\rangle$, $\langle x + 3 + 2\delta\rangle$, $\langle x + 3 + 2\delta^2\rangle$	$\langle x + 3, 2\rangle$

TABLE 3.1: Ideals of $\mathcal{K}_1$

Trivial ideals	Principal ideals	Non-principal ideals
$\{0\}, \mathcal{K}_2$	$\langle 2\rangle, \langle x^4+x^3+x^2+x+1\rangle,$ $\langle 2x^4+2x^3+2x^2+2x+2\rangle$ $\langle x^4+x^3+x^2+x+1+2G(x)\rangle$	$\langle x^4+x^3+x^2+x+1, 2\rangle$

TABLE 3.2: [a]Ideals of $\mathcal{K}_2$

$\langle 2\rangle$	$\langle 2\rangle \oplus \langle x^4+x^3+x^2+x+1+2G(x)\rangle$
$\langle x+3\rangle \oplus \langle 2\rangle$	$\langle x+3\rangle \oplus \langle x^4+x^3+x^2+x+1+2G(x)\rangle$
$\langle x+1\rangle \oplus \langle 2\rangle$	$\langle x+1\rangle \oplus \langle x^4+x^3+x^2+x+1+2G(x)\rangle$
$\langle x+3+2\delta\rangle \oplus \langle 2\rangle$	$\langle x+3+2\delta\rangle \oplus \langle x^4+x^3+x^2+x+1+2G(x)\rangle$
$\langle x+3+2\delta^2\rangle \oplus \langle 2\rangle$	$\langle x+3+2\delta^2\rangle \oplus \langle x^4+x^3+x^2+x+1+2G(x)\rangle$
$\langle 2\rangle \oplus \langle x^4+x^3+x^2+x+1\rangle$	$\langle x+3+2\delta^2\rangle \oplus \langle x^4+x^3+x^2+x+1\rangle$
$\langle x+1\rangle \oplus \langle x^4+x^3+x^2+x+1\rangle$	$\langle x+3+2\delta\rangle \oplus \langle x^4+x^3+x^2+x+1\rangle$
$\langle x+3\rangle \oplus \langle x^4+x^3+x^2+x+1\rangle$	

TABLE 3.3: [a]Some self-dual cyclic codes of length 10 over GR$(4,3)$

[a]Here $G(x)$ runs over $\mathcal{P}_4(\mathcal{T}) \setminus \{0\}$.

If $\mathcal{T} = \{0, 1, \delta, \delta^2\}$ is the Teichmüller set of GR$(4,3)$, then by applying Theorem 3.2.2, we list all the ideals of $\mathcal{K}_1$ and $\mathcal{K}_2$ in Tables 3.1 and 3.2, respectively. In Table 3.3, we list some self-dual cyclic codes of length 10 over GR$(4,3)$ by applying Corollary 3.2.2.

Chapter 4

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

4.1 Introduction

In this chapter, we shall determine all repeated-root constacyclic codes of arbitrary lengths over the chain ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ and their dual codes. We shall also determine the number of codewords in each code. Besides this, we shall list some isodual codes within the class of constacyclic codes. We shall also determine ranks, Hamming distances, Rosenbloom-Tsfasman (RT) distances and Rosenbloom-Tsfasman (RT) weight distributions of some classes of repeated-root constacyclic codes over the chain ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. Using these results, we shall identify some MDS Hamming and MDS RT codes within this class of codes.

For this, throughout this chapter, 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 $\mathscr{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$ be the finite commutative chain ring (i.e., quasi-Galois ring) with unity. Let λ be a unit in $\mathscr{R}$. One can easily observe that the unit $\lambda \in \mathscr{R}$ can be uniquely expressed as $\lambda = \alpha + u\beta + u^2\delta$, where $\alpha, \beta, \delta \in \mathbb{F}_{p^m}$ and $\alpha \neq 0$. Further, as $\alpha(\neq 0) \in \mathbb{F}_{p^m}$, there exists $\alpha_0 \in \mathbb{F}_{p^m}$ satisfying $\alpha = \alpha_0^{p^s}$, so that we have $\lambda = \alpha_0^{p^s} + u\beta + u^2\delta$.

This chapter is organized as follows: In Section 4.2, we determine all λ-constacyclic codes of length np^s over $\mathscr{R}$ and their dual codes. We also list some isodual λ-constacyclic codes of length np^s over $\mathscr{R}$ when the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. In Section 4.3, we obtain ranks, Hamming distances, Rosenbloom-Tsfasman (RT) distances and Rosenbloom-Tsfasman (RT) weight distributions of all λ-constacyclic codes of length np^s over $\mathscr{R}$ and

identify all MDS λ-constacyclic codes of length np^s over $\mathscr{R}$ with respect to the Hamming and RT metrics when the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. In Section 4.4, we obtain Hamming distances of all λ-constacyclic codes of length $2p^s$ over $\mathscr{R}$ and identified all MDS codes within this class of constacyclic codes with respect to the Hamming metric.

4.2 Algebraic structures of constacyclic codes of length np^s over $\mathscr{R}$ and their dual codes

In this section, we will provide a method to construct all λ-constacyclic codes of length np^s over $\mathscr{R}$ for the purpose of error-detection and error-correction. We will also determine their dual codes and the number of codewords in each code. Besides this, we will list some isodual constacyclic codes of length np^s over $\mathscr{R}$.

To do this, we recall that a λ-constacyclic code of length np^s over $\mathscr{R}$ is an ideal of the quotient ring $\mathscr{R}_\lambda = \mathscr{R}[x]/\langle x^{np^s} - \lambda\rangle$. The unit λ can be uniquely expressed as $\lambda = \alpha + u\beta + u^2\delta$, where $\alpha, \beta, \delta \in \mathbb{F}_{p^m}$ and α is non-zero. Furthermore, as $\alpha(\neq 0) \in \mathbb{F}_{p^m}$, there exists $\alpha_0 \in \mathbb{F}_{p^m}$ satisfying $\alpha = \alpha_0^{p^s}$, which implies that $\lambda = \alpha_0^{p^s} + u\beta + u^2\delta$. 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 $\mathscr{R}[x]$.

Lemma 4.2.1. 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

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

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

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

Proof. To prove the result, we see that

$$x^{np^s} - \lambda = (x^n - \alpha_0)^{p^s} - u\beta - u^2\delta = f_1(x)^{p^s} f_2(x)^{p^s} \cdots f_r(x)^{p^s} - u\beta - u^2\delta. \quad (4.2.1)$$

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

$$v_j(x)f_j(x)^{p^s} + w_j(x)\prod_{i=j+1}^{r} f_i(x)^{p^s} = 1. \quad (4.2.2)$$

Now by (4.2.1) and (4.2.2), we obtain

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

Furthermore, using (4.2.2) again, we get

$$\prod_{i=2}^{r} f_i(x)^{p^s} - u\beta v_1(x) - u^2 v_1(x)\{\delta + \beta^2 v_1(x)w_1(x)\}$$

$$= \{f_2(x)^{p^s} - u\beta v_1(x)w_2(x) - u^2 v_1(x)w_2(x)\big(\delta + \beta^2 v_1(x)w_1(x) + \beta^2 v_1(x)v_2(x)w_2(x)\big)\}$$
$$\times\Big\{\prod_{i=3}^{r} f_i(x)^{p^s} - u\beta v_1(x)v_2(x) - u^2 v_1(x)v_2(x)\big(\delta + \beta^2 v_1(x)w_1(x) + \beta^2 v_1(x)v_2(x)w_2(x)\big)\Big\}.$$

Proceeding like this, we obtain $x^{np^s} - \lambda = \prod_{j=1}^{r}\Big(f_j(x)^{p^s} + ug_j(x) + u^2h_j(x)\Big)$ with

- $g_1(x) = -\beta$ and $h_1(x) = -\delta$ when $r = 1$; and
- $g_j(x) = -\beta w_j(x)\prod_{i=1}^{j-1} v_i(x)$, $\quad g_r(x) = -\beta\prod_{i=1}^{r-1} v_i(x)$,

  $h_j(x) = -w_j(x)\prod_{i=1}^{j-1} v_i(x)\Big(\delta + \beta^2\sum_{\ell=1}^{j} v_1(x)v_2(x)v_3(x)\cdots v_\ell(x)w_\ell(x)\Big)$ and

$$h_r(x) = -\prod_{i=1}^{r-1} v_i(x)\Big(\delta + \beta^2 \sum_{\ell=1}^{r-1} v_1(x)v_2(x)v_3(x)\cdots v_\ell(x)w_\ell(x)\Big)$$

for $1 \le j \le r-1$ when $r \ge 2$.

From this, the desired result follows. □

From now on, we define $\ell_j(x) = f_j(x)^{p^s} + ug_j(x) + u^2h_j(x)$ for $1 \le j \le r$. Then we have $x^{np^s} - \lambda = \prod_{j=1}^{r} \ell_j(x)$. Further, let deg $f_j(x) = d_j$ for each j. By Lemma 4.2.1, we see that $\ell_1(x), \ell_2(x), \cdots, \ell_r(x)$ are pairwise coprime in $\mathscr{R}[x]$. This, by Chinese Remainder Theorem, implies that

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

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

Proposition 4.2.1. (a) Let $\mathscr{C}$ be a λ-constacyclic code of length np^s over $\mathscr{R}$, i.e., an ideal of the ring $\mathscr{R}_\lambda$. Then we have

$$\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2 \oplus \cdots \oplus \mathscr{C}_r,$$

where $\mathscr{C}_j$ is an ideal of $\mathscr{K}_j$ for $1 \le j \le r$.

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

$$|I| = |I_1||I_2|\cdots|I_r|.$$

Proof. Proof is trivial. □

Next if $\mathscr{C}$ is a λ-constacyclic code of length np^s over $\mathscr{R}$, then its dual code $\mathscr{C}^\perp$ is a λ^{-1}-constacyclic code of length np^s over $\mathscr{R}$. This implies that $\mathscr{C}^\perp$ is an ideal of the quotient ring $\mathscr{R}_{\lambda^{-1}} = \mathscr{R}[x]/\langle x^{np^s} - \lambda^{-1}\rangle$. In order to determine $\mathscr{C}^\perp$ more explicitly, we observe that $x^{np^s} - \lambda^{-1} = -\lambda^{-1}\ell_1^*(x)\ell_2^*(x)\cdots\ell_r^*(x)$. By applying the Chinese Remainder Theorem again, we get

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

where $\widehat{\mathscr{K}_j} = \mathscr{R}[x]/\langle \ell_j^*(x)\rangle$ for $1 \leq j \leq r$. Then we have the following:

Proposition 4.2.2. Let $\mathscr{C}$ be a λ-constacyclic code of length np^s over $\mathscr{R}$, i.e., an ideal of the ring $\mathscr{R}_\lambda$. If $\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2 \oplus \cdots \oplus \mathscr{C}_r$ with $\mathscr{C}_j$ an ideal of $\mathscr{K}_j$ for each j, then the dual code $\mathscr{C}^\perp$ of $\mathscr{C}$ is given by $\mathscr{C}^\perp = \mathscr{C}_1^\perp \oplus \mathscr{C}_2^\perp \oplus \cdots \oplus \mathscr{C}_r^\perp$, where $\mathscr{C}_j^\perp = \{a_j(x) \in \widehat{\mathscr{K}_j} : a_j(x)c_j^*(x) = 0 \text{ in } \widehat{\mathscr{K}_j} \text{ for all } c_j(x) \in \mathscr{C}_j\}$ is the orthogonal complement of $\mathscr{C}_j$ for each j. Furthermore, $\mathscr{C}_j^\perp$ is an ideal of $\widehat{\mathscr{K}_j} = \mathscr{R}[x]/\langle \ell_j^*(x)\rangle$ for each j.

Proof. Its proof is straightforward. □

In view of Propositions 4.2.1 and 4.2.2, we see that to determine all λ-constacyclic codes of length np^s over $\mathscr{R}$, their sizes and their dual codes, we need to determine all ideals of the ring $\mathscr{K}_j$, their cardinalities and their orthogonal complements in $\widehat{\mathscr{K}_j}$ for $1 \leq j \leq r$. To do so, throughout this chapter, let $1 \leq j \leq r$ be a fixed integer. From now on, we shall represent elements of the rings $\mathscr{K}_j$ and $\widehat{\mathscr{K}_j}$ (resp. $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$) by their representatives in $\mathscr{R}[x]$ (resp. $\mathbb{F}_{p^m}[x]$) of degree less than $d_j p^s$, and we shall perform their addition and multiplication modulo $\ell_j(x)$ and $\ell_j^*(x)$ (resp. $f_j(x)^{p^s}$), respectively. To determine all ideals of the ring $\mathscr{K}_j$, we make the following observation.

Lemma 4.2.2. Let $1 \leq j \leq r$ be fixed. In the ring $\mathscr{K}_j$, 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 $\mathscr{K}_j$. As a consequence, any non-zero polynomial in $\mathbb{F}_{p^m}[x]$ of degree less than d_j is a unit in $\mathscr{K}_j$.

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

As a consequence, $f_j(x)$ is a nilpotent element of $\mathscr{K}_j$. 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 $\delta \neq 0$, while the nilpotency index of $f_j(x)$ is p^s when $\beta = \delta = 0$.

Proof. (a) As $f_j(x)$ is irreducible over $\mathbb{F}_{p^m}$ and $\gcd(g(x), f_j(x)) = 1$, we have $\gcd(g(x), f_j(x)^{p^s}) = 1$ in $\mathbb{F}_{p^m}[x]$. By Euclidean algorithm, there exist polynomials $a(x), b(x) \in \mathbb{F}_{p^m}[x]$ such that $a(x)g(x) + b(x)f_j(x)^{p^s} = 1$. This implies that $a(x)g(x) + b(x)(f_j(x)^{p^s} + ug_j(x) +$

$u^2h_j(x)) = 1 + ub(x)(g_j(x) + uh_j(x))$. From this, we get $a(x)g(x) = 1 + ub(x)(g_j(x) + uh_j(x))$ in $\mathscr{K}_j$. As $u^3 = 0$ in $\mathscr{K}_j$, we see that $1 + ub(x)(g_j(x) + uh_j(x))$ is a unit in $\mathscr{K}_j$, which implies that $g(x)$ is a unit in $\mathscr{K}_j$.

(b) It follows immediately from Lemma 4.2.1 and part (a). □

Next for a positive integer k, let us recall that $\mathcal{P}_k(\mathbb{F}_{p^m}) = \{g(x) \in \mathbb{F}_{p^m}[x] : \text{ either } g(x) = 0 \text{ or } \deg g(x) < k\}$. Note that by repeatedly applying the division algorithm in $\mathscr{R}[x]$, every element $a(x) \in \mathscr{K}_j$ can be uniquely expressed as $a(x) = \sum_{i=0}^{p^s-1} A_i(x)f_j(x)^i$, where $A_i(x) \in \mathcal{P}_{d_j}(\mathscr{R})$ for $0 \le i \le p^s - 1$. Further, each $A_i(x) \in \mathcal{P}_{d_j}(\mathscr{R})$ can be uniquely written as $A_i(x) = A_{i,0}(x) + uA_{i,1}(x) + u^2A_{i,2}(x)$,where $A_{i,0}(x), A_{i,1}(x), A_{i,2}(x) \in \mathcal{P}_{d_j}(\mathbb{F}_{p^m})$. That is, each element $a(x) \in \mathscr{K}_j$ can be uniquely expressed as

$$a(x) = \sum_{i=0}^{p^s-1} A_{i,0}(x)f_j(x)^i + u\sum_{i=0}^{p^s-1} A_{i,1}(x)f_j(x)^i + u^2\sum_{i=0}^{p^s-1} A_{i,2}(x)f_j(x)^i,$$

where $A_{i,0}(x), A_{i,1}(x), A_{i,2}(x) \in \mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for each i.

Now to determine cardinalities of all ideals of $\mathscr{K}_j$, we observe the following:

Lemma 4.2.3. Let $1 \le j \le r$ be a fixed integer. For an ideal $\mathscr{I}$ of $\mathscr{K}_j$, let us define $\text{Tor}_0(\mathscr{I}) = \{a_0(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle : a_0(x) + ua_1(x) + u^2a_2(x) \in \mathscr{I} \text{ for some } a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle\}$, $\text{Tor}_1(\mathscr{I}) = \{a_1(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle : ua_1(x) + u^2a_2(x) \in \mathscr{I} \text{ for some } a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle\}$ and $\text{Tor}_2(\mathscr{I}) = \{a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle : u^2a_2(x) \in \mathscr{I}\}$. Then $\text{Tor}_0(\mathscr{I})$, $\text{Tor}_1(\mathscr{I})$ and $\text{Tor}_2(\mathscr{I})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. Moreover, we have

$$|\mathscr{I}| = |\text{Tor}_0(\mathscr{I})||\text{Tor}_1(\mathscr{I})||\text{Tor}_2(\mathscr{I})|.$$

Proof. One can easily observe that $\text{Tor}_0(\mathscr{I})$, $\text{Tor}_1(\mathscr{I})$ and $\text{Tor}_2(\mathscr{I})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. In order to prove the second part, we define a map

$$\phi : \mathscr{I} \to \text{Tor}_0(\mathscr{I})$$

as $\phi(a(x)) = a_0(x)$ for each $a(x) = a_0(x)+ua_1(x)+u^2a_2(x) \in \mathscr{I}$ with $a_0(x), a_1(x), a_2(x) \in$

$\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. We observe that ϕ is a surjective $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$-module homomorphism and its kernel is given by

$$K_{\mathscr{I}} = \{ua_1(x) + u^2a_2(x) \in \mathscr{I} : a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle\}.$$

This implies that

$$|\mathscr{I}| = |\text{Tor}_0(\mathscr{I})||K_{\mathscr{I}}|. \tag{4.2.3}$$

We further define a map

$$\psi : K_{\mathscr{I}} \to \text{Tor}_1(\mathscr{I})$$

as $\psi(ua_1(x) + u^2a_2(x)) = a_1(x)$ for each $ua_1(x) + u^2a_2(x) \in K_{\mathscr{I}}$, where $a_1(x), a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. We see that ψ is also a surjective $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$-module homomorphism with the kernel as ker $\psi = \{u^2a_2(x) \in K_{\mathscr{I}} : a_2(x) \in \mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle\}$. From this, it follows that

$$|K_{\mathscr{I}}| = |\text{Tor}_1(\mathscr{I})||\text{ker } \psi| = |\text{Tor}_1(\mathscr{I})||\text{Tor}_2(\mathscr{I})|,$$

which, by (4.2.3), implies that

$$|\mathscr{I}| = |\text{Tor}_0(\mathscr{I})||\text{Tor}_1(\mathscr{I})||\text{Tor}_2(\mathscr{I})|.$$

□

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

Lemma 4.2.4. Let $1 \leq j \leq r$ be a fixed integer. Let $\mathscr{I}$ be an ideal of the ring $\mathscr{K}_j$ with the orthogonal complement as $\mathscr{I}^\perp$. Then the following hold.

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

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

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

(d) For non-zero polynomials $f(x), g(x) \in \mathscr{K}_j$, 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

$$(f+g)^*(x) = \begin{cases} f^*(x) + x^{deg\, f(x)-deg\, g(x)}g^*(x) \text{ if } \deg f(x) > \deg g(x); \\ x^{\deg (f+g)(x)-\deg f(x)}(f^*(x) + g^*(x)) \text{ if } \deg f(x) = \deg g(x). \end{cases}$$

Proof. Its proof is straightforward. □

From the above lemma, we see that to determine $\mathscr{I}^{\perp}$, it is enough to determine ann$(\mathscr{I})$ for each ideal $\mathscr{I}$ of $\mathscr{K}_j$. Further, to write down all ideals of $\mathscr{K}_j$, we see, by Lemma 4.2.3, that if $\mathscr{I}$ is an ideal of $\mathscr{K}_j$, then $\text{Tor}_0(\mathscr{I})$, $\text{Tor}_1(\mathscr{I})$ and $\text{Tor}_2(\mathscr{I})$ 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 Theorem 2.0.5, 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 $\text{Tor}_0(\mathscr{I}) = \langle f_j(x)^a\rangle$, $\text{Tor}_1(\mathscr{I}) = \langle f_j(x)^b\rangle$ and $\text{Tor}_2(\mathscr{I}) = \langle f_j(x)^c\rangle$ 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 $\mathscr{R}$ can be determined by using the results derived in Cao [9] and by applying the ring isomorphism from $\mathscr{R}[x]/\langle x^{np^s} - 1 - u\alpha^{-1}\beta - u^2\alpha^{-1}\delta\rangle$ onto $\mathscr{R}[x]/\langle x^{np^s} - \alpha - u\beta - u^2\delta\rangle$, defined as $a(x) \mapsto a(\mu^{-1}x)$ for each $a(x) \in \mathscr{R}[x]/\langle x^{np^s} - 1 - u\alpha^{-1}\beta - u^2\alpha^{-1}\delta\rangle$. 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 $(\alpha+u\beta+u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$. In fact, the problem of determination of all $(\alpha + u\beta + u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$ and their dual codes is not yet completely solved. Propositions 4.2.1 and 4.2.2 and the following theorem completely solves this problem when β is non-zero.

Theorem 4.2.1. When $\beta \neq 0$, the following hold.

(a) All ideals of the ring $\mathscr{K}_j$ 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 $\text{ann}(\langle f_j(x)^\ell \rangle) = \langle f_j(x)^{3p^s-\ell} \rangle$.

(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 $\mathscr{R}$-module.

Proof. (a) To prove the result, we first observe that an element $a(x) \in \mathscr{K}_j$ can be uniquely expressed as $a(x) = a_0(x) + ua_1(x) + u^2a_2(x)$, where $a_0(x), a_1(x), a_2(x) \in \mathcal{P}_{d_jp^s}(\mathbb{F}_{p^m})$. By division algorithm in $\mathbb{F}_{p^m}[x]$, there exist unique polynomials $q(x), r(x) \in \mathbb{F}_{p^m}[x]$ such that $a_0(x) = f_j(x)q(x) + r(x)$, where either $r(x) = 0$ or deg $r(x) < d_j$. This implies that $a(x) = f_j(x)q(x) + r(x) + ua_1(x) + u^2a_2(x)$. Now in view of Lemma 4.2.2(b), we see that $a(x)$ is a unit in $\mathscr{K}_j$ if and only if $r(x)$ is a unit in $\mathscr{K}_j$. Further, by Lemma 4.2.2(a), we see that $r(x) \in \mathbb{F}_{p^m}[x]$ is a unit in $\mathscr{K}_j$ if and only if $r(x) \neq 0$. This shows that $a(x)$ is a non-unit in $\mathscr{K}_j$ if and only if $r(x) = 0$ if and only if $a(x) \in \langle f_j(x) \rangle$. That is, all the non-units of $\mathscr{K}_j$ are given by $\langle f_j(x) \rangle$. Now by Theorem 2.0.5 and Lemma 4.2.2(b), we see that $\mathscr{K}_j$ is a chain ring and all its ideals are given by $\langle f_j(x)^\ell \rangle$, where $0 \leq \ell \leq 3p^s$. Furthermore, we observe that the residue field of $\mathscr{K}_j$ is given by $\overline{\mathscr{K}_j} = \mathscr{K}_j/\langle f_j(x) \rangle$, and that $|\overline{\mathscr{K}_j}| = p^{md_j}$. Now by Theorem 2.0.5 and Lemma 4.2.2(b) again, we obtain $|\langle f_j(x)^\ell \rangle| = p^{md_j(3p^s-\ell)}$ for $0 \leq \ell \leq 3p^s$. Further, it is easy to observe that $\text{ann}(\langle f_j(x)^\ell \rangle) = \langle f_j(x)^{3p^s-\ell} \rangle$.

(b) When $kp^s \leq \ell \leq (k+1)p^s$ with $k \in \{0,1,2\}$, by Lemma 4.2.2(b), we see that $\langle f_j(x)^\ell \rangle = \langle u^k f_j(x)^{\ell-kp^s} \rangle$. Using this, it is easy to observe that 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 $\mathscr{R}$-module.

□

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

Corollary 4.2.1. Let $n \geq 1$ be an integer, and let $\alpha_0 \in \mathbb{F}_{p^m}$ be such that the binomial $x^n - \alpha_0$ is irreducible over $\mathbb{F}_{p^m}$. Let $\alpha = \alpha_0^{p^s}$, and $\beta(\neq 0), \delta \in \mathbb{F}_{p^m}$. Then there exists an isodual $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ 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 $(\alpha + u\beta + u^2\delta)$-constacyclic code of length $n2^s$ over $\mathscr{R}$.

Proof. On taking $f_j(x) = x^n - \alpha_0$ in Theorem 4.2.1, we see that all $(\alpha + u\beta + u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$ 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 $\mathscr{C} = \langle (x^n - \alpha_0)^\ell \rangle$ is isodual, then we must have $|\mathscr{C}| = |\mathscr{C}^\perp|$. 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 $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$. 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 $(\alpha + u\beta + u^2\delta)$-constacyclic code of length $n2^s$ over $\mathscr{R}$, which completes the proof. □

Remark 4.2.1. By Theorem 3.75 of [53], 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 $\beta = \delta = 0$, and we determine all non-trivial ideals of the ring $\mathscr{K}_j$, their cardinalities, their annihilators and their minimal generating sets.

Theorem 4.2.2. Let $\beta = \delta = 0$, and let $\mathscr{I}$ be a non-trivial ideal of the ring $\mathscr{K}_j$ with $\mathrm{Tor}_0(\mathscr{I}) = \langle f_j(x)^a \rangle$, $\mathrm{Tor}_1(\mathscr{I}) = \langle f_j(x)^b \rangle$ and $\mathrm{Tor}_2(\mathscr{I}) = \langle f_j(x)^c \rangle$ for some integers a, b, c satisfying $0 \leq c \leq b \leq a \leq p^s$. Suppose that $B_i(x), C_k(x), Q_\ell(x), W_z(x)$ run over $\mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for each relevant i, k, ℓ and z. Then the following hold.

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

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

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

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

and the set

$$\{u^2 f_j(x)^c, u^2 x f_j(x)^c, \cdots, u^2 x^{d_j p^s - d_j c - 1} f_j(x)^c\}$$

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

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

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

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 $\mathscr{K}_j$ of the form $\sum_{i=0}^{c-t-1} B_i(x) f_j(x)^i$. Moreover, we have

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

and the set

$$\{u f_j(x)^b + u^2 f_j(x)^t G(x), x(u f_j(x)^b + u^2 f_j(x)^t G(x)), \cdots, x^{d_j p^s - d_j b - 1}(u f_j(x)^b + u^2 f_j(x)^t G(x))\} \cup \{u^2 f_j(x)^c, u^2 x f_j(x)^c, \cdots, u^2 x^{d_j b - d_j c - 1} f_j(x)^c\}$$

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

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

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

where $\max\{0, a + b - p^s\} \leq t_1 < b$ 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 $\mathscr{K}_j$ 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 $\mathscr{K}_j$ 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 $\mathscr{K}_j$ 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

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

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

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

and the set

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

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

Proof. As $\mathscr{I}$ is a non-trivial ideal of $\mathscr{K}_j$, we note that neither $a = 0$ nor $a = b = c = p^s$ hold. Further, by Lemma 4.2.3, we have $|\mathscr{I}| = p^{md_j(3p^s-a-b-c)}$. Now to write down all such non-trivial ideals of $\mathscr{K}_j$ 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 $\mathscr{I} \subseteq \langle u^2\rangle$. In this case, we have $0 \le c < p^s$. Here we observe that $\mathscr{I} = \langle u^2 f_j(x)^c\rangle$. Now to find ann$(\mathscr{I})$, we consider the ideal $\mathscr{B}_1 =$

$\langle f_j(x)^{p^s-c}, u, u^2\rangle$, and we see that $\mathscr{B}_1 \subseteq \text{ann}(\mathscr{I})$ and that $|\mathscr{B}_1| = p^{md_j(2p^s+c)}$. As

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

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

(ii) When $a = p^s$ and $b < p^s$, we have $\mathscr{I} \subseteq \langle u\rangle$ and $\mathscr{I} \not\subseteq \langle u^2\rangle$. Here we observe that

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

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

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

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

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

where $G(x)$ is either 0 or a unit in $\mathscr{K}_j$ 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 $0 \leq i \leq c-t-1$.

Further, as $f_j(x)^{p^s-b}\{uf_j(x)^b + u^2f_j(x)^tG(x)\} = u^2f_j(x)^{p^s-b+t}G(x) \in \mathscr{I}$, we must have $p^s - b + t \geq c$ when $G(x) \neq 0$. Moreover, let $\mathscr{B}_2 = \langle f_j(x)^{p^s-c} - uf_j(x)^{p^s-c+t-b}G(x),\ uf_j(x)^{p^s-b},\ u^2\rangle$. We observe that $\mathscr{B}_2 \subseteq \text{ann}(\mathscr{I})$ and $|\mathscr{B}_2| \geq p^{md_j(p^s+b+c)}$. Since

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

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

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

(iii) When $a < p^s$, we have $\mathscr{I} \not\subseteq \langle u\rangle$. In this case, we see that $a > 0$. Here we observe that

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

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

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

where $D_1(x)$ is either 0 or a unit in $\mathscr{K}_j$ 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 $\mathscr{K}_j$ 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 $\mathscr{K}_j$ of the form $\sum_{i=\theta}^{c-1} W_i(x)f_j(x)^{i-\theta}$ with $A_\ell(x), B_k(x), W_i(x) \in \mathscr{K}_j$ for each ℓ, k and i.

In order to determine $\text{ann}(\mathscr{I})$, we first observe that

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

which implies that $p^s-a+t_1 \geq b$ when $D_1(x) \neq 0$. Next we see that $f_j(x)^{p^s-b}\{uf_j(x)^b + u^2f_j(x)^\theta V(x)\} \in \mathscr{I}$, which gives $p^s - b + \theta \geq c$ when $V(x) \neq 0$. Moreover, as $uf_j(x)^a + u^2f_j(x)^{t_1}D_1(x) \in \mathscr{I}$ and $f_j(x)^{a-b}\{uf_j(x)^b + u^2f_j(x)^\theta V(x)\} \in \mathscr{I}$, we note that $u^2\{f_j(x)^{t_1}D_1(x) - f_j(x)^{a-b+\theta}V(x)\} \in \mathscr{I}$, which implies that

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

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

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

can be rewritten as

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

which implies that

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

This further implies that

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

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

Next consider the ideal

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

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

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

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

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

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

Corollary 4.2.2. 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

4.2.2, we have the following:

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

(b) There exists an isodual α-constacyclic code of Type II over $\mathscr{R}$ 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 $\mathscr{R}$.

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

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

(a) Let $\mathscr{C}$ be of Type I, i.e., $\mathscr{C} = \langle u^2(x^n - \alpha_0)^c\rangle$ for some integer c satisfying $0 \leq c < p^s$. By Theorem 4.2.2, we see that $|\mathscr{C}| = p^{mn(p^s - c)}$ and $|\text{ann}(\mathscr{C})| = p^{mn(2p^s + c)}$. Now if the code $\mathscr{C}$ is isodual, then we must have $|\mathscr{C}| = |\text{ann}(\mathscr{C})|$. 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 $\mathscr{R}$.

(b) Suppose that the code $\mathscr{C}$ is of Type II, i.e., $\mathscr{C} = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^t G(x), u^2(x^n - \alpha_0)^c\rangle$, where $0 \leq c \leq b < p^s$ and $0 \leq t < c$ if $G(x) \neq 0$. By Theorem 4.2.2, we have $|\mathscr{C}| = p^{mn(2p^s - b - c)}$, $\text{ann}(\mathscr{C}) = \langle (x^n - \alpha_0)^{p^s - c} - u(x^n - \alpha_0)^{p^s - c + t - b} G(x), u(x^n - \alpha_0)^{p^s - b}, u^2\rangle$ and $|\text{ann}(\mathscr{C})| = p^{mn(p^s + b + c)}$. Now if the code $\mathscr{C}$ is isodual, then we must have $|\mathscr{C}| = |\text{ann}(\mathscr{C})|$, which gives $p = 2$ and $c = 2^{s-1} - b$. Further, if the code $\mathscr{C}$ is $\mathscr{R}$-linearly equivalent to $\text{ann}(\mathscr{C})$, then $\text{Tor}_0(\mathscr{C}) = \{0\}$ must be $\mathbb{F}_{2^m}$-linearly equivalent to $\text{Tor}_0(\text{ann}(\mathscr{C})) = \langle (x^n - \alpha_0)^{2^s - c}\rangle$, 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 4.2.2 again, we see that $\mathscr{C} = \text{ann}(\mathscr{C})$ holds, which implies that the codes $\mathscr{C}(\subseteq \mathscr{R}_\alpha)$ and $\mathscr{C}^{\perp}(\subseteq \widehat{\mathscr{R}_\alpha})$ are $\mathscr{R}$-linearly equivalent.

(c) Suppose that the code $\mathscr{C}$ is of Type III, i.e., $\mathscr{C} = \langle (x^n-\alpha_0)^a + u(x^n-\alpha_0)^{t_1}D_1(x) + u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^{\theta}V(x), u^2(x^n-\alpha_0)^c\rangle$, 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 4.2.2, we have $|\mathscr{C}| = p^{mn(3p^s-a-b-c)}$ and $|\text{ann}(\mathscr{C})| = p^{mn(a+b+c)}$. From this, we see that if the code $\mathscr{C}$ 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 4.2.2 again, that for $2^{s-1} \leq a < 2^s$, the code $\mathscr{C} = \langle (x^n-\alpha_0)^a + u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^{2^{s-1}}, u^2(x^n-\alpha_0)^{2^s-a}\rangle$ satisfies $\mathscr{C} = \text{ann}(\mathscr{C})$, from which part (c) follows.

□

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

Theorem 4.2.3. Let $\beta = 0$ and δ be a non-zero element of $\mathbb{F}_{p^m}$. Let $\mathscr{I}$ be a non-trivial ideal of the ring $\mathscr{K}_j$ with $\text{Tor}_0(\mathscr{I}) = \langle f_j(x)^a\rangle$, $\text{Tor}_1(\mathscr{I}) = \langle f_j(x)^b\rangle$ and $\text{Tor}_2(\mathscr{I}) = \langle f_j(x)^c\rangle$ for some integers a, b, c satisfying $0 \leq c \leq b \leq a \leq p^s$. Suppose that $B_i(x), C_k(x), Q_\ell(x), W_z(x)$ run over $\mathcal{P}_{d_j}(\mathbb{F}_{p^m})$ for each relevant i, k, ℓ and z. Then the following hold.

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

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

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

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

and the set

$$\left\{u^2 f_j(x)^c, u^2 x f_j(x)^c, \cdots, u^2 x^{d_j p^s - d_j c - 1} f_j(x)^c\right\}$$

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

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

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

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 $\mathscr{K}_j$ of the form $\sum_{i=0}^{c-t-1} B_i(x) f_j(x)^i$. Furthermore, we have

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

and the set

$$\{uf_j(x)^b + u^2 f_j(x)^t G(x), x(uf_j(x)^b + u^2 f_j(x)^t G(x)), \cdots, x^{d_j p^s - d_j b - 1}(uf_j(x)^b + u^2 f_j(x)^t G(x))\} \cup \{u^2 f_j(x)^c, u^2 x f_j(x)^c, \cdots, u^2 x^{d_j b - d_j c - 1} f_j(x)^c\}$$

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

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

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

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 $\mathscr{K}_j$ 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 $\mathscr{K}_j$ 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 $\mathscr{K}_j$ of the form $\sum_{i=0}^{c-\theta-1} W_i(x) f_j(x)^i$. Furthermore, we have

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

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

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

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

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

and the set

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

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

Proof. Working as in Theorem 4.2.2 and by applying Lemmas 4.2.2(c) and 4.2.3, the desired result follows. □

In the following corollary, we list some isodual $(\alpha+u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$ when $\delta \neq 0$ and the binomial $x^n-\alpha_0$ is irreducible over $\mathbb{F}_{p^m}$.

Corollary 4.2.3. 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 δ be a non-zero element of $\mathbb{F}_{p^m}$. Following the same notations as in Theorem 4.2.3, we have the following:

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

(b) There exists an isodual $(\alpha+u^2\delta)$-constacyclic code of Type II over $\mathscr{R}$ 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 $(\alpha+u^2\delta)$-constacyclic code of Type II over $\mathscr{R}$.

(c) There exists an isodual $(\alpha+u^2\delta)$-constacyclic code of Type III over $\mathscr{R}$ if and only if $p=2$. Furthermore, when $p=2$, the codes $\mathscr{C} = \langle (x^n-\alpha_0)^a + u(x^n-\alpha_0)^{a-2^{s-1}}\delta^{2^{m-1}} +$

$u^2(x^n-\alpha_0)^{t_2}D_2(x), u(x^n-\alpha_0)^{2^{s-1}}+u^2\delta^{2^{m-1}}, u^2(x^n-\alpha_0)^{2^s-a}\rangle$, $2^{s-1}\leq a<2^s$, are isodual $(\alpha+u^2\delta)$-constacyclic codes of Type III over $\mathscr{R}$.

Proof. Working in a similar manner as in Corollary 4.2.2 and by applying Theorem 4.2.3, the desired result follows. □

4.3 Ranks, Hamming distances, RT distances and RT weight distributions of some constacyclic codes over $\mathscr{R}$

Let $\alpha,\beta,\delta\in\mathbb{F}_{p^m}$ be such that α is non-zero. Furthermore, as $\alpha\in\mathbb{F}_{p^m}\setminus\{0\}$, there exists $\alpha_0\in\mathbb{F}_{p^m}$ satisfying $\alpha=\alpha_0^{p^s}$. 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 $(\alpha+u\beta+u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$. We shall also list all MDS Hamming and MDS RT $(\alpha+u\beta+u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$.

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

Theorem 4.3.1. The following hold.

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

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

(b) Let $\mathscr{C}$ be an $(\alpha+u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ with $\text{Tor}_2(\mathscr{C})=\langle(x^n-\alpha_0)^c\rangle$, where $0\leq c\leq p^s-1$. Then we have $\text{rank}(\mathscr{C})=np^s-nc$.

Proof. It follows immediately from Theorems 4.2.1(b), 4.2.2 and 4.2.3. □

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

Theorem 4.3.2. Let $\beta \in \mathbb{F}_{p^m} \setminus \{0\}$, and let $\mathscr{C} = \langle (x^n - \alpha_0)^\nu \rangle$ be an $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$, where $0 \leq \nu \leq 3p^s - 1$. Then with respect to the Hamming metric, the following hold.

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

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

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

Proof. The Hamming distance of the code $\mathscr{C}$ can be determined by applying Theorems 2.0.8 and 2.0.7(d), while Theorem 4.3.1(a) gives the rank of the code $\mathscr{C}$. □

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

Theorem 4.3.3. Let $\beta \in \mathbb{F}_{p^m} \setminus \{0\}$. The code $\mathscr{C} = \langle 1 \rangle$ is the only MDS Hamming $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$.

Proof. Let $\mathscr{C}$ be a non-zero $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$. Then by Theorem 4.2.1, we see that $\mathscr{C} = \langle (x^n - \alpha_0)^\nu \rangle$, where $0 \leq \nu \leq 3p^s - 1$. By Theorem 4.2.1 again, we see that $|\mathscr{C}| = p^{mn(3p^s - \nu)}$.

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

$$n\nu = 3\{d_H(\mathscr{C}) - 1\}. \tag{4.3.1}$$

When $0 \leq \nu \leq 2p^s$, we see, by Theorem 4.3.2, that $d_H(\mathscr{C}) = 1$. This, by (4.3.1), implies that the code $\mathscr{C}$ is MDS Hamming if and only if $\nu = 0$.

Next let $2p^s+1 \leq \nu \leq 3p^s-1$. Here working as in Theorem 4.3.2, we see that $d_H(\mathscr{C})$ is equal to the Hamming distance of the α-constacyclic code $\mathscr{D} = \langle (x^n-\alpha_0)^{\nu-2p^s}\rangle$ of length np^s over $\mathbb{F}_{p^m}$. By Theorem 2.0.5, we see that $|\mathscr{D}| = p^{mn(p^s-\nu+2p^s)}$. By 2.0.1(a), we have $|\mathscr{D}| \leq p^{m(np^s-d_H(\mathscr{D})+1)}$. This implies that $n\nu - 2np^s \geq d_H(\mathscr{D}) - 1 = d_H(\mathscr{C}) - 1$. From this and using the fact that $np^s \geq d_H(\mathscr{C}) > d_H(\mathscr{C}) - 1$, we get $n\nu > 3\{d_H(\mathscr{C}) - 1\}$. This, by (4.3.1), implies that the code $\mathscr{C}$ is not MDS Hamming code when $2p^s+1 \leq \nu \leq 3p^s-1$.

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

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

Theorem 4.3.4. Let $\beta \in \mathbb{F}_{p^m} \setminus \{0\}$, and let $\mathscr{C} = \langle (x^n-\alpha_0)^\nu\rangle$ be an $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$, where $0 \leq \nu \leq 3p^s-1$. With respect to the RT metric, the following hold.

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

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

Proof. By Lemma 4.2.2(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 $1 \leq \nu \leq 2p^s$. This implies that $d_{RT}(\mathscr{C}) = 1$ for $1 \leq \nu \leq 2p^s$.

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

From this and by Theorem 4.3.1(a), we get the desired result. □

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

Theorem 4.3.5. Let $\beta \in \mathbb{F}_{p^m}\backslash\{0\}$. Then the code $\mathscr{C} = \langle 1\rangle$ is the only MDS RT $(\alpha+u\beta+u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$.

Proof. Let $\mathscr{C}$ be a non-zero $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$. Then by Theorem 4.2.1, we have $\mathscr{C} = \langle (x^n - \alpha_0)^\nu\rangle$, where $0 \leq \nu \leq 3p^s - 1$. By Theorem 4.2.1 again, we see that $|\mathscr{C}| = p^{mn(3p^s-\nu)}$. Further, the code $\mathscr{C}$ is MDS RT Code if and only if $p^{mn(3p^s-\nu)} = |\mathscr{C}| = p^{3m(np^s-d_{RT}(\mathscr{C})+1)}$, which holds if and only if

$$n\nu = 3\{d_{RT}(\mathscr{C}) - 1\}. \tag{4.3.2}$$

Now for $0 \leq \nu \leq 2p^s$, by Theorem 4.3.4, we see that $d_{RT}(\mathscr{C}) = 1$. By (4.3.2), we note that the code $\mathscr{C}$ is MDS RT Code if and only if $\nu = 0$.

On the other hand, when $2p^s + 1 \leq \nu \leq 3p^s - 1$, by Theorem 4.3.4, we see that $d_{RT}(\mathscr{C}) = n\nu - 2np^s + 1$. One can easily verify that (4.3.2) does not hold in this case. This shows that the code $\mathscr{C}$ is not MDS RT Code when $2p^s + 1 \leq \nu \leq 3p^s - 1$. □

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

Theorem 4.3.6. Let $\beta \in \mathbb{F}_{p^m} \setminus \{0\}$, and let $\mathscr{C} = \langle (x^n - \alpha_0)^\nu\rangle$ be an $(\alpha + u\beta + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$, where $0 \leq \nu \leq 3p^s$. For $0 \leq \rho \leq np^s$, let $\mathcal{A}_\rho$ denote the number of codewords in $\mathscr{C}$ 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 $2p^s + 1 \leq \nu \leq 3p^s - 1$, we have

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

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

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

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

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

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

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

(b) Let $2p^s + 1 \leq \nu \leq 3p^s - 1$. Here by Theorem 4.3.4, we see that $d_{RT}(\mathscr{C}) = n\nu - 2np^s + 1$, which gives $\mathcal{A}_\rho = 0$ for $1 \leq \rho \leq n\nu - 2np^s$. Next let $n\nu - 2np^s + 1 \leq \rho \leq np^s$. Here by Lemma 4.2.2(b), we see that $\langle (x^n - \alpha_0)^{p^s} \rangle = \langle u \rangle$. This implies that $\mathscr{C} = \langle u^2(x^n - \alpha_0)^{\nu - 2p^s} \rangle = \{u^2(x^n - \alpha_0)^{\nu - 2p^s} F(x) : F(x) \in \mathbb{F}_{p^m}[x]\}$. From this, we observe that the RT weight of the codeword $u^2(x^n - \alpha_0)^{\nu - 2p^s} F(x) \in \mathscr{C}$ 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 4.2.2(b), we see that $\mathscr{C} = \langle (x^n - \lambda_0)^{yp^s} \rangle = \langle u^y \rangle = \{u^y F(x) : F(x) \in \mathcal{P}_{np^s}(\mathscr{R})\}$. From this, we see that $\mathcal{A}_\rho = (p^{m(3-y)} - 1)p^{m(3-y)(\rho-1)}$ for $1 \leq \rho \leq np^s$.

(d) Next let $(k-1)p^s + 1 \leq \nu \leq kp^s - 1$, where $k \in \{1, 2\}$. Here also, by Lemma 4.2.2(b), we have $\langle (x^n - \alpha_0)^{p^s} \rangle = \langle u \rangle$, which implies that $u^k \in \mathscr{C}$ and $\mathscr{C} = \langle u^{k-1}(x^n - \alpha_0)^{\nu - (k-1)p^s} \rangle$. Further, we observe that any codeword $Q(x) \in \mathscr{C}$ can be uniquely written as $Q(x) = u^{k-1}(x^n - \alpha_0)^{\nu - (k-1)p^s} F_Q(x) + u^k H_Q(x)$ with $F_Q(x) \in \mathcal{P}_{knp^s - n\nu}(\mathbb{F}_{p^m})$, $H_Q(x) \in \mathcal{P}_{np^s}(\mathbb{F}_{p^m})$ when $k = 2$ and $H_Q(x) \in \mathcal{P}_{np^s}(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})$ when $k = 1$.

When $1 \leq \rho \leq n\nu - (k-1)np^s$, we see that the RT weight of the codeword $Q(x) \in \mathscr{C}$ 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 $1 \leq \rho \leq n\nu$.

Next let $n\nu - (k-1)np^s + 1 \leq \rho \leq np^s$. In this case, we see that the RT weight of the codeword $Q(x) \in \mathscr{C}$ 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 $H_Q(x)$ is either 0 or $\deg H_Q(x) \leq \rho - 1$, 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 $(\alpha + u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$ are determined.

Theorem 4.3.7. Let $\mathscr{C}$ be a non-trivial $(\alpha + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ with $\text{Tor}_2(\mathscr{C}) = \langle (x^n - \alpha_0)^c \rangle$ for some integer c satisfying $0 \leq c < p^s$ (as determined in Theorems 4.2.2 and 4.2.3). Then with respect to the Hamming metric, the code $\mathscr{C}$ is an $[np^s, n(p^s - c), d_H(\mathscr{C})]$-code over $\mathscr{R}$, where

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

Proof. By Theorem 4.3.1(b), we see that $\text{rank}(\mathscr{C}) = np^s - nc$. Further, by applying Theorems 2.0.8 and 2.0.7(d), one can determine the Hamming distance of the code $\mathscr{C}$. □

One can easily observe that the $(\alpha + u^2\delta)$-constacyclic code $\mathscr{C} = \langle 1 \rangle$ of length np^s over $\mathscr{R}$ is MDS Hamming and MDS RT Code. In the following theorem, we list all non-trivial

MDS Hamming $(\alpha + u^2\delta)$-constacyclic codes of length np^s over $\mathscr{R}$.

Theorem 4.3.8. The following hold.

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

(b) When $\delta = 0$, there exists a non-trivial MDS Hamming α-constacyclic code of length np^s over $\mathscr{R}$ if and only if $n = 1$. Furthermore, when $n = 1$, all the distinct non-trivial α-constacyclic codes of length p^s over $\mathscr{R}$ 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 $1 \leq a \leq p-1$ if $s = 1$ while $a \in \{1, p^s-1\}$ if $s \geq 2$, $\max\{0, 2a-p^s\} \leq t_1 < a$ 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 $\mathscr{R}_\alpha$ 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 $\mathscr{R}_\alpha$ 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 $\mathscr{C}$ be a non-trivial $(\alpha + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ with $\mathrm{Tor}_2(\mathscr{C}) = \langle (x^n-\alpha_0)^c\rangle$, where $0 \leq c < p^s$ (as determined in Theorems 4.2.2 and 4.2.3). Here by Theorem 4.3.7, we note that $d_H(\mathscr{C}) = d_H(\mathrm{Tor}_2(\mathscr{C}))$. By applying Theorem 2.0.1(a), we have $p^{mn(p^s-c)} = |\mathrm{Tor}_2(\mathscr{C})| \leq p^{mn(p^s - d_H(\mathrm{Tor}_2(\mathscr{C}))+1)}$. This gives

$$nc \geq d_H(\mathrm{Tor}_2(\mathscr{C})) - 1 = d_H(\mathscr{C}) - 1. \tag{4.3.3}$$

(i) First let $\mathscr{C}$ be of Type I. Here by Theorems 4.2.2 and 4.2.3, we have $\mathscr{C} = \langle u^2(x^n - \alpha_0)^c\rangle$. By Theorems 4.2.2 and 4.2.3 again, we see that $|\mathscr{C}| = p^{mn(p^s-c)}$. Now by Theorem 2.0.1(a), the code $\mathscr{C}$ is MDS Hamming code if and only if $p^{mn(p^s-c)} =$

$|\mathscr{C}| = p^{3m(np^s - d_H(\mathscr{C})+1)}$, which holds if and only if

$$2np^s + nc = 3\{d_H(\mathscr{C}) - 1\}. \tag{4.3.4}$$

By (4.3.3) and using the fact that $p^s > c$, we get $2np^s + nc > 3\{d_H(\mathscr{C}) - 1\}$. This, by (4.3.4), implies that the code $\mathscr{C}$ is not MDS Hamming code in this case.

(ii) Now let $\mathscr{C}$ be of Type II. Here by Theorems 4.2.2 and 4.2.3, we have $\mathscr{C} = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^t G(x), u^2(x^n - \alpha_0)^c \rangle$, where $0 \leq c \leq b < p^s$, $\max\{0, c + b - p^s\} \leq t < c$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $\mathscr{R}_{\alpha+u^2\delta}$ 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 4.2.2 and 4.2.3 again, we have $|\mathscr{C}| = p^{mn(2p^s - b - c)}$. Now the code $\mathscr{C}$ is MDS code if and only if $p^{mn(2p^s-b-c)} = |\mathscr{C}| = p^{3m(np^s - d_H(\mathscr{C})+1)}$, which holds if and only if

$$np^s + nb + nc = 3\{d_H(\mathscr{C}) - 1\}. \tag{4.3.5}$$

Now by (4.3.3) and using the fact that $p^s > b \geq c$, we get $np^s + nb + nc > 3\{d_H(\mathscr{C}) - 1\}$. This, by (4.3.5), shows that the code $\mathscr{C}$ is not MDS Hamming code in this case.

(iii) Next let $\mathscr{C}$ be of Type III. Here by Theorems 4.2.2 and 4.2.3, we have $\mathscr{C} = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^{t_1} D_1(x) + u^2(x^n - \alpha_0)^{t_2} D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^\theta V(x), u^2(x^n - \alpha_0)^c \rangle$, where $a > 0$, $0 \leq c \leq b \leq a < p^s$, $\max\{0, a + b - p^s\} \leq t_1 < b$ 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 $V(x) \neq 0$, $D_1(x)$ is either 0 or a unit in $\mathscr{R}_{\alpha+u^2\delta}$ 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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 4.2.2 and 4.2.3 again, we see that

$$u^2\{(x^n - \alpha_0)^{p^s - a + t_1 - b + \theta} V(x) D_1(x) - (x^n - \alpha_0)^{p^s - a + t_2} D_2(x) - \delta\} \in \langle u^2(x^n - \alpha_0)^c \rangle, \tag{4.3.6}$$

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

$$na + nb + nc = 3\{d_H(\mathscr{C}) - 1\}. \tag{4.3.7}$$

By (4.3.3) and using the fact that $a \geq b \geq c$, we have $na + nb + nc \geq 3\{d_H(\mathscr{C}) - 1\}$ and equality holds if and only if $na = nb = nc = d_H(\mathscr{C}) - 1 = d_H(\text{Tor}_2(\mathscr{C})) - 1$.

Now when $a = b = c$, we see that $u^2\left\{(x^n-\alpha_0)^{t_1}D_1(x) - (x^n-\alpha_0)^{\theta}V(x)\right\} \in \langle u^2(x^n-\alpha_0)^a\rangle$, which implies that $t_1 = \theta$ and $D_1(x) = V(x)$. From this and using (4.3.6), we see that

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

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 $\delta \neq 0$.

Further, we see, by Theorem 2.0.8, that the code $\langle (x^n-\alpha_0)^a\rangle$, $0 \leq a < p^s$, of length np^s over $\mathbb{F}_{p^m}$ is MDS Hamming code if and only if

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

Using this, the desired result follows immediately.

□

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

Theorem 4.3.9. Let $\mathscr{C}$ be a non-trivial $(\alpha + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ with $\text{Tor}_2(\mathscr{C}) = \langle (x^n-\alpha_0)^c\rangle$ for some integer c satisfying $0 \leq c < p^s$ (as determined in

Theorems 4.2.2 and 4.2.3). Then the code $\mathscr{C}$ 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

$$w_{RT}(Q(x)) \geq w_{RT}(uQ(x)) \text{ for each } Q(x) \in \mathscr{R}_{\alpha+u^2\delta}. \tag{4.3.8}$$

(i) When $\mathscr{C}$ is of Type I, we have $\mathscr{C} = \langle u^2(x^n-\alpha_0)^c\rangle$. Here we note that $\mathscr{C} = \langle u^2(x^n-\alpha_0)^c\rangle = \{u^2(x^n-\alpha_0)^c f(x) : f(x) \in \mathbb{F}_{p^m}[x]\}$. Now for each non-zero $Q(x) \in \mathscr{C}$, by (4.3.8), we see that $w_{RT}(Q(x)) \geq w_{RT}(u^2(x^n-\alpha_0)^c) = nc+1$, which implies that $d_{RT}(\mathscr{C}) \geq nc+1$. Since $u^2(x^n-\alpha_0)^c \in \mathscr{C}$, we obtain $d_{RT}(\mathscr{C}) = nc+1$.

(ii) When $\mathscr{C}$ is of Type II, we have $\mathscr{C} = \langle u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^t G(x), u^2(x^n-\alpha_0)^c\rangle$, where $c \leq b < p^s$, $\max\{0, c+b-p^s\} \leq t < c$ if $G(x) \neq 0$ and $G(x)$ is either 0 or a unit in $\mathbb{F}_{p^m}[x]/\langle f_j(x)^{p^s}\rangle$. Here by (4.3.8), we note that $w_{RT}(Q(x)) \geq w_{RT}(uQ(x))$ for each $Q(x) \in \mathscr{C} \setminus \langle u^2\rangle$, which implies that $w_{RT}(Q(x)) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$ for each $Q(x) \in \mathscr{C} \setminus \langle u^2\rangle$. From this, we get $d_{RT}(\mathscr{C}) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. Since $\langle u^2(x^n-\alpha_0)^c\rangle \subseteq \mathscr{C}$, we have $d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle) \geq d_{RT}(\mathscr{C})$. This implies that $d_{RT}(\mathscr{C}) = d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. From this and by case (i), we get $d_{RT}(\mathscr{C}) = nc+1$.

(iii) When $\mathscr{C}$ is of Type III, we have $\mathscr{C} = \langle (x^n-\alpha_0)^a + u(x^n-\alpha_0)^{t_1} D_1(x) + u^2(x^n-\alpha_0)^{t_2} D_2(x), u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^\theta V(x), u^2(x^n-\alpha_0)^c\rangle$, 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 $Q(x) \in \mathscr{C} \setminus \langle u\rangle$, by (4.3.8), we see that $w_{RT}(Q(x)) \geq w_{RT}(u^2Q(x))$. From this, we get $w_{RT}(Q(x)) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$ for each $Q(x) \in \mathscr{C}\setminus\langle u\rangle$. Further, for a codeword $Q(x) \in \mathscr{C}\setminus\langle u^2(x^n-\alpha_0)^c\rangle$ with $Q(x) \in \langle u\rangle$, by (4.3.8) 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 $d_{RT}(\mathscr{C}) \geq d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. On the other hand, as $\langle u^2(x^n-\alpha_0)^c\rangle \subseteq \mathscr{C}$, we have $d_{RT}(u^2(x^n-\alpha_0)^c\rangle) \geq d_{RT}(\mathscr{C})$, which implies that $d_{RT}(\mathscr{C}) = d_{RT}(\langle u^2(x^n-\alpha_0)^c\rangle)$. From this and by case (i), we get $d_{RT}(\mathscr{C}) = nc+1$.

From this and by Theorem 4.3.1(b), the desired result follows. □

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

Theorem 4.3.10. The following hold.

(a) When $\delta \neq 0$, there exists a non-trivial MDS RT $(\alpha + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ if and only if $p = 2$. Furthermore, when $p = 2$, all the distinct $(\alpha + u^2\delta)$-constacyclic codes of length $2^s n$ over $\mathscr{R}$ 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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:

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

(b) When $\delta = 0$, all the distinct non-trivial MDS RT α-constacyclic codes of length np^s over $\mathscr{R}$ 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 $\mathscr{R}_\alpha$ 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 $\mathscr{R}_\alpha$ 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 the result, let $\mathscr{C}$ be a non-trivial $(\alpha + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ with $\mathrm{Tor}_2(\mathscr{C}) = \langle (x^n - \alpha_0)^c\rangle$, where $0 \leq c < p^s$ (as determined in Theorems 4.2.2 and 4.2.3). Then by Theorem 4.3.9, we see that $d_{RT}(\mathscr{C}) = nc + 1$.

(i) First let $\mathscr{C}$ be of Type I. Here by Theorems 4.2.2 and 4.2.3, we have $\mathscr{C} = \langle u^2(x^n - \alpha_0)^c \rangle$. By Theorems 4.2.2 and 4.2.3 again, we see that $|\mathscr{C}| = p^{mn(p^s-c)}$. Now the code $\mathscr{C}$ is MDS RT code if and only if $p^{mn(p^s-c)} = |\mathscr{C}| = p^{3m(np^s - d_{RT}(\mathscr{C})+1)}$, which holds if and only if

$$2np^s + nc = 3\{d_{RT}(\mathscr{C}) - 1\} = 3nc. \tag{4.3.9}$$

As $p^s > c$, we get $2np^s + nc > 3nc$. From this and by (4.3.9), we see that the code $\mathscr{C}$ is not MDS RT code in this case.

(ii) Let $\mathscr{C}$ be of Type II. Here by Theorems 4.2.2 and 4.2.3, we have $\mathscr{C} = \langle u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^t G(x), u^2(x^n - \alpha_0)^c \rangle$, 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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 4.2.2 and 4.2.3 again, we have $|\mathscr{C}| = p^{mn(2p^s-b-c)}$. Now the code $\mathscr{C}$ is MDS RT code if and only if $p^{mn(2p^s-b-c)} = |\mathscr{C}| = p^{3m(np^s - d_H(\mathscr{C})+1)}$, which holds if and only if

$$np^s + nb + nc = 3\{d_{RT}(\mathscr{C}) - 1\} = 3nc. \tag{4.3.10}$$

Now as $p^s > b \geq c$, we have $np^s + nb + nc > 3nc$. From this and by (4.3.10), we see that the code $\mathscr{C}$ is not MDS RT code in this case.

(iii) Let $\mathscr{C}$ be of Type III. Here by Theorems 4.2.2 and 4.2.3, we have $\mathscr{C} = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^{t_1} D_1(x) + u^2(x^n - \alpha_0)^{t_2} D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^\theta V(x), u^2(x^n - \alpha_0)^c \rangle$, 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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 $\mathscr{R}_{\alpha+u^2\delta}$ 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 4.2.2 and 4.2.3 again, we see that

$$\begin{aligned} u^2\{(x^n - \alpha_0)^{p^s-a+t_1-b+\theta} V(x) D_1(x) - (x^n - \alpha_0)^{p^s-a+t_2} D_2(x) - \delta\} \\ \in \langle u^2(x^n - \alpha_0)^c \rangle, \end{aligned} \tag{4.3.11}$$

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

$$na + nb + nc = 3\{d_{RT}(\mathscr{C}) - 1\} = 3nc. \tag{4.3.12}$$

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 (4.3.11), we get $u^2\{(x^n - \alpha_0)^{p^s-2a+2t_1} D_1(x)^2 - (x^n - \alpha_0)^{p^s-a+t_2} D_2(x) - \delta\} \in \langle u^2(x^n - \alpha_0)^a\rangle$. 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 $\delta \neq 0$.

From this, the desired result follows.

□

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

Theorem 4.3.11. Let $\mathscr{C}$ be an $(\alpha + u^2\delta)$-constacyclic code of length np^s over $\mathscr{R}$ with $\text{Tor}_0(\mathscr{C}) = \langle (x^n - \alpha_0)^a\rangle$, $\text{Tor}_1(\mathscr{C}) = \langle (x^n - \alpha_0)^b\rangle$ and $\text{Tor}_2(\mathscr{C}) = \langle (x^n - \alpha_0)^c\rangle$ for some integers a, b, c satisfying $0 \leq c \leq b \leq a \leq p^s$ (as determined in Theorems 4.2.2 and 4.2.3). For $0 \leq \rho \leq np^s$, let $\mathcal{A}_\rho$ denote the number of codewords in $\mathscr{C}$ having the RT weight as ρ.

(a) If $\mathscr{C} = \{0\}$, then we have $\mathcal{A}_0 = 1$ and $\mathcal{A}_\rho = 0$ for $1 \leq \rho \leq np^s$.

(b) If $\mathscr{C} = \langle 1\rangle$, 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 $\mathscr{C} = \langle u^2(x^n - \alpha_0)^c\rangle$ is of Type I, then we have

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

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

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

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

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

Proof. Proofs of parts (a) and (b) are trivial. To prove parts (c)-(e), by Theorem 4.3.9(c), we see that $d_{RT}(\mathscr{C}) = nc+1$, which implies that $\mathcal{A}_\rho = 0$ for $1 \le \rho \le nc$. So from now on, we assume that $nc+1 \le \rho \le np^s$.

(c) Let $\mathscr{C} = \langle u^2(x^n-\alpha_0)^c\rangle$. Here we see that $\mathscr{C} = \langle u^2(x^n-\alpha_0)^c\rangle = \{u^2(x^n-\alpha_0)^c F(x) : F(x) \in \mathbb{F}_{p^m}[x]\}$. This implies that the codeword $u^2(x^n-\alpha_0)^c F(x) \in \mathscr{C}$ 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 $\mathscr{C} = \langle u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^t G(x), u^2(x^n-\alpha_0)^c\rangle$. Here we observe that each codeword $Q(x) \in \mathscr{C}$ can be uniquely expressed as $Q(x) = (u(x^n-\alpha_0)^b + u^2(x^n-\alpha_0)^t G(x))A_Q(x) + u^2(x^n-\alpha_0)^c B_Q(x)$, where $A_Q(x), B_Q(x) \in \mathbb{F}_{p^m}[x]$ satisfy deg $A_Q(x) \le n(p^s-b)-1$ if $A_Q(x) \ne 0$ and deg $B_Q(x) \le n(p^s-c)-1$ if $B_Q(x) \ne 0$. From this, we see that if $nc+1 \le \rho \le nb$, then the RT weight of the codeword $Q(x) \in \mathscr{C}$ 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 $nc+1 \le \rho \le nb$. Further, if $nb+1 \le \rho \le np^s$, then the RT weight of the codeword $Q(x) \in \mathscr{C}$ 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 $A_Q(x) \leq \rho - nb - 2$ 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 $\mathscr{C} = \langle (x^n - \alpha_0)^a + u(x^n - \alpha_0)^{t_1} D_1(x) + u^2(x^n - \alpha_0)^{t_2} D_2(x), u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^\theta V(x), u^2(x^n - \alpha_0)^c \rangle$. Here we see that each codeword $Q(x) \in \mathscr{C}$ can be uniquely expressed as $Q(x) = ((x^n - \alpha_0)^a + u(x^n - \alpha_0)^{t_1} D_1(x) + u^2(x^n - \alpha_0)^{t_2} D_2(x))M_Q(x) + (u(x^n - \alpha_0)^b + u^2(x^n - \alpha_0)^\theta V(x))N_Q(x) + u^2(x^n - \alpha_0)^c W_Q(x)$, 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 $Q(x) \in \mathscr{C}$ 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 $Q(x) \in \mathscr{C}$ 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 $\mathcal{A}_\rho = (p^{2m} - 1)p^{m(2\rho - nb - nc - 2)}$.

Next let $na + 1 \leq \rho \leq np^s$. Here the RT weight of the codeword $Q(x) \in \mathscr{C}$ 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. □

4.4 Hamming distances of constacyclic codes of length $2p^s$ over $\mathscr{R}$ and determination of MDS Hamming 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 $\mathscr{R}$, and we will also identify all MDS Hamming constacyclic codes of length $2p^s$ over $\mathscr{R}$. For this, we recall that $\lambda = \alpha + u\beta + u^2\delta$, where α, β, δ are elements of $\mathbb{F}_{p^m}$ and α is non-zero. As $\alpha \in \mathbb{F}_{p^m} \setminus \{0\}$, there exists $\alpha_0 \in \mathbb{F}_{p^m}$ satisfying $\alpha = \alpha_0^{p^s}$. Here we have $\mathscr{R}_\lambda = \mathscr{R}[x]/\langle x^{2p^s} - \lambda\rangle$.

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 $(\alpha + u\beta + u^2\delta)$-constacyclic codes of length $2p^s$ over $\mathscr{R}$ and identify all MDS Hamming codes within this class of codes on taking $n = 2$ in Theorems 4.3.2, 4.3.3, 4.3.7 and 4.3.8.

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 $\xi(\neq 0) \in \mathbb{F}_{p^m}$ such that $\alpha_0 = \xi^2$. This implies that $x^2 - \alpha_0 = (x + \xi)(x - \xi)$. From this and working as in Section 4.2, we get $\mathscr{R}_\lambda \simeq \mathscr{K}_1 \oplus \mathscr{K}_2$, where $\mathscr{K}_1 = \mathscr{R}[x]/\langle (x+\xi)^{p^s} + ug_1(x) + u^2h_1(x)\rangle$ and $\mathscr{K}_2 = \mathscr{R}[x]/\langle (x-\xi)^{p^s} + ug_2(x) + u^2h_2(x)\rangle$, where for $j \in \{1, 2\}$, the polynomials $g_j(x), h_j(x) \in \mathbb{F}_{p^m}[x]$ satisfy $\gcd(x + \xi, g_1(x)) = \gcd(x - \xi, g_2(x)) = 1$ when $\beta \neq 0$, $g_j(x) = h_j(x) = 0$ when $\beta = \delta = 0$, while $g_j(x) = 0$ and $\gcd(x + \xi, h_1(x)) = \gcd(x - \xi, h_2(x)) = 1$ when $\beta = 0$ and $\delta \neq 0$.

Now let $\mathscr{C}$ be an $(\alpha + u\beta + u^2\delta)$-constacyclic code of length $2p^s$ over $\mathscr{R}$, i.e., an ideal of the ring $\mathscr{R}_\lambda$. Then by Proposition 4.2.1, we have

$$\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2, \tag{4.4.1}$$

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

$\{c_2(x) \in \mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle : u^2c_2(x) \in \mathscr{C}\}$. Then we make the following observation.

Proposition 4.4.1. Let $\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2$ be an $(\alpha + u\beta + u^2\delta)$-constacyclic code of length $2p^s$ over $\mathscr{R}$ (i.e., an ideal of the ring $\mathscr{R}_\lambda$), where $\mathscr{C}_j$ is an ideal of $\mathscr{K}_j$ for $j \in \{1,2\}$. Then $\mathrm{Tor}_0(\mathscr{C})$, $\mathrm{Tor}_1(\mathscr{C})$ and $\mathrm{Tor}_2(\mathscr{C})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle$. Moreover, we have $\mathrm{Tor}_i(\mathscr{C}) = \mathrm{Tor}_i(\mathscr{C}_1) \oplus \mathrm{Tor}_i(\mathscr{C}_2)$ for $0 \le i \le 2$, where for $i \in \{0,1,2\}$, $\mathrm{Tor}_i(\mathscr{C}_1)$ and $\mathrm{Tor}_i(\mathscr{C}_2)$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x+\xi)^{p^s}\rangle$ and $\mathbb{F}_{p^m}[x]/\langle (x-\xi)^{p^s}\rangle$, respectively.

Proof. Proof is trivial. □

Remark 4.4.1. Each $(\alpha + u\beta + u^2\delta)$-constacyclic code $\mathscr{C}$ of length $2p^s$ over $\mathscr{R}$ can be expressed as $\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2$, where $\mathscr{C}_j$ is an ideal of $\mathscr{K}_j$ for $j \in \{1,2\}$. By Proposition 4.4.1, we see that $\mathrm{Tor}_0(\mathscr{C})$, $\mathrm{Tor}_1(\mathscr{C})$ and $\mathrm{Tor}_2(\mathscr{C})$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x^2-\alpha_0)^{p^s}\rangle$, and that $\mathrm{Tor}_i(\mathscr{C}) = \mathrm{Tor}_i(\mathscr{C}_1) \oplus \mathrm{Tor}_i(\mathscr{C}_2)$ for $0 \le i \le 2$, where for $i \in \{0,1,2\}$, $\mathrm{Tor}_i(\mathscr{C}_1)$ and $\mathrm{Tor}_i(\mathscr{C}_2)$ are ideals of $\mathbb{F}_{p^m}[x]/\langle (x+\xi)^{p^s}\rangle$ and $\mathbb{F}_{p^m}[x]/\langle (x-\xi)^{p^s}\rangle$, respectively. Further, as $\mathbb{F}_{p^m}[x]/\langle (x+\xi)^{p^s}\rangle$ and $\mathbb{F}_{p^m}[x]/\langle (x-\xi)^{p^s}\rangle$ are finite commutative chain rings with the respective maximal ideals as $\langle x+\xi\rangle$ and $\langle x-\xi\rangle$, we have $\mathrm{Tor}_0(\mathscr{C}_1) = \langle (x+\xi)^{a_1}\rangle$, $\mathrm{Tor}_0(\mathscr{C}_2) = \langle (x-\xi)^{a_2}\rangle$, $\mathrm{Tor}_1(\mathscr{C}_1) = \langle (x+\xi)^{b_1}\rangle$, $\mathrm{Tor}_1(\mathscr{C}_2) = \langle (x-\xi)^{b_2}\rangle$, $\mathrm{Tor}_2(\mathscr{C}_1) = \langle (x+\xi)^{c_1}\rangle$ and $\mathrm{Tor}_2(\mathscr{C}_2) = \langle (x-\xi)^{c_2}\rangle$ for some integers $a_1, b_1, c_1, a_2, b_2, c_2$ satisfying $0 \le c_1 \le b_1 \le a_1 \le p^s$ and $0 \le c_2 \le b_2 \le a_2 \le p^s$. Now by applying the Chinese Remainder Theorem, we get $\mathrm{Tor}_0(\mathscr{C}) = \langle (x+\xi)^{a_1}(x-\xi)^{a_2}\rangle$, $\mathrm{Tor}_1(\mathscr{C}) = \langle (x+\xi)^{b_1}(x-\xi)^{b_2}\rangle$ and $\mathrm{Tor}_2(\mathscr{C}) = \langle (x+\xi)^{c_1}(x-\xi)^{c_2}\rangle$.

Now we proceed to determine Hamming distances of all non-zero $(\alpha + u\beta + u^2\delta)$-constacyclic codes of length $2p^s$ over $\mathscr{R}$. For this, we need the following theorem.

Theorem 4.4.1. [57] 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 $\xi \in \mathbb{F}_{p^m}$ such that $\omega_0 = \xi^2$. Now let $\mathscr{C}$ be a non-zero ω-constacyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$. Then we have $\mathscr{C} = \langle (x+\xi)^{\upsilon_1}(x-\xi)^{\upsilon_2}\rangle$, where $0 \le \upsilon_1, \upsilon_2 \le p^s$.

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

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

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

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

Moreover, the code $\mathscr{C}$ is an MDS Hamming 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 $\upsilon_2 = p^s$.

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

Theorem 4.4.2. Let $\mathscr{C}$ be a non-zero $(\alpha+u\beta+u^2\delta)$-constacyclic code of length $2p^s$ over $\mathscr{R}$ with $\text{Tor}_2(\mathscr{C}) = \langle (x+\xi)^{c_1}(x-\xi)^{c_2}\rangle$ for some integers c_1, c_2 satisfying $0 \le c_1, c_2 \le p^s$.

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

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

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

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

Proof. It follows immediately by applying Theorems 4.4.1 and 2.0.7(d). □

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

Theorem 4.4.3. Let $\mathscr{C}$ be an $(\alpha+u\beta+u^2\delta)$-constacyclic code of length $2p^s$ over $\mathscr{R}$ with $\text{Tor}_0(\mathscr{C}) = \langle (x+\xi)^{a_1}(x-\xi)^{a_2}\rangle$, $\text{Tor}_1(\mathscr{C}) = \langle (x+\xi)^{b_1}(x-\xi)^{b_2}\rangle$ and $\text{Tor}_2(\mathscr{C}) = \langle (x+\xi)^{c_1}(x-\xi)^{c_2}\rangle$ for some integers $a_1, b_1, c_1, a_2, b_2, c_2$ satisfying $0 \le c_1 \le b_1 \le a_1 \le p^s$ and $0 \le c_2 \le b_2 \le a_2 \le p^s$. Then the code $\mathscr{C}$ is an MDS Hamming code if and only if $a_1 = b_1 = c_1$, $a_2 = b_2 = c_2$ and $\text{Tor}_2(\mathscr{C})$ is an MDS Hamming α-constacyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$.

Proof. To prove the result, we see, by (4.4.1), that $\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2$, where $\mathscr{C}_j$ is an ideal of $\mathscr{K}_j$ for $j \in \{1, 2\}$. Further, by applying Proposition 4.4.1 and the Chinese Remainder Theorem, we get $\text{Tor}_0(\mathscr{C}_1) = \langle (x+\xi)^{a_1} \rangle$, $\text{Tor}_0(\mathscr{C}_2) = \langle (x-\xi)^{a_2} \rangle$, $\text{Tor}_1(\mathscr{C}_1) = \langle (x+\xi)^{b_1} \rangle$, $\text{Tor}_1(\mathscr{C}_2) = \langle (x-\xi)^{b_2} \rangle$, $\text{Tor}_2(\mathscr{C}_1) = \langle (x+\xi)^{c_1} \rangle$ and $\text{Tor}_2(\mathscr{C}_2) = \langle (x-\xi)^{c_2} \rangle$.

Now since $\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2$, by Lemma 4.2.3, we have

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

From this, we observe that the code $\mathscr{C}$ is MDS Hamming code if and only if

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

which holds if and only if

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

Next by Theorem 2.0.7(d), we see that the Hamming distance $d_H(\mathscr{C})$ of the code $\mathscr{C}$ is equal to the Hamming distance $d_H(\text{Tor}_2(\mathscr{C}))$ of the α-constacyclic code $\text{Tor}_2(\mathscr{C}) = \langle (x+\xi)^{c_1}(x-\xi)^{c_2} \rangle$ of length $2p^s$ over $\mathbb{F}_{p^m}$. Now by Theorem 2.0.1(a), we have $p^{m(2p^s - c_1 - c_2)} \leq p^{m(2p^s - d_H(\text{Tor}_2(\mathscr{C})) + 1)}$, which implies that $c_1 + c_2 + 1 \geq d_H(\text{Tor}_2(\mathscr{C})) = d_H(\mathscr{C})$. 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 $a_1 + a_2 + b_1 + b_2 + c_1 + c_2 + 3 \geq 3d_H(\mathscr{C})$, with the equality holds if and only if $a_1 = b_1 = c_1$, $a_2 = b_2 = c_2$ and $\text{Tor}_2(\mathscr{C})$ is an MDS Hamming code of length $2p^s$ over $\mathbb{F}_{p^m}$. This completes the proof of the theorem. □

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

Theorem 4.4.4. The following hold.

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

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

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

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

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

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

Proof. To prove the result, let $\mathscr{C}$ be a non-zero $(\alpha+u\beta+u^2\delta)$-constacyclic code of length $2p^s$ over $\mathscr{R}$ with $\mathrm{Tor}_0(\mathscr{C}) = \langle (x+\xi)^{a_1}(x-\xi)^{a_2}\rangle$, $\mathrm{Tor}_1(\mathscr{C}) = \langle (x+\xi)^{b_1}(x-\xi)^{b_2}\rangle$ and $\mathrm{Tor}_2(\mathscr{C}) = \langle (x+\xi)^{c_1}(x-\xi)^{c_2}\rangle$ 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 (4.4.1), we have $\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2$, where $\mathscr{C}_j$ is an ideal of $\mathscr{K}_j$ for $j \in \{1, 2\}$. Further, by applying Proposition 4.4.1 and the Chinese Remainder Theorem, we have $\mathrm{Tor}_0(\mathscr{C}_1) = \langle (x+\xi)^{a_1}\rangle$, $\mathrm{Tor}_0(\mathscr{C}_2) = \langle (x-\xi)^{a_2}\rangle$, $\mathrm{Tor}_1(\mathscr{C}_1) = \langle (x+\xi)^{b_1}\rangle$, $\mathrm{Tor}_1(\mathscr{C}_2) = \langle (x-\xi)^{b_2}\rangle$, $\mathrm{Tor}_2(\mathscr{C}_1) = \langle (x+\xi)^{c_1}\rangle$ and $\mathrm{Tor}_2(\mathscr{C}_2) = \langle (x-\xi)^{c_2}\rangle$.

By Theorem 4.4.3, we see that the code $\mathscr{C}$ is MDS Hamming code if and only if $a_1 = b_1 = c_1$, $a_2 = b_2 = c_2$ and $\mathrm{Tor}_2(\mathscr{C})$ is an MDS Hamming α-constacyclic code of length $2p^s$

over $\mathbb{F}_{p^m}$. 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 4.2.2(b), we note that $\langle (x+\xi)^{p^s} \rangle = \langle u \rangle$ in $\mathscr{K}_1$ and $\langle (x-\xi)^{p^s} \rangle = \langle u \rangle$ in $\mathscr{K}_2$. This implies that when $1 \leq a_1, a_2 \leq p^s - 1$, we have $u \in \mathscr{C}_1$ and $u \in \mathscr{C}_2$, which implies that $b_1 = c_1 = 0$ and $b_2 = c_2 = 0$. In view of this and by applying Theorems 4.4.3 and 4.4.1, we observe that the code $\mathscr{C}$ is MDS Hamming code if and only if $a_1 = b_1 = c_1 = 0$ and $a_2 = b_2 = c_2 = 0$. So the code $\mathscr{C} = \langle 1 \rangle$ is the only MDS Hamming $(\alpha + u\beta + u^2\delta)$-constacyclic code of length $2p^s$ over $\mathscr{R}$.

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

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

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

To do this, by Theorems 4.4.3 and 4.4.1, we observe that the code $\mathscr{C}$ is an MDS Hamming 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 $\mathscr{C}_2 = \{0\}$. As $a_1 = b_1 = c_1$, by Theorems 4.2.2 and 4.2.3, we observe that the code $\mathscr{C}_1$ must be of Type III. So we have $\mathscr{C} = \langle (x+\xi)^{a_1} + u(x+\xi)^{t_1}D_1(x) + u^2(x+\xi)^{t_2}D_2(x), u(x+\xi)^{a_1} + u^2(x+\xi)^{\theta}V(x), u^2(x+\xi)^{a_1} \rangle$, 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 $\mathscr{K}_1$ of the form $\sum_{k=0}^{a_1-t_1-1} C_k(x+\xi)^k$, $D_2(x)$ is either 0 or a unit in $\mathscr{K}_1$ of the form $\sum_{\ell=0}^{a_1-t_2-1} Q_\ell(x+\xi)^\ell$ and $V(x)$ is either 0 or a unit in $\mathscr{K}_1$ of the form $\sum_{i=0}^{a_1-\theta-1} W_i(x+\xi)^i$ with $C_k, Q_\ell, W_i \in \mathbb{F}_{p^m}$ for each relevant k, ℓ and i. Furthermore, by Theorems 4.2.2 and 4.2.3 again, we see that

$$u^2\{\delta(2\xi^{p^s})^{-1} + (x+\xi)^{p^s-2a_1+t_1+\theta}V(x)D_1(x) - (x+\xi)^{p^s-a_1+t_2}D_2(x)\} \in \langle u^2(x+\xi)^{a_1}\rangle. \tag{4.4.2}$$

We also note that $u^2\{(x+\xi)^{t_1}D_1(x) - (x+\xi)^\theta V(x)\} \in \langle u^2(x+\xi)^{a_1}\rangle$, which implies that $t_1 = \theta$ and $D_1(x) = V(x)$. From this and by (4.4.2), we get

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

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 $\delta \neq 0$. Hence we get a contradiction in this case when δ is non-zero.

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

□

Chapter 5

Repeated-root constacyclic codes of prime power lengths over finite commutative chain rings

5.1 Introduction

In this chapter, we shall determine all repeated-root constacyclic codes of prime power lengths over finite commutative chain rings. We shall also determine their symbol-pair distances, Rosenbloom-Tsfasman (RT) distances, and Rosenbloom-Tsfasman (RT) weight distributions. Using these results, we shall identify all MDS Hamming, MDS symbol-pair and MDS RT codes within this class of codes. Besides this, we shall provide an algorithm to decode these codes with respect to Hamming, symbol-pair and RT metrics.

For this, throughout this chapter, let s be a positive integer, and let $\mathcal{R}$ be a finite commutative chain ring with unity 1. Let γ be a generator of the maximal ideal of $\mathcal{R}$. Further, let e be the nilpotency index of γ, and let $\overline{\mathcal{R}} = \mathcal{R}/\langle\gamma\rangle$ be the residue field of $\mathcal{R}$. As $\overline{\mathcal{R}}$ is a finite field, let us suppose that $\overline{\mathcal{R}} \simeq \mathbb{F}_{p^m}$ for some prime p and for some positive integer m, where $\mathbb{F}_{p^m}$ is the finite field of order p^m.

This chapter is structured as follows: In Section 5.2, we derive necessary and sufficient conditions under which the quotient ring $\mathcal{R}[x]/\langle x^{p^s} - \lambda\rangle$ is a chain ring. When $\mathcal{R}[x]/\langle x^{p^s} - \lambda\rangle$ is a chain ring, all λ-constacyclic codes of length p^s over $\mathcal{R}$ are known. Here we establish algebraic structures of all λ-constacyclic codes of length p^s over $\mathcal{R}$ when $\mathcal{R}[x]/\langle x^{p^s} - \lambda\rangle$ is a non-chain ring. We also determine the number of codewords in each of these codes. In Section 5.3, we derive a necessary and sufficient condition for a constacyclic code of length p^s over $\mathcal{R}$ to be an MDS Hamming code. Using this result, we also list all MDS

Hamming constacyclic codes of length p^s over $\mathcal{R}$. In Section 5.4, we obtain symbol-pair distances of all constacyclic codes of length p^s over $\mathcal{R}$. We also derive a necessary and sufficient condition for a constacyclic code of length p^s over $\mathcal{R}$ to be an MDS symbol-pair code, and identify all MDS symbol-pair codes within this class of constacyclic codes. In Section 5.5, we determine Rosenbloom-Tsfasman (RT) distances and Rosenbloom-Tsfasman (RT) weight distributions of all constacyclic codes of length p^s over $\mathcal{R}$. We also derive a necessary and sufficient condition for a constacyclic code of length p^s over $\mathcal{R}$ to be an MDS RT code, and identify all MDS RT codes within this class of constacyclic codes. In Section 5.6, we provide an algorithm to decode constacyclic codes of length p^s over $\mathcal{R}$ with respect to Hamming, symbol-pair and RT metrics.

5.2 Algebraic structures of constacyclic codes of length p^s over $\mathcal{R}$

Throughout this chapter, let λ be a unit in $\mathcal{R}$. We recall that a λ-constacyclic code of length p^s over $\mathcal{R}$ is an ideal of the quotient ring $\mathcal{R}_\lambda = \mathcal{R}[x]/\langle x^{p^s} - \lambda\rangle$. By Theorem 2.0.6(c), the unit $\lambda \in \mathcal{R}$ can be uniquely expressed as $\lambda = \theta + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\theta, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\theta \neq 0$. When β_1 is non-zero, Dinh et al. [25] determined all λ-constacyclic codes of length p^s over $\mathcal{R}$ and their sizes, by showing that $\mathcal{R}_\lambda$ is a chain ring and by applying Theorem 2.0.5. In this section, we will show that the quotient ring $\mathcal{R}_\lambda$ is a chain ring if and only if β_1 is non-zero. We will also determine all λ-constacyclic codes of length p^s over $\mathcal{R}$ and their sizes when $\beta_1 = 0$. We will also obtain symbol-pair distances, RT distances and RT weight distributions of all constacyclic codes of length p^s over $\mathcal{R}$. Besides this, we will derive necessary and sufficient conditions under which a constacyclic code of length p^s over $\mathcal{R}$ is MDS with respect to the (i) Hamming metric, (ii) symbol-pair metric and (iii) RT metric. To do this, we first observe, by Theorem 2.0.6(b), that there exists $\lambda_0 \in \mathcal{T} \setminus \{0\}$ such that $\theta = \lambda_0^{p^s}$. This implies that $x^{p^s} - \lambda = x^{p^s} - \lambda_0^{p^s} - \gamma\beta_1 - \gamma^2\beta_2 - \cdots - \gamma^{e-1}\beta_{e-1}$. From this, it is easy to see that

$$(x - \lambda_0)^{p^s} \in \langle\gamma\rangle \quad \text{in} \quad \mathcal{R}_\lambda.$$

Now we make the following observation.

Remark 5.2.1. Let k be a positive integer, and let $\mathcal{S}$ be a subset of either $\mathcal{R}$ or $\overline{\mathcal{R}}$ such that $0 \in \mathcal{S}$. Let us recall that $\mathcal{P}_k(\mathcal{S}) = \{g(x) \in \mathcal{S}[x] : \text{either } g(x) = 0 \text{ or deg } g(x) < k\}$. By repeatedly applying the division algorithm in $\mathcal{R}[x]$, every element $A(x) \in \mathcal{R}_\lambda$ can be uniquely expressed as $A(x) = \sum_{i=0}^{p^s-1} A_i(x-\lambda_0)^i$, where $A_i \in \mathcal{R}$ for $0 \le i \le p^s - 1$. Further, by Theorem 2.0.6(c), each element $A_i \in \mathcal{R}$ can be uniquely written as $A_i = \sum_{j=0}^{e-1} \gamma^j A_{ij}$, where $A_{ij} \in \mathcal{T}$ for each i and j. From this, it follows that each element $A(x) \in \mathcal{R}_\lambda$ can be uniquely expressed as

$$A(x) = \sum_{j=0}^{e-1} \gamma^j \left(\sum_{i=0}^{p^s-1} A_{ij}(x-\lambda_0)^i \right),$$

where $A_{ij} \in \mathcal{T}$ for each i and j. From now on, we shall view the set $\mathcal{P}_k(\mathcal{T})$ as a subset of $\mathcal{R}_\lambda$ for each integer $k \ge 1$. It is easy to see that the restriction map of μ to $\mathcal{P}_{p^s}(\mathcal{T})$ (viewed as a subset of $\mathcal{R}_\lambda$) is a bijection from $\mathcal{P}_{p^s}(\mathcal{T})$ onto $\overline{\mathcal{R}}_\lambda$.

When $\beta_1 \neq 0$, Dinh et al. [25] determined all λ-constacyclic codes of length p^s over $\mathcal{R}$, which are listed in the following theorem.

Theorem 5.2.1. [25, Th. 3.18] Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1} \in \mathcal{R}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and both λ_0, β_1 are non-zero. Then we have the following:

(a) The ring $\mathcal{R}_\lambda = \mathcal{R}[x]/\langle x^{p^s} - \lambda\rangle$ is a finite commutative chain ring with the unique maximal ideal as $\langle x - \lambda_0\rangle$.

(b) In the ring $\mathcal{R}_\lambda$, we have $\langle (x-\lambda_0)^{p^s}\rangle = \langle\gamma\rangle$, and the nilpotency index of $x - \lambda_0$ is ep^s.

(c) All the distinct λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by $\langle (x-\lambda_0)^\nu\rangle$, where $0 \le \nu \le ep^s$. Moreover, for $0 \le \nu \le ep^s$, the code $\langle (x-\lambda_0)^\nu\rangle$ has $p^{m(ep^s-\nu)}$ codewords.

In the following theorem, we derive necessary and sufficient conditions for the quotient ring $\mathcal{R}_\lambda$ to be a chain ring.

Theorem 5.2.2. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Then the quotient ring $\mathcal{R}_\lambda = \mathcal{R}[x]/\langle x^{p^s} - \lambda\rangle$ is a chain ring if and only if

$\beta_1 \neq 0$.

Proof. By Lemma 3.1 and Proposition 3.3 of Dinh et al. [25], we see that $\mathcal{R}_\lambda$ is a local ring with the maximal ideal as $\mathcal{M} = \langle x - \lambda_0, \gamma \rangle$. Here we assert that the ideal $\mathcal{M}$ is principal if and only if $\beta_1 \neq 0$.

When $\beta_1 \neq 0$, by Theorem 5.2.1(b), we see that $\gamma \in \langle x - \lambda_0 \rangle$, which gives $\mathcal{M} = \langle x - \lambda_0 \rangle$.

Next let $\beta_1 = 0$. Here we will show that the ideal $\mathcal{M}$ is not principal, for which it is enough to show that $\gamma \notin \langle x - \lambda_0 \rangle$ and $(x - \lambda_0) \notin \langle \gamma \rangle$. For, if $\gamma \in \langle x - \lambda_0 \rangle$, then there exist polynomials $h_1(x), h_2(x) \in \mathcal{R}[x]$ such that $\gamma = (x - \lambda_0)h_1(x) + (x^{p^s} - \lambda)h_2(x)$ in $\mathcal{R}[x]$, which implies that $\gamma = -(\gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1})h_2(\lambda_0)$. This gives $\gamma \in \langle \gamma^2 \rangle$, which is a contradiction. On the other hand, if $x - \lambda_0 \in \langle \gamma \rangle$, then there exist polynomials $g_1(x), g_2(x) \in \mathcal{R}[x]$ such that $x - \lambda_0 = \gamma g_1(x) + (x^{p^s} - \lambda)g_2(x)$ in $\mathcal{R}[x]$. This implies that $x - \overline{\lambda}_0 = (x - \overline{\lambda}_0)^{p^s}\overline{g_2(x)}$ in $\overline{\mathcal{R}}[x]$, which is a contradiction.

Now by the above assertion and by applying Theorem 2.0.5, the desired result follows. □

The following theorem presents some results on torsion codes of a λ-constacyclic code of length p^s over $\mathcal{R}$.

Theorem 5.2.3. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. If $\mathcal{C}$ is a λ-constacyclic code of length p^s over $\mathcal{R}$, then we have the following:

(a) For $0 \leq i \leq e-1$, $\mathrm{Tor}_i(\mathcal{C})$ is a $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$. Furthermore, we have $\mathrm{Tor}_i(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_i} \rangle$, where T_i is an integer satisfying $0 \leq T_i \leq p^s$ for each i.

(b) $|\mathrm{Tor}_i(\mathcal{C})| = p^{m(p^s - T_i)}$ for $0 \leq i \leq e-1$.

(c) $p^s \geq T_0 \geq T_1 \geq \cdots \geq T_{e-1} \geq 0$.

(d) $|\mathcal{C}| = p^{m(ep^s - (T_0 + T_1 + \cdots + T_{e-1}))}$.

(For $0 \leq i \leq e-1$, the integer $T_i = T_i(\mathcal{C})$ is called the ith-torsional degree of the code $\mathcal{C}$.)

Proof. It is easy to see that $\mathrm{Tor}_i(\mathcal{C})$ is an ideal of the ring $\overline{\mathcal{R}}_\lambda$, i.e., $\mathrm{Tor}_i(\mathcal{C})$ is a $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$. Next we observe that the ring $\overline{\mathcal{R}}_\lambda$ is a finite commutative chain ring with the maximal ideal as $\langle x-\overline{\lambda}_0\rangle$. Now by applying Theorems 2.0.5(c) and 2.0.7(b)-(c), the desired result follows immediately. □

In the following theorem, we consider the case $\beta_1 = 0$, and we determine all λ-constacyclic codes of length p^s over $\mathcal{R}$ by obtaining unique generating sets for these codes.

Theorem 5.2.4. Let $\lambda = \lambda_0^{p^s} + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a λ-constacyclic code of length p^s over $\mathcal{R}$, and let $\mathrm{Tor}_i(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_i}\rangle$ be the ith torsion code of $\mathcal{C}$, where $0 \leq T_i \leq p^s$ for $0 \leq i \leq e-1$. Then the code $\mathcal{C}$ can be uniquely generated by the codewords $f_0(x), f_1(x), \cdots, f_{e-1}(x)$, where for $0 \leq i \leq e-1$,

$$f_i(x) = \gamma^i(x-\lambda_0)^{T_i} + \gamma^{i+1}(x-\lambda_0)^{t_{1,i}}g_{1,i}(x) + \gamma^{i+2}(x-\lambda_0)^{t_{2,i}}g_{2,i}(x) + \cdots + \gamma^{e-1}(x-\lambda_0)^{t_{e-1-i,i}}g_{e-1-i,i}(x)$$

with $0 \leq t_{j,i} < T_{j+i}$ if $g_{j,i}(x) \neq 0$, and $g_{j,i}(x) \in \mathcal{P}_{T_{j+i}-t_{j,i}}(\mathcal{T})$ as either 0 or a unit in $\mathcal{R}_\lambda$ for each j when $1 \leq T_i < p^s$; $f_i(x) = 0$ when $T_i = p^s$; and $f_i(x) = \gamma^i$ when $T_i = 0$.

Proof. To prove the result, let $\mathcal{C}$ be a non-zero λ-constacyclic code of length p^s over $\mathcal{R}$. Then there exists an integer k satisfying $0 \leq k \leq e-1$ and $T_k < p^s$. Here we observe that

$$\mathcal{C} = \langle \gamma^k(x-\lambda_0)^{T_k} + \gamma^{k+1}h_k(x), \gamma^{k+1}(x-\lambda_0)^{T_{k+1}} + \gamma^{k+2}h_{k+1}(x), \cdots, \gamma^{e-2}(x-\lambda_0)^{T_{e-2}} + \gamma^{e-1}h_{e-2}(x), \gamma^{e-1}(x-\lambda_0)^{T_{e-1}}\rangle$$

for some $h_k(x), h_{k+1}(x), \cdots, h_{e-2}(x) \in \mathcal{R}_\lambda$. By Remark 5.2.1, we can write $\gamma^{e-1}h_{e-2}(x) = \gamma^{e-1}\sum_{j=0}^{p^s-1} A_j(x-\lambda_0)^j$, where $A_j \in \mathcal{T}$ for each j. Now for all integers j satisfying $j \geq T_{e-1}$, we see that $\gamma^{e-1}(x-\lambda_0)^j \in \langle \gamma^{e-1}(x-\lambda_0)^{T_{e-1}}\rangle$. This implies that

$$\mathcal{C} = \langle \gamma^k(x-\lambda_0)^{T_k} + \gamma^{k+1}h_k(x), \gamma^{k+1}(x-\lambda_0)^{T_{k+1}} + \gamma^{k+2}h_{k+1}(x), \cdots, \gamma^{e-2}(x-\lambda_0)^{T_{e-2}} + \gamma^{e-1}\sum_{j=0}^{T_{e-1}-1} A_j(x-\lambda_0)^j, \gamma^{e-1}(x-\lambda_0)^{T_{e-1}}\rangle.$$

If $\gamma^{e-1}\sum_{j=0}^{T_{e-1}-1} A_j(x-\lambda_0)^j \neq 0$, then there exists a smallest integer $t_{1,e-2}$ satisfying $0 \leq t_{1,e-2} \leq T_{e-1}-1$ and $A_{t_{1,e-2}} \neq 0$, and we can write

$$\gamma^{e-1}\sum_{j=0}^{T_{e-1}-1} A_j(x-\lambda_0)^j = \gamma^{e-1}(x-\lambda_0)^{t_{1,e-2}} g_{1,e-2}(x),$$

where $g_{1,e-2}(x) = \sum_{j=t_{1,e-2}}^{T_{e-1}-1} A_j(x-\lambda_0)^{j-t_{1,e-2}}$ is a unit in $\mathcal{R}_\lambda$. This gives

$$\begin{aligned}\mathcal{C} = \langle &\gamma^k(x-\lambda_0)^{T_k} + \gamma^{k+1}h_k(x), \gamma^{k+1}(x-\lambda_0)^{T_{k+1}} + \gamma^{k+2}h_{k+1}(x), \cdots, \\ &\gamma^{e-2}(x-\lambda_0)^{T_{e-2}} + \gamma^{e-1}(x-\lambda_0)^{t_{1,e-2}} g_{1,e-2}(x), \gamma^{e-1}(x-\lambda_0)^{T_{e-1}}\rangle.\end{aligned}$$

Working in a similar manner with the rest of the generators of the code $\mathcal{C}$, one can show that

$$\mathcal{C} = \langle f_k(x), f_{k+1}(x), \cdots, f_{e-1}(x)\rangle,$$

where for $k \leq i \leq e-1$,

$$\begin{aligned}f_i(x) = \gamma^i(x-\lambda_0)^{T_i} + \gamma^{i+1}(x-\lambda_0)^{t_{1,i}} g_{1,i}(x) + \gamma^{i+2}(x-\lambda_0)^{t_{2,i}} g_{2,i}(x) \\ + \cdots + \gamma^{e-1}(x-\lambda_0)^{t_{e-1-i,i}} g_{e-1-i,i}(x)\end{aligned}$$

with $0 \leq t_{j,i} < T_{j+i}$ if $g_{j,i}(x) \neq 0$, and $g_{j,i}(x) \in \mathcal{P}_{T_{j+i}-t_{j,i}}(\mathcal{T})$ as either 0 or a unit in $\mathcal{R}_\lambda$ for each j when $1 \leq T_i < p^s$; $f_i(x) = 0$ when $T_i = p^s$; and $f_i(x) = \gamma^i$ when $T_i = 0$.

Now to prove the uniqueness part, let us suppose that

$$\mathcal{C} = \langle a_k(x), a_{k+1}(x), \cdots, a_{e-1}(x)\rangle,$$

where for $k \leq i \leq e-1$,

$$\begin{aligned}a_i(x) = \gamma^i(x-\lambda_0)^{T_i} + \gamma^{i+1}(x-\lambda_0)^{u_{1,i}} b_{1,i}(x) + \gamma^{i+2}(x-\lambda_0)^{u_{2,i}} b_{2,i}(x) \\ + \cdots + \gamma^{e-1}(x-\lambda_0)^{u_{e-1-i,i}} b_{e-1-i,i}(x)\end{aligned}$$

with $0 \leq u_{j,i} < T_{j+i}$ if $b_{j,i}(x) \neq 0$, and $b_{j,i}(x) \in \mathcal{P}_{T_{j+i}-u_{j,i}}(\mathcal{T})$ as either 0 or a unit in $\mathcal{R}_\lambda$ for each j when $1 \leq T_i < p^s$; $a_i(x) = 0$ when $T_i = p^s$; and $a_i(x) = \gamma^i$ when $T_i = 0$.

Here we assert that $f_i(x) = a_i(x)$ for $k \leq i \leq e-1$.

To prove this assertion, we first note that $f_{e-1}(x) = a_{e-1}(x)$. Further, since

$$f_{e-2}(x) - a_{e-2}(x) = \gamma^{e-1}\{(x-\lambda_0)^{t_{1,e-1}} g_{1,e-1}(x) - (x-\lambda_0)^{u_{1,e-1}} b_{1,e-1}(x)\} \in \mathcal{C},$$

we see that $f_{e-2}(x) - a_{e-2}(x)$ is either the zero polynomial or a non-zero polynomial of degree strictly less than T_{e-1} and $f_{e-2}(x) - a_{e-2}(x) \in \langle \gamma^{e-1}(x-\lambda_0)^{T_{e-1}} \rangle$. So we must have

$$f_{e-2}(x) = a_{e-2}(x).$$

Proceeding in a similar manner as above, one can show that $f_i(x) = a_i(x)$ for $k \leq i \leq e-3$.

This completes the proof of the theorem. □

Remark 5.2.2. When $\beta_1 \neq 0$, by Theorem 5.2.1(b) and (c), one can easily observe that all the distinct non-zero λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by $\mathcal{C}_{k,u} = \langle \gamma^k (x-\lambda_0)^u \rangle$, where $0 \leq k \leq e-1$ and $0 \leq u < p^s$. Further, we see that

$$\mathrm{Tor}_i(\mathcal{C}_{k,u}) = \begin{cases} \{0\} & \text{if } 0 \leq i < k; \\ \langle (x-\overline{\lambda}_0)^u \rangle & \text{if } i = k; \\ \overline{\mathcal{R}}_\lambda & \text{if } k < i \leq e-1. \end{cases}$$

This implies that the torsional degrees of $\mathcal{C}_{k,u}$ are given by $T_0 = T_1 = \cdots = T_{k-1} = p^s$, $T_k = u$ and $T_{k+1} = T_{k+2} = \cdots = T_{e-1} = 0$. In view of this and by applying Theorem 5.2.3(c), we observe that the code $\mathcal{C}_{k,u}$ can be uniquely generated by the codewords $f_0(x), f_1(x), \cdots, f_{e-1}(x)$, where $f_i(x) = 0$ for $0 \leq i \leq k-1$, $f_k(x) = \gamma^k (x-\lambda_0)^{T_k}$, and $f_j(x) = \gamma^j$ for $k+1 \leq j \leq e-1$.

To illustrate Theorem 5.2.4 and Remark 5.2.2, we determine all constacyclic codes of length p^s over the finite commutative chain ring $\mathbb{F}_{p^m}[\gamma]/\langle \gamma^2 \rangle$ as follows:

Example 5.2.1. Let $\mathcal{R} = \mathbb{F}_{p^m}[\gamma]/\langle \gamma^2 \rangle$. Here we see that $\mathcal{T} = \mathbb{F}_{p^m}$. Further, by Theorem 2.0.6(b) and (c), we see that a unit λ in $\mathcal{R}$ can be uniquely expressed as $\lambda = \lambda_0^{p^s} + \gamma\beta_1$,

where $\lambda_0, \beta_1 \in \mathbb{F}_{p^m}$ and $\lambda_0 \neq 0$.

When $\beta_1 \neq 0$, by Remark 5.2.2, all the distinct non-zero λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by $\langle (x-\lambda_0)^a, \gamma \rangle$ with $T_0 = a$, $T_1 = 0$, and by $\langle \gamma(x-\lambda_0)^a \rangle$ with $T_0 = p^s$, $T_1 = a$, where $0 \leq a \leq p^s - 1$.

When $\beta_1 = 0$, by Theorem 5.2.4, all the distinct non-zero λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by $\langle (x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x), \gamma(x-\lambda_0)^b \rangle$ with $T_0 = a$, $T_1 = b$, and by $\langle \gamma(x-\lambda_0)^b \rangle$ with $T_0 = p^s$, $T_1 = b$, where $0 \leq b \leq a \leq p^s - 1$, $0 \leq t < b$ if $g(x) \neq 0$, and $g(x) \in \mathcal{P}_{b-t}(\mathbb{F}_{p^m})$ is either 0 or a unit in $\mathcal{R}_\lambda$.

5.3 Determination of MDS Hamming codes

In this section, we shall determine all MDS Hamming constacyclic codes of length p^s over $\mathcal{R}$. For this, let $\mathcal{C}$ be a λ-constacyclic code of length p^s over $\mathcal{R}$. It is easy to see that $d_H(\mathcal{C}) = 0$ when $\mathcal{C} = \{0\}$, while $d_H(\mathcal{C}) = 1$ when $\mathcal{C} = \langle 1 \rangle$. In the following theorem, we determine Hamming distances of all non-trivial λ-constacyclic codes of length p^s over $\mathcal{R}$.

Theorem 5.3.1. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1\beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$ with $\mathrm{Tor}_{e-1}(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_{e-1}} \rangle$, where $0 \leq T_{e-1} < p^s$. Then the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is given by

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

Proof. It follows immediately from Theorems 2.0.7(d), 2.0.8 and 5.2.3(a). □

In the following theorem, we derive necessary and sufficient conditions for a λ-constacyclic code of length p^s over $\mathcal{R}$ to be an MDS Hamming code.

Theorem 5.3.2. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-zero λ-constacyclic code of length p^s over $\mathcal{R}$. Then the code $\mathcal{C}$ is an MDS Hamming code if and only if $\text{Tor}_0(\mathcal{C}) = \text{Tor}_{e-1}(\mathcal{C})$ and $\text{Tor}_0(\mathcal{C})$ is an MDS Hamming $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$.

Proof. To prove the result, let $\text{Tor}_i(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i < p^s$ for $0 \leq i \leq e-1$. Then by Theorem 5.2.3(d), we see that $|\mathcal{C}| = p^{m(ep^s - (T_0 + T_1 + \cdots + T_{e-1}))}$. Now the code $\mathcal{C}$ is an MDS Hamming code if and only if $p^{m(ep^s - (T_0 + T_1 + \cdots + T_{e-1}))} = |\mathcal{C}| = p^{me(p^s - d_H(\mathcal{C}) + 1)}$, which holds if and only if

$$T_0 + T_1 + \cdots + T_{e-1} = e\{d_H(\mathcal{C}) - 1\}.$$

By Theorem 2.0.7(d), we see that the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$ is equal to the Hamming distance of the $\overline{\lambda}_0^{p^s}$-constacyclic code $\text{Tor}_{e-1}(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_{e-1}} \rangle$ of length p^s over $\overline{\mathcal{R}}$. By Theorem 5.2.3(b), we have $|\text{Tor}_{e-1}(\mathcal{C})| = p^{m(p^s - T_{e-1})}$. Now by the Singleton bound for $\text{Tor}_{e-1}(\mathcal{C})$ with respect to the Hamming metric, we have $p^{m(p^s - T_{e-1})} \leq p^{m(p^s - d_H(\text{Tor}_{e-1}(\mathcal{C})) + 1)}$. This implies that $T_{e-1} \geq d_H(\text{Tor}_{e-1}(\mathcal{C})) - 1 = d_H(\mathcal{C}) - 1$. Further, by applying Theorem 5.2.3(c), we get $T_i \geq d_H(\mathcal{C}) - 1$ for each i. This implies that $T_0 + T_1 + \cdots + T_{e-1} \geq e\{d_H(\mathcal{C}) - 1\}$ and the equality holds if and only if $T_0 = T_1 = \cdots = T_{e-1} = d_H(\mathcal{C}) - 1$. From this, the desired result follows immediately. □

In the following corollary, we determine all MDS Hamming λ-constacyclic codes of length p^s over $\mathcal{R}$.

Corollary 5.3.1. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. The following hold.

(a) When $\beta_1 \neq 0$, the code $\mathcal{C} = \langle 1 \rangle$ is the only MDS Hamming λ-constacyclic code of length p^s over $\mathcal{R}$.

(b) When $\beta_1 = 0$, all the distinct MDS Hamming λ-constacyclic codes of length p over $\mathcal{R}$ are given by the principal ideals

$$\langle (x - \lambda_0)^{T_0} + \gamma(x - \lambda_0)^{t_{1,0}} g_{1,0}(x) + \gamma^2(x - \lambda_0)^{t_{2,0}} g_{2,0}(x) + \cdots + \gamma^{e-1}(x - \lambda_0)^{t_{e-1-i,0}} g_{e-1,0}(x) \rangle$$

with the ith-torsional degree as T_0 for $0 \leq i \leq e-1$, where $0 \leq T_0 \leq p-1$, $0 \leq t_{j,0} < T_0$ if $g_{j,0}(x) \neq 0$, and $g_{j,0}(x) \in \mathcal{P}_{T_0-t_{j,0}}(\mathcal{T})$ is either 0 or a unit in $\mathcal{R}_\lambda$ for $1 \leq j \leq e-1$.

(c) When $\beta_1 = 0$ and $s \geq 2$, all the distinct MDS Hamming λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by the principal ideals

$$\langle (x-\lambda_0)^{T_0} + \gamma(x-\lambda_0)^{t_{1,0}} g_{1,0}(x) + \gamma^2(x-\lambda_0)^{t_{2,0}} g_{2,0}(x) + \cdots + \gamma^{e-1}(x-\lambda_0)^{t_{e-1,0}} g_{e-1,0}(x) \rangle$$

with the ith-torsional degree as T_0 for $0 \leq i \leq e-1$, where $T_0 \in \{0, 1, p^s-1\}$, $0 \leq t_{j,0} < T_0$ if $g_{j,0}(x) \neq 0$, and $g_{j,0}(x) \in \mathcal{P}_{T_0-t_{j,0}}(\mathcal{T})$ is either 0 or a unit in $\mathcal{R}_\lambda$ for $1 \leq j \leq e-1$.

Proof. Let $\mathcal{C}$ be a λ-constacyclic code of length p^s over $\mathcal{R}$ with $\text{Tor}_i(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$ for each i. By applying Theorem 5.3.2, we see that the code $\mathcal{C}$ is an MDS Hamming code if and only if $\text{Tor}_0(\mathcal{C}) = \text{Tor}_{e-1}(\mathcal{C})$ and $\text{Tor}_0(\mathcal{C})$ is an MDS Hamming $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$. This implies that for the code $\mathcal{C}$ to be an MDS Hamming code, we must have $T_0 = T_{e-1} < p^s$.

Now we shall distinguish the following two cases: (i) $\beta_1 \neq 0$ and (ii) $\beta_1 = 0$.

(i) First let $\beta_1 \neq 0$. When $T_0 < p^s$, we see, by Remark 5.2.2, that $\mathcal{C} = \langle (x-\lambda_0)^{T_0} \rangle = \langle (x-\lambda_0)^{T_0}, \gamma, \gamma^2, \cdots, \gamma^{e-1} \rangle$, and that $T_1 = T_2 = \cdots = T_{e-1} = 0$. From this, we observe that the code $\mathcal{C}$ is an MDS Hamming code if and only if $T_0 = T_{e-1} = 0$, which holds if and only if $\mathcal{C} = \langle 1 \rangle$.

(ii) Next let $\beta_1 = 0$. Here we see that $\text{Tor}_0(\mathcal{C}) = \text{Tor}_{e-1}(\mathcal{C})$ if and only if $T_0 = T_{e-1}$. This, by Theorems 5.2.3(c) and 5.2.4, implies that $T_0 = T_1 = \cdots = T_{e-1}$ and that $\mathcal{C}$ is a principal ideal of the ring $\mathcal{R}_\lambda$. Further, by Theorem 5.2.3(a), we note that $\text{Tor}_0(\mathcal{C})$ is a $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$. Now by applying Theorem 2.0.8, we see that the code $\text{Tor}_0(\mathcal{C})$ is an MDS Hamming code if and only if

- $0 \leq T_0 \leq p-1$ when $s = 1$;

- $T_0 \in \{0, 1, p^s - 1\}$ when $s \geq 2$.

From this and by applying Theorem 5.2.4 again, we get the desired result.

□

To illustrate the above results, we determine all non-trivial MDS Hamming constacyclic codes of length p^s over the finite commutative chain ring $\mathbb{F}_{p^m}[\gamma]/\langle\gamma^2\rangle$ as follows:

Example 5.3.1. Let $\mathcal{R} = \mathbb{F}_{p^m}[\gamma]/\langle\gamma^2\rangle$. Recall that a unit $\lambda \in \mathcal{R}$ can be uniquely expressed as $\lambda = \lambda_0^{p^s} + \gamma\beta_1$, where $\lambda_0(\neq 0), \beta_1 \in \mathbb{F}_{p^m}$.

When $\beta_1 \neq 0$, by Corollary 5.3.1(a), we see that there does not exist any non-trivial MDS Hamming λ-constacyclic code of length p^s over $\mathcal{R}$.

Now let $\beta_1 = 0$. Here by Example 5.2.1, we see that a λ-constacyclic code $\mathcal{C}$ of length p^s over $\mathcal{R}$ is either of the type $\langle(x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x), \gamma(x-\lambda_0)^b\rangle$ with $T_0 = a$ and $T_1 = b$, or of the type $\langle\gamma(x-\lambda_0)^b\rangle$ with $T_0 = p^s$ and $T_1 = b$, where $0 \leq b \leq a \leq p^s - 1$, $0 \leq t < b$ if $g(x) \neq 0$, and $g(x) \in \mathcal{P}_{b-t}(\mathbb{F}_{p^m})$ is either 0 or a unit in $\mathcal{R}_\lambda$. When $\mathcal{C}$ is of the type $\langle(x-\lambda_0)^a+\gamma(x-\lambda_0)^t g(x), \gamma(x-\lambda_0)^b\rangle$ with $g(x) \neq 0$, we see that $\gamma(x-\lambda_0)^{p^s-a+t} g(x) \in \mathcal{C}$, which implies that $(x-\lambda_0)^{p^s-a+t} \in \mathrm{Tor}_1(\mathcal{C}) = \langle(x-\lambda_0)^b\rangle$. This implies that $p^s - a + t \geq b$ if $g(x) \neq 0$. From this and by Corollary 5.3.1(b), we see that when $s = 1$, all the distinct non-trivial MDS Hamming λ-constacyclic codes of length p over $\mathcal{R}$ are given by

$$\langle(x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x)\rangle,$$

where $1 \leq a \leq p-1$, $\max\{0, 2a-p\} \leq t < a$ if $g(x) \neq 0$, and either $g(x) = 0$ or $g(x) = \sum_{\ell=0}^{a-t-1} A_\ell(x-\lambda_0)^\ell$ with each $A_\ell \in \mathbb{F}_{p^m}$ and $A_0 \neq 0$. Further, by Corollary 5.3.1(c), we see that when $s \geq 2$, all the distinct non-trivial MDS Hamming λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by

$$\langle x - \lambda_0 + \gamma g\rangle \text{ and } \langle(x-\lambda_0)^{p^s-1} + \gamma(x-\lambda_0)^{p^s-2} g\rangle, \text{ where } g \in \mathbb{F}_{p^m}.$$

5.4 Determination of symbol-pair distances and MDS symbol-pair codes

In this section, we shall first determine symbol-pair distances of all λ-constacyclic codes of length p^s over $\mathcal{R}$. To do this, we need the following theorem.

Theorem 5.4.1. [24, Th. 4.13] Let η be a non-zero element of the finite field $\mathbb{F}_{p^m}$. Let $\mathcal{C}$ be an η-constacyclic code of length p^s over $\mathbb{F}_{p^m}$. Then there exists $\eta_0 \in \mathbb{F}_{p^m}$ satisfying $\eta = \eta_0^{p^s}$ and $\mathcal{C} = \langle (x-\eta_0)^{\upsilon} \rangle$, where υ is an integer satisfying $0 \leq \upsilon \leq p^s$. Furthermore, the symbol-pair distance of the code $\mathcal{C}$ is given by

$$d_{sp}(\mathcal{C}) = \begin{cases} 2 & \text{if } \upsilon = 0; \\ 3p^k & \text{if } \upsilon = p^s - p^{s-k} + 1, \text{ where } 0 \leq k \leq s-2; \\ 4p^k & \text{if } p^s - p^{s-k} + 2 \leq \upsilon \leq p^s - p^{s-k} + p^{s-k+1}, \text{ where } 0 \leq k \leq s-2; \\ 2(\tau+2)p^k & \text{if } p^s - p^{s-k} + \tau p^{s-k-1} + 1 \leq \upsilon \leq p^s - p^{s-k} + (\tau+1)p^{s-k-1}, \\ & \text{where } 0 \leq k \leq s-2 \text{ and } 1 \leq \tau \leq p-2; \\ (\tau+2)p^{s-1} & \text{if } \upsilon = p^s - p + \tau, \text{ where } 1 \leq \tau \leq p-2; \\ p^s & \text{if } \upsilon = p^s - 1; \\ 0 & \text{if } \upsilon = p^s. \end{cases}$$

Now let $\mathcal{C}$ be a λ-constacyclic code of length p^s over $\mathcal{R}$. It is easy to see that $d_{sp}(\mathcal{C}) = 0$ when $\mathcal{C} = \{0\}$, while $d_{sp}(\mathcal{C}) = 2$ when $\mathcal{C} = \langle 1 \rangle$. In the following theorem, we determine symbol-pair distances of all non-trivial λ-constacyclic codes of length p^s over $\mathcal{R}$.

Theorem 5.4.2. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$ with $\text{Tor}_{e-1}(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_{e-1}} \rangle$, where $0 \leq T_{e-1} < p^s$. Then the symbol-pair distance $d_{sp}(\mathcal{C})$ of the code $\mathcal{C}$ is

given by

$$d_{sp}(\mathcal{C}) = \begin{cases} 2 & \text{if } T_{e-1} = 0; \\ 3p^k & \text{if } T_{e-1} = p^s - p^{s-k} + 1 \text{ with } 0 \le k \le s-2; \\ 4p^k & \text{if } p^s - p^{s-k} + 2 \le T_{e-1} \le p^s - p^{s-k} + p^{s-k+1} \text{ with } 0 \le k \\ & \le s-2; \\ 2(\tau+2)p^k & \text{if } p^s - p^{s-k} + \tau p^{s-k-1} + 1 \le T_{e-1} \le p^s - p^{s-k} + (\tau+1)p^{s-k-1} \\ & \text{with } 0 \le k \le s-2 \text{ and } 1 \le \tau \le p-2; \\ (\tau+2)p^{s-1} & \text{if } T_{e-1} = p^s - p + \tau \text{ with } 1 \le \tau \le p-2; \\ p^s & \text{if } T_{e-1} = p^s - 1. \end{cases}$$

Proof. To prove the result, we assert that

$$d_{sp}(\mathcal{C}) = d_{sp}(\text{Tor}_{e-1}(\mathcal{C})). \tag{5.4.1}$$

Towards this, we first note that $\text{Tor}_{e-1}(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_{e-1}} \rangle$. This implies that $\langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle \subseteq \mathcal{C}$, from which it follows that

$$d_{sp}(\langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle) \ge d_{sp}(\mathcal{C}). \tag{5.4.2}$$

Next we observe that

$$w_{sp}(Q(x)) \ge w_{sp}(\gamma Q(x)) \text{ for each } Q(x) \in \mathcal{R}_\lambda. \tag{5.4.3}$$

Further, for any non-zero codeword $Q(x) \in \mathcal{C}$, there exists an integer i, $0 \le i \le e-1$, such that $Q(x) \in \langle \gamma^i \rangle \setminus \langle \gamma^{i+1} \rangle$. Now using (5.4.3), we get

$$w_{sp}(Q(x)) \ge w_{sp}(\gamma Q(x)) \ge w_{sp}(\gamma^2 Q(x)) \ge \cdots \ge w_{sp}(\gamma^{e-1-i} Q(x)). \tag{5.4.4}$$

It is easy to observe that $\gamma^{e-1-i}Q(x) (\neq 0) \in \langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle$, which implies that $w_{sp}(\gamma^{e-1-i}Q(x)) \ge d_{sp}(\langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle)$. From this and by (5.4.4), we obtain

$$w_{sp}(Q(x)) \ge d_{sp}(\langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle) \quad \text{for each} \quad Q(x) \in \mathcal{C} \setminus \{0\},$$

which implies that

$$d_{sp}(\mathcal{C}) \geq d_{sp}(\langle \gamma^{e-1}(x-\lambda_0)^{T_{e-1}} \rangle). \tag{5.4.5}$$

Now by (5.4.2) and (5.4.5), we get

$$d_{sp}(\mathcal{C}) = d_{sp}(\langle \gamma^{e-1}(x-\lambda_0)^{T_{e-1}} \rangle). \tag{5.4.6}$$

Further, we observe that $d_{sp}(\langle \gamma^{e-1}(x-\lambda_0)^{T_{e-1}} \rangle)$ is equal to the symbol-pair distance of the $\overline{\lambda}_0^{p^s}$-constacyclic code $\text{Tor}_{e-1}(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_{e-1}} \rangle$ of length p^s over $\overline{\mathcal{R}}$. From this, the desired assertion follows immediately.

Finally, by the above assertion and by applying Theorem 5.4.1, we get the desired result. □

In the following theorem, we derive necessary and sufficient conditions for a λ-constacyclic code of length p^s over $\mathcal{R}$ to be an MDS symbol-pair code.

Theorem 5.4.3. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-zero λ-constacyclic code of length p^s over $\mathcal{R}$. Then the code $\mathcal{C}$ is an MDS symbol-pair code if and only if $\text{Tor}_0(\mathcal{C}) = \text{Tor}_{e-1}(\mathcal{C})$ and $\text{Tor}_0(\mathcal{C})$ is an MDS symbol-pair $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$.

Proof. To prove the result, let $\text{Tor}_i(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$ for $0 \leq i \leq e-1$. Further, by Theorem 5.2.3(a), we see that $\text{Tor}_{e-1}(\mathcal{C})$ is a $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$. By the Singleton bound for $\text{Tor}_{e-1}(\mathcal{C})$ with respect to the symbol-pair metric and by applying Theorem 5.2.3(b) and using (5.4.1), we get

$$p^{m(p^s-T_{e-1})} = |\text{Tor}_{e-1}(\mathcal{C})| \leq p^{m(p^s-d_{sp}(\text{Tor}_{e-1}(\mathcal{C}))+2)} = p^{m(p^s-d_{sp}(\mathcal{C})+2)},$$

which gives $T_{e-1} \geq d_{sp}(\mathcal{C}) - 2$. This, by Theorem 5.2.3(c), implies that

$$T_i \geq d_{sp}(\mathcal{C}) - 2 \text{ for } 0 \leq i \leq e-1. \tag{5.4.7}$$

Further, by Theorem 5.2.3(d), we see that the code $\mathcal{C}$ is an MDS symbol-pair code if and only if $p^{m(ep^s-(T_0+T_1+\cdots+T_{e-1}))} = |\mathcal{C}| = p^{me(p^s-d_{sp}(\mathcal{C})+2)}$, which holds if and only if

$T_0 + T_1 + \cdots + T_{e-1} = e\{d_{sp}(\mathcal{C}) - 2\}$ and by (5.4.7), the equality holds if and only if $T_0 = T_1 = \cdots = T_{e-1} = d_{sp}(\mathcal{C}) - 2$. From this, the desired result follows immediately. □

In the following corollary, we determine all MDS symbol-pair λ-constacyclic codes of length p^s over $\mathcal{R}$.

Corollary 5.4.1. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. The following hold.

(a) When $\beta_1 \neq 0$, the code $\mathcal{C} = \langle 1 \rangle$ is the only MDS symbol-pair λ-constacyclic code of length p^s over $\mathcal{R}$.

(b) When $\beta_1 = 0$, all the distinct MDS symbol-pair λ-constacyclic codes of length p over $\mathcal{R}$ are given by the principal ideals

$$\langle (x-\lambda_0)^{T_0} + \gamma(x-\lambda_0)^{t_{1,0}} g_{1,0}(x) + \gamma^2(x-\lambda_0)^{t_{2,0}} g_{2,0}(x) + \cdots + \gamma^{e-1}(x-\lambda_0)^{t_{e-1,0}} g_{e-1,0}(x) \rangle$$

with the ith-torsional degree as T_0 for $0 \leq i \leq e-1$, where $0 \leq T_0 \leq p-2$, $0 \leq t_{j,0} < T_0$ if $g_{j,0}(x) \neq 0$, and $g_{j,0}(x) \in \mathcal{P}_{T_0 - t_{j,0}}(\mathcal{T})$ is either 0 or a unit in $\mathcal{R}_\lambda$ for $1 \leq j \leq e-1$.

(c) When $\beta_1 = 0$ and $s \geq 2$, all the distinct MDS symbol-pair λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by the principal ideals

$$\langle (x-\lambda_0)^{T_0} + \gamma(x-\lambda_0)^{t_{1,0}} g_{1,0}(x) + \gamma^2(x-\lambda_0)^{t_{2,0}} g_{2,0}(x) + \cdots + \gamma^{e-1}(x-\lambda_0)^{t_{e-1,0}} g_{e-1,0}(x) \rangle$$

with the ith-torsional degree as T_0 for $0 \leq i \leq e-1$, where $T_0 \in \{0, 1, 2, 4, 7\}$ if $p^s = 9$, while $T_0 \in \{0, 1, 2, p^s - 2\}$ if $p^s \neq 9$, $0 \leq t_{j,0} < T_0$ if $g_{j,0}(x) \neq 0$, and $g_{j,0}(x) \in \mathcal{P}_{T_0 - t_{j,0}}(\mathcal{T})$ is either 0 or a unit in $\mathcal{R}_\lambda$ for $1 \leq j \leq e-1$.

Proof. Let $\mathcal{C}$ be a λ-constacyclic code of length p^s over $\mathcal{R}$ with $\mathrm{Tor}_i(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i < p^s$ for each i. By applying Theorem 5.4.3, we see that the code $\mathcal{C}$ is an MDS symbol-pair code if and only if $\mathrm{Tor}_0(\mathcal{C}) = \mathrm{Tor}_{e-1}(\mathcal{C})$ and $\mathrm{Tor}_0(\mathcal{C})$ is an MDS symbol-pair

$\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$. This implies that for the code $\mathcal{C}$ to be an MDS symbol-pair code, we must have $T_0 < p^s$.

Now we shall distinguish the following two cases: (i) $\beta_1 \neq 0$ and (ii) $\beta_1 = 0$.

(i) First let $\beta_1 \neq 0$. When $T_0 < p^s$, we see, by Remark 5.2.2, that $\mathcal{C} = \langle (x-\lambda_0)^{T_0} \rangle = \langle (x-\lambda_0)^{T_0}, \gamma, \gamma^2, \cdots, \gamma^{e-1} \rangle$, and that $T_1 = T_2 = \cdots = T_{e-1} = 0$. From this, we observe that the code $\mathcal{C}$ is an MDS symbol-pair code if and only if $T_0 = T_{e-1} = 0$, which holds if and only if $\mathcal{C} = \langle 1 \rangle$.

(ii) Next let $\beta_1 = 0$. In this case, we see that $\mathrm{Tor}_0(\mathcal{C}) = \mathrm{Tor}_{e-1}(\mathcal{C})$ if and only if $T_0 = T_{e-1}$. This, by Theorems 5.2.3(c) and 5.2.4, implies that $T_0 = T_1 = \cdots = T_{e-1}$ and that $\mathcal{C}$ is a principal ideal of the ring $\mathcal{R}_\lambda$. Further, by Theorem 5.2.3(a), we note that $\mathrm{Tor}_0(\mathcal{C})$ is a $\overline{\lambda}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$. Now by Theorem 5.2 of Dinh et al. [24], we see that the code $\mathrm{Tor}_0(\mathcal{C})$ is an MDS symbol-pair code if and only if

- $0 \leq T_0 \leq p-2$ when $s = 1$;
- $T_0 \in \{0, 1, 2, 4, 7\}$ when $p = 3$ and $s = 2$;
- $T_0 \in \{0, 1, 2, p^s - 2\}$ when $s \geq 2$ and $p^s \neq 9$.

From this and by applying Theorem 5.2.4 again, the desired result follows.

□

To illustrate the above results, we determine all non-trivial MDS symbol-pair constacyclic codes of length p^s over the finite commutative chain ring $\mathbb{F}_{p^m}[\gamma]/\langle \gamma^2 \rangle$ as follows:

Example 5.4.1. Let $\mathcal{R} = \mathbb{F}_{p^m}[\gamma]/\langle \gamma^2 \rangle$. Recall that a unit $\lambda \in \mathcal{R}$ can be uniquely expressed as $\lambda = \lambda_0^{p^s} + \gamma\beta_1$, where $\lambda_0 (\neq 0), \beta_1 \in \mathbb{F}_{p^m}$.

When $\beta_1 \neq 0$, by Corollary 5.4.1(a), we see that there does not exist any non-trivial MDS symbol-pair λ-constacyclic code of length p^s over $\mathcal{R}$.

Now let $\beta_1 = 0$. Here by Example 5.2.1, we see that a λ-constacyclic code $\mathcal{C}$ of length p^s over $\mathcal{R}$ is either of the type $\langle (x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x), \gamma(x-\lambda_0)^b \rangle$ with $T_0 = a$,

$T_1 = b$, or of the type $\langle \gamma(x-\lambda_0)^b \rangle$ with $T_0 = p^s$, $T_1 = b$, where $0 \leq b \leq a \leq p^s - 1$, $0 \leq t < b$ if $g(x) \neq 0$, and $g(x) \in \mathcal{P}_{b-t}(\mathbb{F}_{p^m})$ is either 0 or a unit in $\mathcal{R}_\lambda$. When $\mathcal{C}$ is of the type $\langle (x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x), \gamma(x-\lambda_0)^b \rangle$ with $g(x) \neq 0$, we see that $\gamma(x-\lambda_0)^{p^s-a+t} g(x) \in \mathcal{C}$, which implies that $(x-\lambda_0)^{p^s-a+t} \in \mathrm{Tor}_1(\mathcal{C}) = \langle (x-\lambda_0)^b \rangle$. This implies that $p^s - a + t \geq b$ in the case when $g(x) \neq 0$. From this and by Corollary 5.4.1(b), we see that when $s = 1$, all the distinct non-trivial MDS symbol-pair λ-constacyclic codes of length p over $\mathcal{R}$ are given by

$$\langle (x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x) \rangle,$$

where $1 \leq a \leq p-2$, $\max\{0, 2a-p\} \leq t < a$ if $g(x) \neq 0$, and either $g(x) = 0$ or $g(x) = \sum_{\ell=0}^{a-t-1} A_\ell (x-\lambda_0)^\ell$ with each $A_\ell \in \mathbb{F}_{p^m}$ and $A_0 \neq 0$. Further, by Corollary 5.4.1(c), we see that when $s \geq 2$ and $p^s \neq 9$, all the distinct non-trivial MDS symbol-pair λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by

$$\langle x-\lambda_0+\gamma g_1 \rangle, \langle (x-\lambda_0)^{p^s-2} + \gamma(x-\lambda_0)^{p^s-3} g_1 \rangle \text{ and } \langle (x-\lambda_0)^{p^s-2} + \gamma(x-\lambda_0)^{p^s-4} g(x) \rangle,$$

where $g_1 \in \mathbb{F}_{p^m}$ and $g(x) = A_0 + A_1(x-\lambda_0)$ with $A_0 (\neq 0), A_1 \in \mathbb{F}_{p^m}$. Furthermore, by Corollary 5.4.1(c), we see that all the distinct non-trivial MDS symbol-pair λ-constacyclic codes of length 9 over $\mathcal{R}$ are given by

$$\langle (x-\lambda_0)^4 \rangle, \langle (x-\lambda_0)^7 \rangle, \langle x-\lambda_0+\gamma g_1 \rangle \text{ and } \langle (x-\lambda_0)^4 + \gamma(x-\lambda_0)^t g(x) \rangle,$$

where $g_1 \in \mathbb{F}_{p^m}$, $0 \leq t \leq 3$ and $g(x) = \sum_{\ell=0}^{4-t-1} A_\ell (x-\lambda_0)^\ell$ with each $A_\ell \in \mathbb{F}_{p^m}$ and $A_0 \neq 0$.

5.5 Determination of RT distances, RT weight distributions and MDS RT codes

In this section, we shall first determine RT distances of all λ-constacyclic codes of length p^s over $\mathcal{R}$. For this, let $\mathcal{C}$ be a λ-constacyclic code of length p^s over $\mathcal{R}$. It is easy to see that $d_{RT}(\mathcal{C}) = 0$ when $\mathcal{C} = \{0\}$, while $d_{RT}(\mathcal{C}) = 1$ when $\mathcal{C} = \langle 1 \rangle$. In the following theorem, we determine RT distances of all non-trivial λ-constacyclic codes of length p^s over $\mathcal{R}$.

Theorem 5.5.1. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$ with $\text{Tor}_{e-1}(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_{e-1}} \rangle$, where $0 \leq T_{e-1} < p^s$. Then the RT distance $d_{RT}(\mathcal{C})$ of the code $\mathcal{C}$ is given by

$$d_{RT}(\mathcal{C}) = T_{e-1} + 1.$$

Proof. To prove the result, we first observe that $w_{RT}(Q(x)) \geq w_{RT}(\gamma Q(x))$ for each $Q(x)(\neq 0) \in \mathcal{R}_\lambda$. Now working in a similar manner as in the proof of (5.4.6), we get $d_{RT}(\mathcal{C}) = d_{RT}(\langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle)$. Further, we note that

$$\langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle = \{\gamma^{e-1}(x - \lambda_0)^{T_{e-1}} A(x) \ : \ A(x) \in \mathcal{P}_{p^s - T_{e-1}}(\mathcal{T})\},$$

from which it follows that $d_{RT}(\langle \gamma^{e-1}(x - \lambda_0)^{T_{e-1}} \rangle) = T_{e-1} + 1$. This gives $d_{RT}(\mathcal{C}) = T_{e-1} + 1$. □

In the following theorem, we derive necessary and sufficient conditions for a λ-constacyclic code of length p^s over $\mathcal{R}$ to be an MDS RT code.

Theorem 5.5.2. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-zero λ-constacyclic code of length p^s over $\mathcal{R}$. Then the code $\mathcal{C}$ is an MDS RT code if and only if $\text{Tor}_0(\mathcal{C}) = \text{Tor}_{e-1}(\mathcal{C})$.

Proof. To prove the result, let $\text{Tor}_i(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$ for $0 \leq i \leq e-1$. Then by Theorem 5.2.3(d), we see that $|\mathcal{C}| = p^{m(ep^s - (T_0 + T_1 + \cdots + T_{e-1}))}$. Now the code $\mathcal{C}$ is an MDS RT code if and only if $p^{m(ep^s - (T_0 + T_1 + \cdots + T_{e-1}))} = |\mathcal{C}| = p^{me(p^s - d_{RT}(\mathcal{C}) + 1)}$, which holds if and only if

$$T_0 + T_1 + \cdots + T_{e-1} = e\{d_{RT}(\mathcal{C}) - 1\}. \tag{5.5.1}$$

By Theorem 5.5.1, we note that $d_{RT}(\mathcal{C}) = T_{e-1} + 1$. Further, by Theorem 5.2.3(c), we see that $p^s \geq T_0 \geq T_1 \geq \cdots \geq T_{e-1} \geq 0$. From this and by (5.5.1), we see that the code $\mathcal{C}$ is an MDS RT code if and only if $T_0 + T_1 + \cdots + T_{e-1} = eT_{e-1}$, which holds if and only if $T_0 = T_1 = \cdots = T_{e-1}$. From this, we get the desired result. □

In the following corollary, we determine all MDS RT λ-constacyclic codes of length p^s over $\mathcal{R}$.

Corollary 5.5.1. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. The following hold.

(a) When $\beta_1 \neq 0$, the code $\mathcal{C} = \langle 1 \rangle$ is the only MDS RTλ-constacyclic code of length p^s over $\mathcal{R}$.

(b) When $\beta_1 = 0$, all the distinct MDS RT λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by the principal ideals

$$\langle (x-\lambda_0)^{T_0} + \gamma(x-\lambda_0)^{t_{1,0}} g_{1,0}(x) + \gamma^2(x-\lambda_0)^{t_{2,0}} g_{2,0}(x) + \cdots + \gamma^{e-1}(x-\lambda_0)^{t_{e-1,0}} g_{e-1,0}(x) \rangle$$

with the ith-torsional degree as T_0 for $0 \leq i \leq e-1$, where $0 \leq T_0 \leq p^s - 1$, $0 \leq t_{j,0} < T_0$ if $g_{j,0}(x) \neq 0$, and $g_{j,0}(x) \in \mathcal{P}_{T_0 - t_{j,0}}(\mathcal{T})$ is either 0 or a unit in $\mathcal{R}_\lambda$ for $1 \leq j \leq e-1$.

Proof. By Theorem 5.5.2, we see that a λ-constacyclic code $\mathcal{C}$ of length p^s over $\mathcal{R}$ is an MDS RT code if and only if $\mathrm{Tor}_0(\mathcal{C}) = \mathrm{Tor}_{e-1}(\mathcal{C})$, which, by Theorem 5.2.3(c), holds if and only if all the torsional degrees of the code $\mathcal{C}$ are equal. From this and by applying Theorem 5.2.4 and Remark 5.2.2, we get the desired result. □

To illustrate the above results, we determine all non-trivial MDS RT constacyclic codes of length p^s over the finite commutative chain ring $\mathbb{F}_{p^m}[\gamma]/\langle\gamma^2\rangle$ as follows:

Example 5.5.1. Let $\mathcal{R} = \mathbb{F}_{p^m}[\gamma]/\langle\gamma^2\rangle$. Recall that a unit $\lambda \in \mathcal{R}$ can be uniquely expressed as $\lambda = \lambda_0^{p^s} + \gamma\beta_1$, where $\lambda_0 (\neq 0), \beta_1 \in \mathbb{F}_{p^m}$.

When $\beta_1 \neq 0$, by Corollary 5.5.1(a), we see that there does not exist any non-trivial MDS RT λ-constacyclic code of length p^s over $\mathcal{R}$.

Now let $\beta_1 = 0$. Here by Example 5.2.1, we see that a λ-constacyclic code $\mathcal{C}$ of length p^s over $\mathcal{R}$ is either of the type $\langle (x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x), \gamma(x-\lambda_0)^b \rangle$ with $T_0 = a$, $T_1 = b$, or of the type $\langle \gamma(x-\lambda_0)^b \rangle$ with $T_0 = p^s$, $T_1 = b$, where $0 \leq b \leq a \leq p^s - 1$,

$0 \leq t < b$ if $g(x) \neq 0$, and $g(x) \in \mathcal{P}_{b-t}(\mathbb{F}_{p^m})$ is either 0 or a unit in $\mathcal{R}_\lambda$. When $\mathcal{C}$ is of the type $\langle (x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x), \gamma(x-\lambda_0)^b \rangle$ with $g(x) \neq 0$, we see that $\gamma(x-\lambda_0)^{p^s-a+t} g(x) \in \mathcal{C}$, which implies that $(x-\lambda_0)^{p^s-a+t} \in \mathrm{Tor}_1(\mathcal{C}) = \langle (x-\lambda_0)^b \rangle$. This shows that $p^s - a + t \geq b$ in the case when $g(x) \neq 0$. From this and by Corollary 5.5.1(b), we see that all the distinct non-trivial MDS RT λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by

$$\langle (x-\lambda_0)^a + \gamma(x-\lambda_0)^t g(x) \rangle,$$

where $1 \leq a \leq p^s - 1$, $\max\{0, 2a - p^s\} \leq t < a$ if $g(x) \neq 0$, and either $g(x) = 0$ or $g(x) = \sum_{\ell=0}^{a-t-1} A_\ell (x-\lambda_0)^\ell$ with each $A_\ell \in \mathbb{F}_{p^m}$ and $A_0 \neq 0$.

In a recent work, Dinh et al. [23] determined all $(4z-1)$-constacyclic codes of length 2^s over the Galois ring $GR(2^e, m)$, where $z \in GR(2^e, m)$. As $GR(2^e, m)$ is a chain ring with the maximal ideal as $\langle 2 \rangle$, the unit $4z - 1 \in GR(2^e, m)$ can be rewritten as $4z - 1 = 1 + 2 + 4(z-1)$, i.e., $\beta_1 = 1$ for a unit λ of the form $4z-1$ for each $z \in GR(2^e, m)$. In the same work, Dinh et al. [23] determined RT weight distributions of all $(4z-1)$-constacyclic codes of length 2^s over the Galois ring $GR(2^e, m)$ (see [23, Prop. 6.3-6.5]). However, we noticed an error in Proposition 6.5 of Dinh et al. [23], which we illustrate in the following example.

Example 5.5.2. Let $GR(4, 1) = \mathbb{Z}_4$ be the Galois ring of characteristic 4 and cardinality 4, and let $\lambda = 3$. By Theorem 3.3 of Dinh et al. [23], we see that all the distinct 3-constacyclic codes of length 4 over $GR(4, 1)$ are ideals of quotient ring $GR(4, 1)[x]/\langle x^4 - 3 \rangle$ and are given by $\langle (x+1)^i \rangle$, where $0 \leq i \leq 8$.

For the code $\mathcal{C}_1 = \langle x + 1 \rangle$, by Proposition 6.5 of Dinh et al. [23], we obtain $\mathcal{A}_0 = 1$, $\mathcal{A}_1 = 1$, $\mathcal{A}_2 = 18$, $\mathcal{A}_3 = 36$ and $\mathcal{A}_4 = 72$. However, by carrying out computations in Magma, we see that the actual values of $\mathcal{A}_2$, $\mathcal{A}_3$ and $\mathcal{A}_4$ are given by $\mathcal{A}_2 = 6$, $\mathcal{A}_3 = 24$ and $\mathcal{A}_4 = 96$, which do not agree with Proposition 6.5 of Dinh et al. [23].

Moreover, for the code $\mathcal{C}_2 = \langle (x+1)^2 \rangle$, by Proposition 6.5 of Dinh et al. [23], we obtain $\mathcal{A}_0 = 1$, $\mathcal{A}_1 = 1$, $\mathcal{A}_2 = 2$, $\mathcal{A}_3 = 20$ and $\mathcal{A}_4 = 40$. However, by carrying out computations in Magma, we see that the actual values of $\mathcal{A}_3$ and $\mathcal{A}_4$ are given by $\mathcal{A}_3 = 12$ and $\mathcal{A}_4 = 48$. This shows that there is an error in Proposition 6.5 of Dinh et al. [23].

Now we proceed to determine RT weight distributions of all λ-constacyclic codes of length p^s over $\mathcal{R}$. To do so, we first prove the following lemma.

Lemma 5.5.1. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$ with $\text{Tor}_i(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$. Further, let $\{f_0(x), f_1(x), \cdots, f_{e-1}(x)\}$ be the unique generating set of the code $\mathcal{C}$ (as determined in Theorem 5.2.4 when $\beta_1 = 0$ and Remark 5.2.2 when $\beta_1 \neq 0$). Then each codeword $C(x) \in \mathcal{C}$ can be uniquely written as

$$C(x) = C_0(x)f_0(x) + C_1(x)f_1(x) + \cdots + C_{e-1}(x)f_{e-1}(x),$$

where $C_j(x) \in \mathcal{P}_{p^s - T_j}(\mathcal{T})$ for $0 \leq j \leq e-1$.

Proof. To prove the result, we consider the set

$$\mathcal{S} = \{A_0(x)f_0(x) + A_1(x)f_1(x) + \cdots + A_{e-1}(x)f_{e-1}(x) : A_j(x) \in \mathcal{P}_{p^s - T_j}(\mathcal{T}) \text{ for } 0 \leq j \leq e-1\},$$

and we assert that $\mathcal{S} = \mathcal{C}$.

To prove the assertion, we first note that $\mathcal{S} \subseteq \mathcal{C}$, and hence it is sufficient to show that $|\mathcal{S}| = |\mathcal{C}|$. Towards this, suppose that there exist $A_j(x), B_j(x) \in \mathcal{P}_{p^s - T_j}(\mathcal{T})$, $0 \leq j \leq e-1$, satisfying

$$\begin{aligned} &A_0(x)f_0(x) + A_1(x)f_1(x) + \cdots + A_{e-1}(x)f_{e-1}(x) \\ &\quad = B_0(x)f_0(x) + B_1(x)f_1(x) + \cdots + B_{e-1}(x)f_{e-1}(x) \in \mathcal{S}. \end{aligned}$$

This implies that

$$\gamma^{e-1}A_0(x)f_0(x) = \gamma^{e-1}B_0(x)f_0(x),$$

which further implies that

$$\gamma^{e-1}(x - \lambda_0)^{T_0}\{A_0(x) - B_0(x)\} = \gamma^{e-1}f_0(x)\{A_0(x) - B_0(x)\} = 0 \text{ in } \mathcal{R}_\lambda.$$

This holds if and only if $(x - \overline{\lambda}_0)^{T_0}\mu(A_0(x) - B_0(x)) = 0$ in $\overline{\mathcal{R}}_\lambda$, which holds if and

only if $\mu(A_0(x)) = \mu(B_0(x))$, as $A_0(x), B_0(x) \in \mathcal{P}_{p^s-T_0}(\mathcal{T})$. Further, as μ is a bijection from $\mathcal{P}_{p^s}(\mathcal{T})(\subseteq \mathcal{R}_\lambda)$ onto $\overline{\mathcal{R}}_\lambda$, we get $A_0(x) = B_0(x)$. Proceeding like this, we see that $A_j(x) = B_j(x)$ for $2 \leq j \leq e-1$. This shows that all the elements in the set S are distinct, which implies that

$$|\mathcal{S}| = p^{m(ep^s-(T_0+T_1+\cdots+T_{e-1}))} = |\mathcal{C}|,$$

by Theorem 5.2.3(c). From this, the desired result follows. □

In the following theorem, we rectify errors in Proposition 6.5 of Dinh et al. [23], and we obtain RT weight distributions of all λ-constacyclic codes of length p^s over $\mathcal{R}$.

Theorem 5.5.3. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$ with $\mathrm{Tor}_i(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$ for $0 \leq i \leq e-1$. Let us define $T_{-1} = p^s$. Then there exists a unique integer k satisfying $0 \leq k \leq e-1$, $T_{k-1} = p^s$ and $T_k < p^s$. If $\mathcal{A}_\rho$ denotes the number of codewords in $\mathcal{C}$ having the RT weight as ρ for $0 \leq \rho \leq p^s$, then

$$\mathcal{A}_\rho = \begin{cases} 1 & \text{if } \rho = 0; \\ 0 & \text{if } 1 \leq \rho \leq T_{e-1}; \\ (p^{m(e-\ell)}-1)p^{m\{(e-\ell)(\rho-1)-(T_\ell+T_{\ell+1}+\cdots+T_{e-1})\}} & \text{if } T_\ell + 1 \leq \rho \leq T_{\ell-1} \text{ with} \\ & k \leq \ell \leq e-1. \end{cases}$$

Proof. Note that $\mathcal{A}_0 = 1$. Further, by Theorem 5.5.1, we see that $d_{RT}(\mathcal{C}) = T_{e-1} + 1$, which implies that $\mathcal{A}_\rho = 0$ for $1 \leq \rho \leq T_{e-1}$. So from now on, we assume that $T_{e-1} + 1 \leq \rho \leq p^s$. As $T_{k-1} = p^s$ and $p^s \geq T_0 \geq T_1 \geq \cdots \geq T_{e-1} \geq 0$, we get $T_0 = T_1 = \cdots = T_{k-1} = p^s$. Then by Remark 5.2.2 and Theorem 5.2.4, we have

$$\mathcal{C} = \langle f_k(x), f_{k+1}(x), \cdots, f_{e-1}(x) \rangle,$$

where $f_k(x) = \gamma^k(x-\lambda_0)^{T_k}$ and $f_j(x) = \gamma^j$ for $k+1 \leq j \leq e-1$ when $\beta_1 \neq 0$; while for $k \leq i \leq e-1$, $f_i(x) = \gamma^i$ if $T_i = 0$ and $f_i(x) = \gamma^i(x-\lambda_0)^{T_i} + \gamma^{i+1}(x-\lambda_0)^{t_{1,i}}g_{1,i}(x) + \gamma^{i+2}(x-\lambda_0)^{t_{2,i}}g_{2,i}(x) + \cdots + \gamma^{e-1}(x-\lambda_0)^{t_{e-1-i,i}}g_{e-1-i,i}(x)$ with each $g_{j,i}(x) \in \mathcal{P}_{T_{j+i}-t_{j,i}}(\mathcal{T})$ as either 0 or a unit in $\mathcal{R}_\lambda$ if $1 \leq T_i < p^s$ when $\beta_1 = 0$. Further, by Lemma 5.5.1, we see

that each codeword $Q(x) \in \mathcal{C}$ can be uniquely expressed as

$$Q(x) = C_k(x)f_k(x) + C_{k+1}(x)f_{k+1}(x) + \cdots + C_{e-1}(x)f_{e-1}(x), \tag{5.5.2}$$

where $C_j(x) \in \mathcal{P}_{p^s-T_j}(\mathcal{T})$ for $k \leq j \leq e-1$. Moreover, we note that

$$w_{RT}(C_j(x)f_j(x)) = T_j + 1 + \text{ deg } C_j(x) \text{ if } C_j(x) \neq 0. \tag{5.5.3}$$

By (5.5.2) and (5.5.3), we see that if $T_{e-1} + 1 \leq \rho \leq T_{e-2}$, then the RT weight of the codeword $Q(x) \in \mathcal{C}$ is ρ if and only if deg $C_{e-1}(x) = \rho - T_{e-1} - 1$ and $C_j(x) = 0$ for $k \leq j \leq e-2$. This implies that $\mathcal{A}_\rho = (p^m - 1)p^{m(\rho - T_{e-1}-1)}$ for $T_{e-1} + 1 \leq \rho \leq T_{e-2}$.

Next let $T_\ell + 1 \leq \rho \leq T_{\ell-1}$, where $k \leq \ell \leq e-2$. Here by (5.5.2) and (5.5.3), we see that the RT weight of the codeword $Q(x) \in \mathcal{C}$ is ρ if and only if $C_j(x) = 0$ for $k \leq j \leq \ell - 1$ and exactly one of the following $(e - \ell)$ conditions is satisfied:

deg $C_\ell(x) = \rho - T_\ell - 1$ and $C_j(x) \in \mathcal{P}_{\rho-T_j}(\mathcal{T})$ for $\ell + 1 \leq j \leq e-1$; **(1)**

deg $C_{\ell+1}(x) = \rho - T_{\ell+1} - 1$, $C_\ell(x) \in \mathcal{P}_{\rho-T_\ell-1}(\mathcal{T})$ and $C_j(x) \in \mathcal{P}_{\rho-T_j}(\mathcal{T})$ for $\ell + 2 \leq j \leq e-1$; **(2)**

deg $C_{\ell+2}(x) = \rho - T_{\ell+2} - 1$, $C_\ell(x) \in \mathcal{P}_{\rho-T_\ell-1}(\mathcal{T}), C_{\ell+1}(x) \in \mathcal{P}_{\rho-T_{\ell+1}-1}(\mathcal{T})$ and $C_j(x) \in \mathcal{P}_{\rho-T_j}(\mathcal{T})$ for $\ell + 3 \leq j \leq e-1$; **(3)**

. . . . . .

. . . . . .

deg $C_{e-2}(x) = \rho - T_{e-2} - 1$, $C_j(x) \in \mathcal{P}_{\rho-T_j-1}(\mathcal{T})$for $\ell \leq j \leq e-3$ and $C_{e-1}(x) \in \mathcal{P}_{\rho-T_{e-1}}(\mathcal{T})$; **$(e - \ell - 1)$**

deg $C_{e-1}(x) = \rho - T_{e-1} - 1$ and $C_j(x) \in \mathcal{P}_{\rho-T_j-1}(\mathcal{T})$ for $\ell \leq j \leq e-2$. **$(e - \ell)$**

From this, we obtain

$$\mathcal{A}_\rho = (p^{m(e-\ell)} - 1)p^{m\{(e-\ell)(\rho-1)-(T_\ell+T_{\ell+1}+\cdots+T_{e-1})\}}$$

for $T_\ell + 1 \leq \rho \leq T_{\ell-1}$, where $k \leq \ell \leq e-2$.

This completes the proof of the theorem. □

5.6 A decoding algorithm for constacyclic codes of length p^s over finite commutative chain rings

Several decoding algorithms are known for linear codes over finite fields with respect to Hamming, symbol-pair and RT metrics (see [13, 37, 39, 54, 68, 81]). In this section, we shall provide an algorithm to decode constacyclic codes of length p^s over $\mathcal{R}$ using the already known decoding algorithms of linear codes of length p^s over the finite field $\overline{\mathcal{R}}$ with respect to these three metrics.

Throughout this section, by a metric, we mean either the Hamming metric or the symbol-pair metric or the RT metric. Likewise, by the weight of a vector, we mean either the Hamming weight or the symbol-pair weight or the RT weight.

Now let $\mathcal{C}$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$ with $\mathrm{Tor}_i(\mathcal{C}) = \langle (x-\overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$ for each i. Let $\{f_0(x), f_1(x), \cdots, f_{e-1}(x)\}$ be the unique generating set of the code $\mathcal{C}$ as determined in Theorem 5.2.4 and Remark 5.2.2. Let $C(x) \in \mathcal{C}$ be the transmitted codeword and let $W(x) \in \mathcal{R}_\lambda$ be the received vector with the error pattern as $E(x) \in \mathcal{R}_\lambda$. Then we have

$$W(x) = C(x) + E(x).$$

Further, both $W(x), E(x) \in R_\lambda$ can be uniquely written as

$$W(x) = W_0(x) + \gamma W_1(x) + \gamma^2 W_2(x) + \cdots + \gamma^{e-1} W_{e-1}(x)$$

and

$$E(x) = E_0(x) + \gamma E_1(x) + \gamma^2 E_2(x) + \cdots + \gamma^{e-1} E_{e-1}(x),$$

where $W_i(x), E_i(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ for each i. We say that the error pattern $E(x) = E_0(x) + \gamma E_1(x) + \gamma^2 E_2(x) + \cdots + \gamma^{e-1} E_{e-1}(x) \in \mathcal{R}_\lambda$ is of the type $(\delta_0, \delta_1, \cdots, \delta_{e-1})$ if the weight of $E_j(x)$ is at most δ_j for $0 \leq j \leq e-1$.

Then the following theorem provides a decoding algorithm for non-trivial constacyclic codes of length p^s over $\mathcal{R}$.

Theorem 5.6.1. Let $\lambda = \lambda_0^{p^s} + \gamma\beta_1 + \gamma^2\beta_2 + \cdots + \gamma^{e-1}\beta_{e-1}$, where $\lambda_0, \beta_1, \beta_2, \cdots, \beta_{e-1} \in \mathcal{T}$ and $\lambda_0 \neq 0$. Let $\mathcal{C}$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$ with $\text{Tor}_i(\mathcal{C}) = \langle (x - \overline{\lambda}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$ for each i. If $\text{Tor}_i(\mathcal{C})$ can correct errors with weight less than or equal to η_i for each i, then the code $\mathcal{C}$ can correct all error patterns of the type $(\eta_0, \eta_1, \cdots, \eta_{e-1})$.

Proof. Let $C(x) \in \mathcal{C}$ be the transmitted codeword and let $W(x) \in \mathcal{R}_\lambda$ be the received vector with the error pattern as $E(x) \in \mathcal{R}_\lambda$. Note that $W(x) = C(x) + E(x)$. Further, suppose that the error pattern $E(x)$ is of the type $(\eta_0, \eta_1, \cdots, \eta_{e-1})$. Then both $W(x), E(x)$ can be uniquely written as $W(x) = W_0(x) + \gamma W_1(x) + \gamma^2 W_2(x) + \cdots + \gamma^{e-1} W_{e-1}(x)$ and $E(x) = E_0(x) + \gamma E_1(x) + \gamma^2 E_2(x) + \cdots + \gamma^{e-1} E_{e-1}(x)$, where $W_j(x), E_j(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ for $0 \leq j \leq e-1$. Further, by Lemma 5.5.1, we see that $C(x) \in \mathcal{C}$ can be uniquely written as

$$C(x) = C_0(x)f_0(x) + C_1(x)f_1(x) + \cdots + C_{e-1}(x)f_{e-1}(x),$$

where $C_j(x) \in \mathcal{P}_{p^s - T_j}(\mathcal{T})$ for $0 \leq j \leq e-1$.

Given the polynomials $W_0(x), W_1(x), \cdots, W_{e-1}(x) \in \mathcal{P}_{p^s}(\mathcal{T})$, our aim is to determine $C_0(x), C_1(x), \cdots, C_{e-1}(x)$ satisfying $C_j(x) \in \mathcal{P}_{p^s - T_j}(\mathcal{T})$ for $0 \leq j \leq e-1$.

Towards this, we shall first determine $C_0(x) \in \mathcal{P}_{p^s - T_0}(\mathcal{T})$ and $E_0(x) \in \mathcal{P}_{p^s}(\mathcal{T})$. Since $W(x) = C(x) + E(x)$, we have $\gamma^{e-1}W(x) = \gamma^{e-1}C(x) + \gamma^{e-1}E(x)$. From this, we get $\gamma^{e-1}\{W_0(x) - E_0(x)\} = \gamma^{e-1}C_0(x)(x - \lambda_0)^{T_0}$, which implies that $\mu(W_0(x)) - \mu(E_0(x)) = \mu(C_0(x))(x - \overline{\lambda}_0)^{T_0} \in \text{Tor}_{e-1}(\mathcal{C}) \cap \text{Tor}_0(\mathcal{C}) = \text{Tor}_0(\mathcal{C})$. Now as $\text{Tor}_0(\mathcal{C})$ can correct all errors with weight at most η_0 and the weight of $\mu(E_0(x))$ is less than or equal to η_0, $\mu(W_0(x))$ can be uniquely decoded to $\mu(C_0(x))(x - \overline{\lambda}_0)^{T_0}$ in $\text{Tor}_0(\mathcal{C})$. From this and using the fact

that μ is a bijection from $\mathcal{P}_{p^s}(\mathcal{T})(\subseteq \mathcal{R}_\lambda)$ onto $\overline{\mathcal{R}}_\lambda$, the polynomials $C_0(x) \in \mathcal{P}_{p^s-T_0}(\mathcal{T})$ and $E_0(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ can be uniquely determined.

Next let i be a fixed integer satisfying $1 \leq i \leq e-1$. Suppose that $C_j(x) \in \mathcal{P}_{p^s-T_j}(\mathcal{T})$ and $E_j(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ are known for $0 \leq j \leq i-1$.

Now we shall determine $C_i(x) \in \mathcal{P}_{p^s-T_i}(\mathcal{T})$ and $E_i(x) \in \mathcal{P}_{p^s}(\mathcal{T})$. For this, we see that $\gamma^{e-i-1}W(x) = \gamma^{e-i-1}C(x) + \gamma^{e-i-1}E(x)$, which gives

$$\begin{aligned}\gamma^{e-i-1}W(x) &= \gamma^{e-i-1}C_0(x)f_0(x) + \gamma^{e-i-1}C_1(x)f_1(x) + \cdots + \gamma^{e-i-1}C_{i-1}(x)f_{i-1}(x)\\ &+\gamma^{e-i-1}C_i(x)f_i(x) + \gamma^{e-i-1}E_0(x) + \gamma^{e-i}E_1(x) + \cdots + \gamma^{e-2}E_{i-1}(x) + \gamma^{e-1}E_i(x).\end{aligned} \tag{5.6.1}$$

Let us define

$$\begin{aligned}\hat{W}_i(x) &= \gamma^{e-i-1}W(x) - \gamma^{e-i-1}C_0(x)f_0(x) - \gamma^{e-i-1}C_1(x)f_1(x) - \cdots\\ &-\gamma^{e-i-1}C_{i-1}(x)f_{i-1}(x) - \gamma^{e-i-1}E_0(x) - \gamma^{e-i}E_1(x) - \cdots - \gamma^{e-2}E_{i-1}(x).\end{aligned}$$

By (5.6.1), we see that $\hat{W}_i(x) = \gamma^{e-i-1}C_i(x)f_i(x) + \gamma^{e-1}E_i(x) \in \langle\gamma^{e-1}\rangle$, and hence $\hat{W}_i(x)$ can be uniquely written as $\hat{W}_i(x) = \gamma^{e-1}W_i^*(x)$ for some $W_i^*(x) \in \mathcal{P}_{p^s}(\mathcal{T})$. From this, we get $\hat{W}_i(x) - \gamma^{e-1}E_i(x) = \gamma^{e-1}W_i^*(x) - \gamma^{e-1}E_i(x) = \gamma^{e-i-1}C_i(x)f_i(x) = \gamma^{e-1}C_i(x)(x-\lambda_0)^{T_i} \in \mathcal{C}$, which implies that $\mu(W_i^*(x)) - \mu(E_i(x)) = \mu(C_i(x))(x-\overline{\lambda}_0)^{T_i} \in \mathrm{Tor}_{e-1}(\mathcal{C}) \cap \mathrm{Tor}_i(\mathcal{C}) = \mathrm{Tor}_i(\mathcal{C})$. Now as $\mathrm{Tor}_i(\mathcal{C})$ can correct all errors with weight at most η_i and the weight of $\mu(E_i(x))$ is less than or equal to η_i, $\mu(W_i^*(x))$ can be uniquely decoded to $\mu(C_i(x))(x-\overline{\lambda}_0)^{T_i}$ in $\mathrm{Tor}_i(\mathcal{C})$. From this and using the fact that μ is a bijection from $\mathcal{P}_{p^s}(\mathcal{T})(\subseteq \mathcal{R}_\lambda)$ onto $\overline{\mathcal{R}}_\lambda$, the polynomials $C_i(x) \in \mathcal{P}_{p^s-T_i}(\mathcal{T})$ and $E_i(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ can be uniquely determined.

This completes the proof of the theorem. □

The above theorem gives rise to the following decoding algorithm for non-trivial constacyclic codes of length p^s over $\mathcal{R}$.

A decoding algorithm for constacyclic codes of length p^s over $\mathcal{R}$

Suppose that for $0 \leq i \leq e-1$, there exists a decoding algorithm $\mathfrak{D}_i$ for $\text{Tor}_i(\mathcal{C})$ that can correct errors with weight at most η_i. Now suppose that the codeword $C(x) \in \mathcal{C}$ is transmitted, the vector $W(x) \in \mathcal{R}_\lambda$ is received, and that the error pattern $E(x)$ in the transmission is of the type $(\eta_0, \eta_1, \cdots, \eta_{e-1})$.

I. Apply the decoding algorithm $\mathfrak{D}_0$ for the code $\text{Tor}_0(\mathcal{C})$ over the finite field $\overline{R}$ to determine the codeword $D_0(x) \in \text{Tor}_0(\mathcal{C})$ and the error pattern $F_0(x)$ from $\mu(W(x))$ in $\overline{\mathcal{R}}_\lambda$.

II. Using the bijection μ from $\mathcal{P}_{p^s}(\mathcal{T})(\subseteq \mathcal{R}_\lambda)$ onto $\overline{\mathcal{R}}_\lambda$, determine $C_0(x) \in \mathcal{P}_{p^s-T_0}(\mathcal{T})$ and $E_0(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ satisfying $(x-\overline{\lambda}_0)^{T_0}\mu(C_0(x)) = D_0(x)$ and $\mu(E_0(x)) = F_0(x)$.

III. Now for $i = 1, 2, \cdots, e-1$, do the following steps:

   a. Given $W(x) \in \mathcal{R}_\lambda$, $E_j(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ and $C_j(x) \in \mathcal{P}_{p^s-T_j}(\mathcal{T})$ for $0 \leq j \leq i-1$, determine $W_i^*(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ satisfying

$$\gamma^{e-1}W_i^*(x) = \gamma^{e-i-1}W(x) - \gamma^{e-i-1}C_0(x)f_0(x) - \gamma^{e-i-1}C_1(x)f_1(x) - \cdots$$
$$-\gamma^{e-i-1}C_{i-1}(x)f_{i-1}(x) - \gamma^{e-i-1}E_0(x) - \gamma^{e-i}E_1(x) - \cdots - \gamma^{e-2}E_{i-1}(x).$$

   b. Apply the decoding algorithm $\mathfrak{D}_i$ for the code $\text{Tor}_i(\mathcal{C})$ over $\overline{\mathcal{R}}$ to determine the codeword $D_i(x) \in \text{Tor}_i(\mathcal{C})$ and the error pattern $F_i(x)$ from $\mu(W_i^*(x))$ in $\overline{\mathcal{R}}_\lambda$.

   c. Using the bijection μ from $\mathcal{P}_{p^s}(\mathcal{T})(\subseteq \mathcal{R}_\lambda)$ onto $\overline{\mathcal{R}}_\lambda$, determine $C_i(x) \in \mathcal{P}_{p^s-T_i}(\mathcal{T})$ and $E_i(x) \in \mathcal{P}_{p^s}(\mathcal{T})$ satisfying $(x-\overline{\lambda}_0)^{T_i}\mu(C_i(x)) = D_i(x)$ and $\mu(E_i(x)) = F_i(x)$.

IV. Decode the received vector $W(x) \in \mathcal{R}_\lambda$ to the codeword $C(x) = C_0(x)f_0(x) + C_1(x)f_1(x) + \cdots + C_{e-1}(x)f_{e-1}(x)$ in $\mathcal{C}$.

In the following example, we illustrate the above decoding algorithm with respect to the Hamming metric.

Example 5.6.1. Let $\mathcal{R} = \mathbb{F}_3[\gamma]/\langle\gamma^2\rangle$. Here we note that $\mathcal{T} = \mathbb{F}_3$ and that $\mu(f(x)) = f(x)$ for each $f(x) \in \mathbb{F}_3[x]/\langle x^9 - 2\rangle$. In view of Example 5.2.1, let $\mathcal{C} = \langle (x-2)^8, \gamma(x-2)^7\rangle$ be a 2-constacyclic code of length 9 over $\mathcal{R}$. Here we observe that $\mathrm{Tor}_0(\mathcal{C}) = \langle (x-2)^8\rangle$ and $\mathrm{Tor}_1(\mathcal{C}) = \langle (x-2)^7\rangle$. By Theorems 2.0.8 and 5.2.3(a), we get $d_H(\mathrm{Tor}_0(\mathcal{C})) = 9$ and $d_H(\mathrm{Tor}_1(\mathcal{C})) = 6 = d_H(\mathcal{C})$. Using the syndrome decoding algorithm, the code $\mathrm{Tor}_0(\mathcal{C})$ can correct all errors with Hamming weight at most 4, while the code $\mathrm{Tor}_1(\mathcal{C})$ can correct all errors with Hamming weight at most 2 (see Section 4.8.3 of [54]). Further, we see, by Lemma 5.5.1, that each codeword $C(x) \in \mathcal{C}$ can be uniquely expressed as $C(x) = C_0(x-2)^8 + \gamma C_1(x)(x-2)^7$, where $C_0 \in \mathbb{F}_3$ and $C_1(x) \in \mathcal{P}_2(\mathbb{F}_3)$.

Now suppose that a codeword $C(x) = C_0(x-2)^8+\gamma C_1(x)(x-2)^7 \in \mathcal{C}$, with $C_0 \in \mathbb{F}_3$ and $C_1(x) \in \mathcal{P}_2(\mathbb{F}_3)$, is transmitted. Suppose that the vector $W(x) = (2+2\gamma)x^8 + (1+2\gamma)x^7 + (2+2\gamma)x^6+(1+2\gamma)x^5+2x^4+(2+\gamma)x^3+(1+\gamma)x^2+2x+(1+2\gamma) \in \mathcal{R}_2 = \mathcal{R}[x]/\langle x^9-2\rangle$ is received, and that the error pattern $E(x)$ in the transmission is of the type $(4, 2)$. Our aim is to decode the vector $W(x)$ to the codeword $C(x) \in \mathcal{C}$, i.e., to determine $C_0 \in \mathbb{F}_3$ and $C_1(x) \in \mathcal{P}_2(\mathbb{F}_3)$.

I. By applying the syndrome decoding algorithm for $\mathrm{Tor}_0(\mathcal{C})$ to the vector $\mu(W(x)) = 2x^8 + x^7 + 2x^6 + x^5 + 2x^4 + 2x^3 + x^2 + 2x + 1 \in \mathbb{F}_3[x]/\langle x^9 - 2\rangle$ using Magma, we get $D_0(x) = 2x^8 + x^7 + 2x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 2 \in \mathrm{Tor}_0(\mathcal{C})$ and $F_0(x) = x^3 + 2x^2 + x + 2$.

II. The element $C_0 \in \mathbb{F}_3$ satisfying $C_0(x-2)^8 = 2x^8 + x^7 + 2x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 2 = 2(x-1)^8$ is given by $C_0 = 2$. Further, we have $E_0(x) = \mu(E_0(x)) = F_0(x) = x^3 + 2x^2 + x + 2$.

III. a. The vector $W_1^*(x) \in \mathbb{F}_3[x]/\langle x^9-2\rangle$ satisfying $\gamma W_1^*(x) = W(x) - C_0(x)f_0(x) - E_0(x) = \gamma(2x^8 + 2x^7 + 2x^6 + 2x^5 + x^3 + x^2 + 2)$ is given by $W_1^*(x) = 2x^8 + 2x^7 + 2x^6 + 2x^5 + x^3 + x^2 + 2$.

b. Now by applying the syndrome decoding algorithm for $\mathrm{Tor}_1(\mathcal{C})$ to the vector $W_1^*(x)$ using Magma, we get $D_1(x) = x^8 + 2x^6 + 2x^5 + x^3 + x^2 + 2$ and $F_1(x) = x^8 + 2x^7$.

c. The vector $C_1(x) \in \mathcal{P}_2(\mathbb{F}_3)$ satisfying $(x-2)^7 C_1(x) = D_1(x)$ is given by $C_1(x) = 2 + x$.

IV. Decode $W(x)$ to the codeword $C(x) = 2(x-2)^8 + \gamma(2+x)(x-2)^7 = (2+\gamma)x^8 + x^7 + (2+2\gamma)x^6 + (1+2\gamma)x^5 + 2x^4 + (1+\gamma)x^3 + (2+\gamma)x^2 + x + (2+2\gamma) \in \mathcal{C}$.

Remark 5.6.1. (a) The decoding algorithm proposed in this chapter works for all those metrics with respect to which decoding algorithms for linear codes over finite fields are known.

(b) All the results obtained in this chapter can be extended for λ-constacyclic codes of length np^s over $\mathcal{R}$, where n is a positive integer such that the binomial $x^n - \overline{\lambda}_0$ is irreducible over $\overline{\mathcal{R}}$.

Chapter 6

On b-symbol distances of repeated-root constacyclic codes

6.1 Introduction

In this chapter, we obtain b-symbol distances of all repeated-root constacyclic codes of prime power lengths over finite fields. Using this result, we determine b-symbol distances of all repeated-root constacyclic codes of prime power lengths over finite commutative chain rings. We also identify all MDS b-symbol repeated-root constacyclic codes of prime power lengths over finite fields, and all MDS b-symbol repeated-root constacyclic codes of prime power lengths over finite commutative chain rings in general.

For this, throughout this chapter, let p be a prime, s be a positive integer, and let b be an integer satisfying $2 \leq b < p^s$. This chapter is organized as follows: In Section 6.2, we state some basic definitions and results that are needed to derive our main results. In Section 6.3, we obtain b-symbol distances of all repeated-root constacyclic codes of length p^s over finite fields. Using this result, in Section 6.4, we list all MDS b-symbol repeated-root constacyclic codes of length p^s over finite fields. In Section 6.5, we determine b-symbol distances of all repeated-root constacyclic codes of length p^s over finite commutative chain rings. We also list all MDS b-symbol repeated-root constacyclic codes of length p^s over finite commutative chain rings.

6.2 Some preliminaries

Let R be a finite commutative ring with unity, N be a positive integer, and let R^N be the R-module consisting of all N-tuples over R. Let b be an integer satisfying $2 \leq b < N$. Recall that for each vector $a = (a_0, a_1, \cdots, a_{N-1}) \in R^N$, the b-symbol read vector of $a \in R^N$ is defined as

$$\pi_b(a) = ((a_0, a_1, \cdots, a_{b-1}), (a_1, a_2, \cdots, a_b), \cdots, (a_{N-1}, a_0, \cdots, a_{b-2})) \in (R^b)^N.$$

The b-symbol weight $w_b(a)$ of the vector $a \in R^N$ is defined as the number of integers i satisfying $0 \leq i \leq N-1$ and $(a_i, a_{i+1}, \cdots, a_{i+b-1}) \neq (0, 0, \cdots, 0)$, where the subscripts $i, i+1, \cdots, i+b-1$ are taken modulo N. Note that $w_b(a)$ equals the Hamming weight of the b-symbol read vector $\pi_b(a)$ over the alphabet R^b. In particular, when $b = 2$, the b-symbol weight $w_b(a)$ of the vector $a \in R^N$ is same as the symbol-pair weight $w_{sp}(a)$ of the vector a.

Now the natural question arises: Is there any relation between the b-symbol weight of a vector and its Hamming weight? Towards this, Cassuto and Blaum [12, Th. 2] derived such a relation when $b = 2$. Recently, Mostafanasab and Sevim [63, Th. 2.1] considered the case $b \geq 3$ and derived a relation between the b-symbol weight and the Hamming weight of a non-zero vector in R^N. However, we noticed that Theorem 2.1 of Mostafanasab and Sevim [63] holds only for those non-zero vectors in R^N, which have a cyclic run of 0 of length at least $b-1$. We illustrate this in the following example.

Example 6.2.1. Let $R = \mathbb{Z}_5$ be the ring of integers modulo 5, and let $N = 17$ and $b = 5$. Let us take $c = (2, 1, 2, 0, 0, 0, 2, 4, 0, 0, 0, 3, 1, 0, 0, 0, 2) \in \mathbb{Z}_5^{17}$. Note that the vector c does not have a cyclic run of 0 of lengths at least 4. By Theorem 2.1 of Mostafanasab and Sevim [63], we obtain $w_5(c) = 8 + 9 + 5 - 1 = 21 > 17 = N$. However, one can easily observe that the actual value of $w_5(c)$ is 17. □

We now take into account both the aforementioned cases and restate Theorem 2.1 of Mostafanasab and Sevim [63] as follows:

Theorem 6.2.1. [63] Let $2 \leq b < N$ be a fixed integer, and let $a = (a_0, a_1, \cdots, a_{N-1}) \in R^N$.

(a) If the vector $a \in R^N$ does not have a cyclic run of 0 of length at least $b-1$, then $w_b(a) = N$.

(b) Suppose that the vector $a \in R^N$ has a cyclic run of 0 of length at least $b-1$. Let $\mathcal{I} = \{0, 1, 2, \cdots, N-1\}$, and let $\mathcal{J}_a$ be the union of all sets of the form $\{u \in \mathcal{I} : i \leq u \leq j, j-i \geq b-2$ and $a_u = 0$ for $i \leq u \leq j\}$ modulo N. Let $\mathcal{K}_a = \mathcal{I} \setminus \mathcal{J}_a$. Let $\mathfrak{B}_a = \{B_1, B_2, \cdots, B_{L_a}\}$ be a minimal partition of the set $\mathcal{K}_a$ into subsets of consecutive indices modulo N. If e_a is the number of integers $k \in \mathcal{K}_a$ satisfying $a_k = 0$, then we have

$$w_b(a) = \sum_{\ell=1}^{L_a} |B_\ell| + L_a(b-1) = w_H(a) + e_a + L_a(b-1).$$

We now illustrate the above theorem in the following example.

Example 6.2.2. Let $R = \mathbb{Z}_5$, $N = 17$ and $b = 5$. Let us take $c = (3, 1, 0, 0, 0, 0, 2, 3, 0, 0, 0, 0, 0, 0, 1, 0, 2) \in \mathbb{Z}_5^{17}$. Note that the vector c has two cyclic runs of 0 of lengths at least 4. Here we see that $\mathcal{J}_c = \{2, 3, 4, 5, 8, 9, 10, 11, 12, 13\}$ and $\mathcal{K}_c = \{0, 1, 6, 7, 14, 15, 16\}$. This implies that $\mathfrak{B}_c = \{B_1, B_2\}$, where $B_1 = \{6, 7\}$ and $B_2 = \{14, 15, 16, 0, 1\}$. Now by applying Theorem 6.2.1(b), we obtain $w_5(c) = |B_1| + |B_2| + 2(5-1) = 15$.

We also make the following observation, which is quite useful in approximating b-symbol weights of non-zero vectors in R^N.

Lemma 6.2.1. Let $a \in R^N$ be such that $a = a_1 + a_2 + \cdots + a_r$, where $a_1, a_2, \cdots, a_r \in R^N$ satisfy $w_H(a) = w_H(a_1) + w_H(a_2) + \cdots + w_H(a_r)$. Then we have

$$w_b(a) \geq \max\{w_b(a_1), w_b(a_2), \cdots, w_b(a_r)\}.$$

Proof. Proof is trivial. □

Ding et al. [28, Th. 2.4] derived a Singleton-type bound for codes over finite fields with respect to the b-symbol metric. In the following theorem, we extend this result to codes over finite commutative rings. Although the proof of the following theorem is similar to that of

Theorem 2.4 of Ding et al. [28], we reproduce the proof for the sake of completeness of this thesis.

Theorem 6.2.2. (Singleton-type bound) Let $|R| \geq 2$, $N \geq 3$ be an integer, and let b be an integer satisfying $2 \leq b < N$. If $\mathcal{C}$ is a b-symbol code of length N and b-symbol distance $d_b(\mathcal{C})$ over R, then we have

$$|\mathcal{C}| \leq |R|^{N-d_b(\mathcal{C})+b}.$$

Proof. Let us take $t = d_b(\mathcal{C})$, and let us consider the set

$$\pi_b(\mathcal{C}) = \{\pi_b(c) : c \in \mathcal{C}\},$$

whose elements are viewed as N-tuples over the alphabet R^b. Now on deleting the last $t-1$ coordinates from all the elements of $\pi_b(\mathcal{C})$, we obtain the set

$$\widehat{\pi_b(\mathcal{C})} = \{\big((a_0, a_1, \cdots, a_{b-1}), (a_1, a_2, \cdots, a_b), \cdots, (a_{N-t}, a_{N-t+1}, \cdots, a_{N-t+b-1})\big) : (a_0, a_1, \cdots, a_{N-1}) \in \mathcal{C}\},$$

whose elements are $(N-t+1)$-tuples over R^b, where the subscripts are taken modulo N. Since the b-symbol distance of the code $\mathcal{C}$ is t, we see that all the elements in the set $\widehat{\pi_b(\mathcal{C})}$ must be distinct, and hence all the elements in the set

$$\Phi_b(\mathcal{C}) = \{(a_0, a_1, \cdots, a_{N-t+b-1}) : (a_0, a_1, \cdots, a_{N-1}) \in \mathcal{C}\} \tag{6.2.1}$$

must be the distinct vectors of R^{N-t+b}. From this, it follows that $|\mathcal{C}| \leq |R|^{N-t+b}$, which proves the theorem. □

A code $\mathcal{C}$ of length N over R is called an MDS b-symbol code if it satisfies

$$|\mathcal{C}| = |R|^{N-d_b(\mathcal{C})+b}. \tag{6.2.2}$$

Note that an MDS b-symbol code has to be non-zero.

From now on, throughout this chapter, let p be a prime, s, m be positive integers, and let b be an integer satisfying $2 \leq b < p^s$. Let $\mathbb{F}_{p^m}$ be the finite field of order p^m, and let $\mathcal{R}$ be a finite commutative chain ring with the characteristic as a power of p. Further, let γ be a generator of the maximal ideal of $\mathcal{R}$, and let e be the nilpotency index of γ.

6.3 b-Symbol distances of constacyclic codes of length p^s over $\mathbb{F}_{p^m}$

In this section, we shall determine b-symbol distances of all constacyclic codes of length p^s over $\mathbb{F}_{p^m}$. For this, we first note that $2 \leq b \leq p^s - 1$. Throughout this section, let λ be a non-zero element of $\mathbb{F}_{p^m}$. Recall that a λ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$ is an ideal of the quotient ring $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \lambda \rangle$. By Theorem 2.0.8, we see that there exists $\lambda_0 \in \mathbb{F}_{p^m} \setminus \{0\}$ satisfying $\lambda = \lambda_0^{p^s}$, and that all λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ are given by $\mathscr{C}_{\lambda_0}(s, \nu) = \langle (x - \lambda_0)^\nu \rangle$, where $0 \leq \nu \leq p^s$. It is easy to see that $d_b(\mathscr{C}_{\lambda_0}(s, 0)) = b$ and $d_b(\mathscr{C}_{\lambda_0}(s, p^s)) = 0$. So from now onwards, we assume that $1 \leq \nu \leq p^s - 1$.

In a recent work, Mostafanasab and Sevim [63] considered the case $\lambda_0 = 1$ and $b \geq 3$, and determined b-symbol distances of the cyclic code $\mathscr{C}_1(1, \nu)$ when $1 \leq \nu \leq p - b$ and the cyclic code $\mathscr{C}_1(s, \nu)$ when $s \geq 2$ and $\nu = p^s - p^{s-\ell} + i$, where $0 \leq \ell \leq s - 1$ and $0 \leq i \leq \min\{p^{s-\ell-1}, p^{s-\ell} - b, b\}$. In this section, we shall determine b-symbol distances of all non-trivial λ-constacyclic codes $\mathscr{C}_{\lambda_0}(s, \nu)$, $1 \leq \nu \leq p^s - 1$, of length p^s over $\mathbb{F}_{p^m}$, thereby extending the work of Mostafanasab and Sevim [63]. For this, we shall consider the following two cases separately: (i) $s = 1$ and (ii) $s \geq 2$.

In the following theorem, we consider the case $s = 1$, and we determine b-symbol distances of all non-trivial λ-constacyclic codes $\mathscr{C}_{\lambda_0}(1, \nu)$, $1 \leq \nu \leq p - 1$, of length p over $\mathbb{F}_{p^m}$ by applying Theorem 6.2.1. When $1 \leq \nu \leq p - b - 1$, the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(1, \nu)$ can also be determined by using Theorem 2.0.8 and by repeatedly applying Theorem 2.5 of Ding et al. [28].

Theorem 6.3.1. For $1 \leq \nu \leq p-1$, we have

$$d_b(\mathscr{C}_{\lambda_0}(1,\nu)) = \min\{\nu + b,\ p\}.$$

Proof. To prove the result, we see, by Theorem 2.0.8, that $d_H(\mathscr{C}_{\lambda_0}(1,\nu)) = \nu + 1$. Further, the codeword $(x-\lambda_0)^\nu \in \mathscr{C}_{\lambda_0}(1,\nu)$ can be written as $(x-\lambda_0)^\nu = \sum_{t=0}^{\nu} a_t x^t$, where $a_t = \binom{\nu}{t}(-\lambda_0)^{\nu-t} \neq 0$ for $0 \leq t \leq \nu$. That is, the codeword $(x-\lambda_0)^\nu$ is of the form $(a_0, a_1, \cdots, a_\nu, \underbrace{0, 0, \cdots, 0}_{p-\nu-1})$ and $w_H((x-\lambda_0)^\nu) = \nu + 1$. Now by applying Theorem 6.2.1, we get

$$w_b((x-\lambda_0)^\nu) = \min\{\nu + b, p\} = \begin{cases} \nu + 1 + (b-1) & \text{if } 1 \leq \nu \leq p-b; \\ p & \text{otherwise,} \end{cases}$$

which implies that

$$d_b(\mathscr{C}_{\lambda_0}(1,\nu)) \leq \min\{\nu + b, p\}. \tag{6.3.1}$$

Next we assert that

$$d_b(\mathscr{C}_{\lambda_0}(1,\nu)) \geq \min\{\nu + b, p\}. \tag{6.3.2}$$

To prove the above assertion, suppose, on the contrary, that there exists a non-zero codeword $c(x) \in \mathscr{C}_{\lambda_0}(1,\nu)$ satisfying $w_b(c(x)) \leq \min\{\nu + b, p\} - 1$. By Theorem 6.2.1(b) and using the fact that $w_H(c(x)) \geq \nu + 1$, $e_c \geq 0$ and $L_c \geq 1$, we get

$$\begin{aligned} \nu + b - 1 \geq \min\{\nu + b, p\} - 1 \geq w_b(c(x)) &= w_H(c(x)) + e_c + L_c(b-1) \\ &\geq w_H(c(x)) + L_c(b-1) \geq \nu + b, \end{aligned}$$

which is a contradiction.

Now by (6.3.1) and (6.3.2), we get the desired result. □

From this point on, throughout this section, we assume that $s \geq 2$. In order to determine b-symbol distances of all non-trivial λ-constacyclic codes $\mathscr{C}_{\lambda_0}(s,\nu)$, $1 \leq \nu \leq p^s - 1$, of length p^s over $\mathbb{F}_{p^m}$, we first partition the set $\{1, 2, \cdots, p^s - 1\}$ as follows:

Remark 6.3.1. [21, Th. 3.4] For $0 \leq k \leq s-1$, let us define $\mathcal{F}_k = \{p^s - p^{s-k} + \omega p^{s-k-1} + \tau : 0 \leq \omega \leq p-2,\ 1 \leq \tau \leq p^{s-k-1}\}$. Then $\{\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2, \cdots, \mathcal{F}_{s-1}\}$ is a partition of the set $\{1, 2, \cdots, p^s - 1\}$. □

Now in the following theorem, we determine b-symbol distances of all non-trivial λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ when $s \geq 2$.

Theorem 6.3.2. Let $s \geq 2$ be a fixed integer. For $0 \leq k \leq s-1$, $0 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-k-1}$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau))$$

$$= \begin{cases} p^k \min\{\omega p^{s-k-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\} & \text{if } 2 \leq b \leq p^{s-k-1}; \\ p^k \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\} & \text{if } p^{s-k-1} < b < p^s. \end{cases}$$

To prove the above theorem, we shall first prove Proposition 6.3.1, which reduces our problem to the problem of determination of b-symbol distances of the codes $\mathscr{C}_{\lambda_0}(s, \nu)$, where $s \geq 1$ and $\nu \in \mathcal{F}_0 = \{\omega p^{s-1} + \tau : 1 \leq \tau \leq p^{s-1} \text{ and } 0 \leq \omega \leq p-2\}$. When $s = 1$, Theorem 6.3.1 provides b-symbol distances of the codes $\mathscr{C}_{\lambda_0}(s, \nu)$ for each $\nu \in \mathcal{F}_0 = \{1, 2, \cdots, p-1\}$. When $s \geq 2$, we shall further distinguish the following two cases: $b \leq p^{s-1}$ and $b \geq p^{s-1}+1$, and we shall determine b-symbol distances of the codes $\mathscr{C}_{\lambda_0}(s, \nu)$, $\nu \in \mathcal{F}_0$, in Proposition 6.3.2 when $b \leq p^{s-1}$ and in Proposition 6.3.3 when $b \geq p^{s-1} + 1$.

In order to prove Proposition 6.3.1, we first prove the following two lemmas:

Lemma 6.3.1. Let $g(x) = x^{i_1} g_1(x^{p^{s-1}}) + x^{i_2} g_2(x^{p^{s-1}}) + \cdots + x^{i_r} g_r(x^{p^{s-1}}) \in \mathbb{F}_{p^m}[x]$, where $i_1, i_2, \cdots, i_r$ are integers satisfying $0 \leq i_1 < i_2 < \cdots < i_r < p^{s-1}$ and $g_1(x^{p^{s-1}}), g_2(x^{p^{s-1}}), \cdots, g_r(x^{p^{s-1}})$ are non-zero polynomials in $x^{p^{s-1}}$ over $\mathbb{F}_{p^m}$. Suppose that $(x - \lambda_0)^\tau$ divides $g(x)$ in $\mathbb{F}_{p^m}[x]$, where $1 \leq \tau \leq p^{s-1} - 1$. Then the following hold.

(a) If $g_r(\lambda_0^{p^{s-1}}) \neq 0$, then $i_r \geq \tau$.

(b) Let ρ be an integer satisfying $1 \leq \rho \leq r-1$. If $g_\rho(\lambda_0^{p^{s-1}}) \neq 0$, then we have $p^{s-1} - i_{\rho+1} + i_\rho \geq \tau$.

Proof. (a) First of all, suppose that $g_r(\lambda_0^{p^{s-1}}) \neq 0$. Let us rewrite the polynomial $g(x)$ as

$$g(x) = \sum_{j=1}^{r} x^{i_j}\big(g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})\big) + \sum_{j=1}^{r} g_j(\lambda_0^{p^{s-1}})x^{i_j}. \tag{6.3.3}$$

Now for $1 \leq j \leq r$, we note that $g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})$ is a polynomial in $x^{p^{s-1}}$ and the polynomial $x - \lambda_0$ divides $g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})$ in $\mathbb{F}_{p^m}[x]$. This implies that $(x-\lambda_0)^{p^{s-1}}$ divides $g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})$ in $\mathbb{F}_{p^m}[x]$ for each j. From this, by (6.3.3) and using the fact that $(x-\lambda_0)^\tau$ divides $g(x)$ in $\mathbb{F}_{p^m}[x]$, we see that $(x-\lambda_0)^\tau$ divides $g_1(\lambda_0^{p^{s-1}})x^{i_1} + g_2(\lambda_0^{p^{s-1}})x^{i_2} + \cdots + g_{r-1}(\lambda_0^{p^{s-1}})x^{i_{r-1}} + g_r(\lambda_0^{p^{s-1}})x^{i_r}$ in $\mathbb{F}_{p^m}[x]$. Further, since $0 \leq i_1 < i_2 < \cdots < i_r$ and $g_r(\lambda_0^{p^{s-1}}) \neq 0$, we get $i_r \geq \tau$.

(b) Here we have $g_\rho(\lambda_0^{p^{s-1}}) \neq 0$. Let us consider

$$\begin{aligned} x^{p^{s-1}-i_{\rho+1}}g(x) &= \sum_{j=1}^{r} x^{p^{s-1}-i_{\rho+1}+i_j}\big(g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})\big) \\ &\quad + \sum_{j=1}^{r} g_j(\lambda_0^{p^{s-1}})x^{p^{s-1}-i_{\rho+1}+i_j} \\ &= \sum_{t=1}^{\rho} g_t(\lambda_0^{p^{s-1}})x^{p^{s-1}-i_{\rho+1}+i_t} + \lambda_0^{p^{s-1}} \sum_{u=\rho+1}^{r} g_u(\lambda_0^{p^{s-1}})x^{i_u-i_{\rho+1}} \\ &\quad + \sum_{j=1}^{r} x^{p^{s-1}-i_{\rho+1}+i_j}\big(g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})\big) \\ &\quad + \sum_{u=\rho+1}^{r} g_u(\lambda_0^{p^{s-1}})\big(x^{p^{s-1}} - \lambda_0^{p^{s-1}}\big)x^{i_u-i_{\rho+1}}. \end{aligned} \tag{6.3.4}$$

Now for $1 \leq j \leq r$, we note that $g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})$ is a polynomial in $x^{p^{s-1}}$ and $x - \lambda_0$ divides $g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})$ in $\mathbb{F}_{p^m}[x]$. This implies that $(x-\lambda_0)^{p^{s-1}}$ divides $g_j(x^{p^{s-1}}) - g_j(\lambda_0^{p^{s-1}})$ in $\mathbb{F}_{p^m}[x]$ for each j. From this, by (6.3.4) and using the fact that $(x-\lambda_0)^\tau$ divides $g(x)$ in $\mathbb{F}_{p^m}[x]$, we see that $(x-\lambda_0)^\tau$ divides $\sum_{t=1}^{\rho} g_t(\lambda_0^{p^{s-1}})x^{p^{s-1}-i_{\rho+1}+i_t} + \lambda_0^{p^{s-1}} \sum_{u=\rho+1}^{r} g_u(\lambda_0^{p^{s-1}})x^{i_u-i_{\rho+1}}$ in $\mathbb{F}_{p^m}[x]$. Further, using the fact that $0 \leq i_1 < i_2 < \cdots < i_r < p^{s-1}$ and $g_\rho(\lambda_0^{p^{s-1}}) \neq 0$, we obtain $p^{s-1} - i_{\rho+1} + i_\rho \geq \tau$.

This proves the lemma. □

The following lemma is quite useful in the determination of the b-symbol weight of a non-zero codeword in $\mathscr{C}_{\lambda_0}(s,\nu)$ for each $\nu \in \mathcal{F}_k$, where $1 \leq k \leq s-1$.

Lemma 6.3.2. Let k be an integer satisfying $1 \leq k \leq s-1$. Let $c(x) = (x-\lambda_0)^{p^s-p^{s-k}} g(x) \in \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \lambda \rangle$, where $g(x) = \sum_{j=0}^{r} g_j x^j \in \mathbb{F}_{p^m}[x]$ with $0 \leq r < p^{s-k}$ and $g_r \neq 0$. Let us define $\widetilde{g} = (\underbrace{g_0, g_1, \cdots, g_r, 0, \cdots, 0}_{p^{s-k}})$. Then we have

$$w_b(c(x)) = \begin{cases} p^k w_b(\widetilde{g}) & \text{if } 2 \leq b \leq p^{s-k}-1; \\ p^s & \text{if } p^{s-k} \leq b \leq p^s - 1. \end{cases}$$

Proof. To prove the result, we first observe that the polynomial $(x-\lambda_0)^{p^s-p^{s-k}}$ can be written as $(x-\lambda_0)^{p^s-p^{s-k}} = \sum_{i=0}^{p^k-1} A_i x^{ip^{s-k}}$, where $A_i = \binom{p^k-1}{i}(-\lambda_0)^{p^{s-k}(p^k-1-i)}$ for $0 \leq i \leq p^k-1$. Further, for $0 \leq i \leq p^k-1$, by applying Theorem 2.0.10, we get $\binom{p^k-1}{i} \equiv \prod_{j=0}^{k-1} \binom{p-1}{i_j} \pmod{p}$, where $i = i_0 + i_1 p + i_2 p^2 + \cdots + i_{k-1}p^{k-1}$ is the p-adic representation of i. From this, it follows that $A_i \neq 0$ for $0 \leq i \leq p^k - 1$. Further, we see that

$$c(x) \;=\; (x-\lambda_0)^{p^s-p^{s-k}} g(x) \;=\; \sum_{i=0}^{p^k-1} \sum_{j=0}^{r} A_i g_j x^{ip^{s-k}+j},$$

which implies that $c(x) \in \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \lambda \rangle$ is of the form

$$c \;=\; \big(\underbrace{A_0 g_0, A_0 g_1, \cdots, A_0 g_r, 0, \cdots, 0}_{p^{s-k}}, \underbrace{A_1 g_0, A_1 g_1, \cdots, A_1 g_r, 0, \cdots, 0}_{p^{s-k}}, \cdots,$$
$$\underbrace{A_{p^k-1} g_0, A_{p^k-1} g_1, \cdots, A_{p^k-1} g_r, 0, \cdots, 0}_{p^{s-k}}\big).$$

From this, one can easily observe that $w_b(c(x)) = p^s$ if $p^{s-k} \leq b \leq p^s - 1$. On the other hand, when $2 \leq b \leq p^{s-k} - 1$, we observe that $w_b(c(x)) = p^k w_b(\widetilde{g})$.

This proves the lemma. □

In order to obtain symbol-pair distances of cyclic codes of length p^s over $\mathbb{F}_{p^m}$, Sun et al. [77] defined a bijection from the cyclic code $\langle (x-1)^{p^s-p^{s-k}+\vartheta} \rangle$ of length p^s over $\mathbb{F}_{p^m}$ onto the cyclic code $\langle (x-1)^{\vartheta} \rangle$ of length p^{s-k} over $\mathbb{F}_{p^m}$, where $1 \leq k \leq s-1$ and

$0 \leq \vartheta \leq p^{s-k}-1$. We observe that the same map can be extended to λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ as follows:

For $1 \leq k \leq s-1$ and $0 \leq \vartheta \leq p^{s-k}-1$, define $\phi_k : \mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\vartheta) \to \mathscr{C}_{\lambda_0}(s-k, \vartheta)$ as

$$\phi_k((x-\lambda_0)^{p^s-p^{s-k}+\vartheta} f(x)) \;=\; (x-\lambda_0)^{\vartheta} f(x)$$

for each $(x-\lambda_0)^{p^s-p^{s-k}+\vartheta} f(x) \in \mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\vartheta)$, (note that each non-zero codeword $c(x) \in \mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\vartheta)$ can be uniquely expressed as $c(x) = (x-\lambda_0)^{p^s-p^{s-k}+\vartheta} f(x)$, where $f(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$ and deg $f(x) < p^{s-k}-\vartheta$). One can easily observe that the map ϕ_k is a bijection from $\mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\vartheta)$ onto $\mathscr{C}_{\lambda_0}(s-k, \vartheta)$.

The following proposition plays an important role in the determination of the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, \nu)$ for each $\nu \in \mathcal{F}_k$, where $1 \leq k \leq s-1$.

Proposition 6.3.1. For $1 \leq k \leq s-1$, $0 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-k-1}$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\omega p^{s-k-1}+\tau))$$

$$= \begin{cases} p^k d_b(\mathscr{C}_{\lambda_0}(s-k, \omega p^{s-k-1}+\tau)) & \text{if } 2 \leq b \leq p^{s-k}-1; \\ p^s & \text{if } p^{s-k} \leq b \leq p^s-1. \end{cases}$$

Proof. To prove the result, we first observe that any non-zero codeword $c(x) \in \mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\omega p^{s-k-1}+\tau)$ can be uniquely expressed as $c(x) = (x-\lambda_0)^{p^s-p^{s-k}+\omega p^{s-k-1}+\tau} f(x)$, where $f(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$ and deg $f(x) < p^{s-k}-\omega p^{s-k-1}-\tau$. Using the fact that $\phi_k(c(x)) = (x-\lambda_0)^{\omega p^{s-k-1}+\tau} f(x)$ and by applying Lemma 6.3.2, we see that

$$w_b(c(x)) = \begin{cases} p^k w_b(\phi_k(c(x))) & \text{if } 2 \leq b \leq p^{s-k}-1; \\ p^s & \text{if } p^{s-k} \leq b \leq p^s-1. \end{cases} \tag{6.3.5}$$

Further, since the map $\phi_k : \mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\omega p^{s-k-1}+\tau) \to \mathscr{C}_{\lambda_0}(s-k, \omega p^{s-k-1}+\tau)$ is a bijection, we obtain

$$d_b(\mathscr{C}_{\lambda_0}(s, p^s-p^{s-k}+\omega p^{s-k-1}+\tau)) = p^k d_b(\mathscr{C}_{\lambda_0}(s-k, \omega p^{s-k-1}+\tau)) \text{ when } 2 \leq b \leq p^{s-k}-1.$$

On the other hand, when $p^{s-k} \leq b \leq p^s-1$, by (6.3.5), we see that $w_b(c(x)) = p^s$ for each

$c(x)(\neq 0) \in \mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)$, which implies that $d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) = p^s$. □

Now in view of Remark 6.3.1, Proposition 6.3.1 and Theorem 6.3.1, we see that to determine b-symbol distances of all non-trivial λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$, it is enough to determine b-symbol distances of the codes $\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)$, where $s \geq 2$, $1 \leq \tau \leq p^{s-1}$ and $0 \leq \omega \leq p-2$. To do this, we shall distinguish the following two cases: $b \leq p^{s-1}$ and $b \geq p^{s-1} + 1$.

6.3.1 The case $b \leq p^{s-1}$

Throughout this section, we assume that $b \leq p^{s-1}$. In the following proposition, we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)$, where $0 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-1}$.

Proposition 6.3.2. Let $2 \leq b \leq p^{s-1}$ be fixed. For $0 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-1}$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) = \min\{\omega p^{s-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\}.$$

To prove the above proposition, we shall consider the following three cases separately: (i) $\omega = 0$ and $1 \leq \tau \leq p^{s-1}$, (ii) $1 \leq \omega \leq p-2$ and $\tau = p^{s-1}$, and (iii) $1 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-1} - 1$.

In the following lemma, we consider the case $\omega = 0$, and we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, \tau)$, where $1 \leq \tau \leq p^{s-1}$.

Lemma 6.3.3. For $1 \leq \tau \leq p^{s-1}$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, \tau)) = \min\{b + \tau,\ 2b\}.$$

Proof. To prove the result, we shall distinguish the following two cases: (i) $1 \leq \tau \leq b$ and (ii) $b + 1 \leq \tau \leq p^{s-1}$.

(i) First let $1 \leq \tau \leq b$. In this case, we see that $(x-\lambda_0)^\tau \in \mathscr{C}_{\lambda_0}(s,\tau)$ can be expressed as $(x-\lambda_0)^\tau = \sum_{t=0}^{\tau} W_t x^t$, where $W_t = \binom{\tau}{t}(-\lambda_0)^{\tau-t}$ for $0 \leq t \leq \tau$. From this, we see that the codeword $(x-\lambda_0)^\tau$ is of the form

$$\big(W_0, W_1, W_2, \cdots\cdots\cdots, W_{\tau-1}, W_\tau, \underbrace{0, 0, \cdots, 0}_{p^s-\tau-1}\big).$$

Now by applying Theorem 6.2.1(b) and using the fact that $p^s - \tau - 1 \geq b-1$, we observe that the codeword $(x-\lambda_0)^\tau \in \mathscr{C}_{\lambda_0}(s,\tau)$ has b-symbol weight

$$w_b((x-\lambda_0)^\tau) = \begin{cases} 2+2(b-1) & \text{if } \tau = b \text{ and } W_1 = W_2 = \cdots = W_{\tau-1} = 0; \\ \tau+1+b-1 & \text{otherwise,} \end{cases}$$

which implies that

$$d_b(\mathscr{C}_{\lambda_0}(s,\tau)) \leq \tau + b. \tag{6.3.6}$$

We further assert that

$$w_b(c(x)) \geq \tau + b \text{ for each non-zero codeword } c(x) \in \mathscr{C}_{\lambda_0}(s,\tau). \tag{6.3.7}$$

To prove the above assertion, suppose, on the contrary, that there exists a non-zero codeword $d(x) \in \mathscr{C}_{\lambda_0}(s,\tau)$ satisfying $w_b(d(x)) \leq \tau+b-1$. By Theorem 6.2.1(b), we have $\tau+b-1 \geq w_b(d(x)) = w_H(d(x))+e_d+L_d(b-1)$. Since $w_H(d(x)) \geq 2$, $e_d \geq 0$ and $\tau \leq b$, we get $2b-1 \geq \tau+b-1 \geq 2+L_d(b-1)$, which gives $L_d = 1$. This implies that $\tau+b-1 \geq w_b(d(x)) = w_H(d(x))+e_d+(b-1)$, which further implies that $w_H(d(x))+e_d \leq \tau$. In view of this, by applying Theorem 6.2.1(b) again and using the fact that $L_d = 1$, we see that there exists an integer j such that $0 \leq j \leq p^s-1$ and $x^j d(x) \in \mathscr{C}_{\lambda_0}(s,\tau)$ is of the form $x^j d(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_u x^u$, where $u = w_H(d(x)) + e_d - 1$, $d_i \in \mathbb{F}_{p^m}$ for $0 \leq i \leq u$ and both d_0, d_u are non-zero. As $w_H(d(x)) \geq 2$, $e_d \geq 0$ and $w_H(d(x)) + e_d \leq \tau$, we note that $1 \leq u \leq \tau - 1$. Therefore there exists a non-zero codeword $x^j d(x) \in \mathscr{C}_{\lambda_0}(s,\tau) = \langle (x-\lambda_0)^\tau \rangle$ satisfying deg $x^j d(x) = u \leq \tau - 1$, which is a contradiction.

Now by (6.3.6) and (6.3.7), we obtain

$$d_b(\mathscr{C}_{\lambda_0}(s,\tau)) = \tau + b \text{ for } 1 \leq \tau \leq b.$$

(ii) Next let $b+1 \leq \tau \leq p^{s-1}$. Here by Theorem 6.2.1(b) again, we see that the codeword $(x-\lambda_0)^{p^{s-1}} \in \mathscr{C}_{\lambda_0}(s, p^{s-1})$ has b-symbol weight $w_b((x-\lambda_0)^{p^{s-1}}) = 2 + 2(b-1)$, which implies that

$$d_b(\mathscr{C}_{\lambda_0}(s,p^{s-1})) \leq 2b. \tag{6.3.8}$$

By case (i), we note that $d_b(\mathscr{C}_{\lambda_0}(s,b)) = 2b$. From this, by (6.3.8) and using the fact that

$$\mathscr{C}_{\lambda_0}(s,b) \supseteq \mathscr{C}_{\lambda_0}(s,b+1) \supseteq \cdots \supseteq \mathscr{C}_{\lambda_0}(s,p^{s-1}),$$

we get

$$2b = d_b(\mathscr{C}_{\lambda_0}(s,b)) \leq d_b(\mathscr{C}_{\lambda_0}(s,b+1)) \leq \cdots \leq d_b(\mathscr{C}_{\lambda_0}(s,p^{s-1})) \leq 2b.$$

This gives

$$d_b(\mathscr{C}_{\lambda_0}(s,b+1)) = d_b(\mathscr{C}_{\lambda_0}(s,b+2)) = \cdots = d_b(\mathscr{C}_{\lambda_0}(s,p^{s-1})) = 2b.$$

This completes the proof of the lemma.

□

In the following lemma, we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})$, where $1 \leq \omega \leq p-2$.

Lemma 6.3.4. For $1 \leq \omega \leq p-2$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})) = (\omega+2)b.$$

Proof. To prove the result, we see that the codeword $(x-\lambda_0)^{(\omega+1)p^{s-1}} \in \mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})$ can be expressed as $(x-\lambda_0)^{(\omega+1)p^{s-1}} = \sum_{t=0}^{\omega+1} W_t x^{tp^{s-1}}$, where $W_t = \binom{\omega+1}{t}(-\lambda_0)^{(\omega+1-t)p^{s-1}} \neq$

0 for $0 \leq t \leq \omega+1$. This implies that the codeword $(x-\lambda_0)^{(\omega+1)p^{s-1}}$ is of the form

$$\big(W_0, \underbrace{0,0,\cdots,0}_{p^{s-1}-1}, W_1, \underbrace{0,0,\cdots,0}_{p^{s-1}-1}, W_2, \cdots\cdots\cdots, W_\omega, \underbrace{0,0,\cdots,0}_{p^{s-1}-1}, W_{\omega+1}, \underbrace{0,0,0,\cdots,0,0}_{p^s-(\omega+1)p^{s-1}-1}\big).$$

Now by applying Theorem 6.2.1(b) and using the fact that $p^{s-1}-1 \geq b-1$, we see that $w_b((x-\lambda_0)^{(\omega+1)p^{s-1}}) = (\omega+2)+(\omega+2)(b-1) = (\omega+2)b$, which implies that

$$d_b(\mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})) \leq (\omega+2)b. \tag{6.3.9}$$

Next we assert that

$$w_b(c(x)) \geq (\omega+2)b \quad \text{for each non-zero codeword} \quad c(x) \in \mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1}). \tag{6.3.10}$$

To prove the assertion, we first note that each non-zero codeword $c(x) \in \mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})$ can be uniquely written as $c(x) = (x-\lambda_0)^{(\omega+1)p^{s-1}} f(x)$, where $f(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$ and deg $f(x) < p^s-(\omega+1)p^{s-1}$. Further, we observe that the polynomial $f(x) \in \mathbb{F}_{p^m}[x]$ can be uniquely expressed as $f(x) = x^{i_1}f_1(x^{p^{s-1}}) + x^{i_2}f_2(x^{p^{s-1}}) + \cdots + x^{i_r}f_r(x^{p^{s-1}})$, where $0 \leq i_1 < i_2 < \cdots < i_r < p^{s-1}$ and $f_u(x^{p^{s-1}})$ is a non-zero polynomial in $x^{p^{s-1}}$ over $\mathbb{F}_{p^m}$ for $1 \leq u \leq r$. This implies that

$$w_H(c(x)) = \sum_{u=1}^{r} w_H\big(x^{i_u}(x-\lambda_0)^{(\omega+1)p^{s-1}} f_u(x^{p^{s-1}})\big). \tag{6.3.11}$$

By Theorem 2.0.8, we note that

$$w_H((x-\lambda_0)^{(\omega+1)p^{s-1}} f_u(x^{p^{s-1}})) \geq \omega+2 \quad \text{for} \quad 1 \leq u \leq r. \tag{6.3.12}$$

We further note that $w_b(x^{i_1}(x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})) = w_b((x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}}))$ and that $(x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})$ is a polynomial in $x^{p^{s-1}}$ over $\mathbb{F}_{p^m}$. So by applying Theorem 6.2.1(b) and by (6.3.12), we see that

$$w_b\big(x^{i_1}(x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})\big) = b \times w_H\big((x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})\big) \geq (\omega+2)b.$$

From this, by (6.3.11) and by applying Lemma 6.2.1, we get

$$w_b(c(x)) \geq w_b(x^{i_1}(x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})) \geq (\omega+2)b,$$

which proves the assertion (6.3.10).

Now by (6.3.9) and (6.3.10), we get the desired result. □

In the following lemma, we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)$, where $1 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-1}-1$.

Lemma 6.3.5. For $1 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-1}-1$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)) = \min\{\omega p^{s-1}+b+\tau, (\omega+2)b, (\omega+1)(b+\tau)\}.$$

Proof. To prove the result, we shall distinguish the following two cases: **I.** $1 \leq \tau \leq b-1$ and **II.** $b \leq \tau \leq p^{s-1}-1$.

I. First let $1 \leq \tau \leq b-1$. In this case, we see that $\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau) \supseteq \mathscr{C}_{\lambda_0}(s, (\omega+1)p^{s-1})$, which, by Lemma 6.3.4, implies that

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)) \leq d_b(\mathscr{C}_{\lambda_0}(s, (\omega+1)p^{s-1})) = (\omega+2)b. \tag{6.3.13}$$

Further, we see that the codeword $(x-\lambda_0)^{\omega p^{s-1}+\tau} \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)$ can be expressed as

$$(x-\lambda_0)^{\omega p^{s-1}+\tau} = \sum_{t=0}^{\omega}\sum_{u=0}^{\tau} W_u^{(t)} x^{u+tp^{s-1}},$$

where $W_u^{(t)} = \binom{\omega}{t}\binom{\tau}{u}(-\lambda_0)^{(\omega-t)p^{s-1}+\tau-u}$ for $0 \leq u \leq \tau$ and $0 \leq t \leq \omega$. This implies that the codeword $(x-\lambda_0)^{\omega p^{s-1}+\tau}$ is of the form

$$\Big(W_0^{(0)}, W_1^{(0)}, \cdots, W_\tau^{(0)}, \underbrace{0, 0, \cdots, 0}_{p^{s-1}-\tau-1}, W_0^{(1)}, W_1^{(1)}, \cdots, W_\tau^{(1)}, \underbrace{0, 0, \cdots, 0}_{p^{s-1}-\tau-1}, \cdots, W_0^{(\omega-1)},$$
$$W_1^{(\omega-1)}, \cdots, W_\tau^{(\omega-1)}, \underbrace{0, 0, \cdots, 0}_{p^{s-1}-\tau-1}, W_0^{(\omega)}, W_1^{(\omega)}, \cdots, W_\tau^{(\omega)}, \underbrace{0, 0, 0, \cdots, 0, 0}_{p^s-\omega p^{s-1}-\tau-1}\Big).$$

Now by applying Theorem 6.2.1(b) and using the fact that $p^s - \omega p^{s-1} - \tau \geq b$, we see that

$$\begin{aligned} w_b((x-\lambda_0)^{\omega p^{s-1}+\tau}) &= \begin{cases} (\omega+1)(\tau+1)+(\omega+1)(b-1) \text{ if } 1 \leq \tau \leq p^{s-1}-b; \\ \omega p^{s-1}+\tau+1+b-1 \text{ if } \tau \geq p^{s-1}-b+1 \end{cases} \\ &= \min\{\omega p^{s-1}+b+\tau, (\omega+1)(b+\tau)\}. \end{aligned}$$

From this and by (6.3.13), we obtain

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)) \leq \min\{\omega p^{s-1}+b+\tau, (\omega+2)b, (\omega+1)(b+\tau)\}. \quad (6.3.14)$$

Next we assert that

$$\begin{aligned} w_b(c(x)) \geq \min\{\omega p^{s-1}+b+\tau, (\omega+2)b, (\omega+1)(b+\tau)\} \text{ for each} \\ c(x)(\neq 0) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau). \end{aligned} \quad (6.3.15)$$

To prove the above assertion, let $c(x)(\neq 0) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)$ be such that $w_b(c(x)) < p^s$. Further, the codeword $c(x)$ can be uniquely written as $c(x) = (x-\lambda_0)^{\omega p^{s-1}+\tau} f(x)$, where $f(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$ and deg $f(x) < p^s - \omega p^{s-1} - \tau$. If we take $g(x) = (x-\lambda_0)^\tau f(x)$, then the codeword $c(x)$ can be rewritten as $c(x) = (x-\lambda_0)^{\omega p^{s-1}} g(x)$, where $g(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$, $\tau \leq$ deg $g(x) < p^s - \omega p^{s-1}$ and $(x-\lambda_0)^\tau$ divides $g(x)$ in $\mathbb{F}_{p^m}[x]$. Next we observe that the polynomial $g(x) = (x-\lambda_0)^\tau f(x)$ can be uniquely expressed as $g(x) = x^{i_1} g_1(x^{p^{s-1}}) + x^{i_2} g_2(x^{p^{s-1}}) + \cdots + x^{i_r} g_r(x^{p^{s-1}})$, where $0 \leq i_1 < i_2 < \cdots < i_r < p^{s-1}$ and $g_j(x^{p^{s-1}})$ is a non-zero polynomial in $x^{p^{s-1}}$ over $\mathbb{F}_{p^m}$ for $1 \leq j \leq r$. This implies that

$$w_H(c(x)) = \sum_{j=1}^{r} w_H\big(x^{i_j}(x-\lambda_0)^{\omega p^{s-1}} g_j(x^{p^{s-1}})\big). \quad (6.3.16)$$

Further, as $w_b(x^e c(x)) = w_b(c(x))$ for each integer $e \geq 0$, without any loss of generality, we can assume that $i_1 = 0$. By Theorem 2.0.8, we note that

$$w_H(x^{i_j}(x-\lambda_0)^{\omega p^{s-1}} g_j(x^{p^{s-1}})) \geq \omega + 1 \text{ for } 1 \leq j \leq r. \tag{6.3.17}$$

Now the following two cases arise:

A. There exists an integer h satisfying $1 \leq h \leq r$ and $w_H(x^{i_h}(x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})) \geq \omega + 2$.

B. $w_H\big(x^{i_j}(x-\lambda_0)^{\omega p^{s-1}} g_j(x^{p^{s-1}})\big) = \omega + 1$ for $1 \leq j \leq r$.

A. Suppose that there exists an integer h satisfying $1 \leq h \leq r$ and $w_H(x^{i_h}(x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})) \geq \omega + 2$. Now as $w_b(x^{i_h}(x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})) = w_b((x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}}))$ and $(x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})$ is a polynomial in $x^{p^{s-1}}$ over $\mathbb{F}_{p^m}$, by applying Theorem 6.2.1(b), we see that

$$\begin{aligned} w_b(x^{i_h}(x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})) &= w_b((x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})) \\ &= b \times w_H((x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})) \\ &\geq (\omega+2)b. \end{aligned}$$

From this, by (6.3.16) and by applying Lemma 6.2.1, we get $w_b(c(x)) \geq w_b\big(x^{i_h}(x-\lambda_0)^{\omega p^{s-1}} g_h(x^{p^{s-1}})\big) \geq (\omega+2)b$, which proves the assertion (6.3.15) in this case.

B. Now suppose that $w_H\big(x^{i_j}(x-\lambda_0)^{\omega p^{s-1}} g_j(x^{p^{s-1}})\big) = \omega + 1$ for $1 \leq j \leq r$. Further, for $1 \leq j \leq r$, we can write

$$x^{i_j}(x-\lambda_0)^{\omega p^{s-1}} g_j(x^{p^{s-1}}) = x^{i_j}\big\{A_0^{(j)} + A_1^{(j)} x^{p^{s-1}} + \cdots + A_{p-1}^{(j)} x^{p^{s-1}(p-1)}\big\},$$

where $A_t^{(j)} \in \mathbb{F}_{p^m}$ for $0 \leq t \leq p-1$ and the Hamming weight of the vector $\big(A_0^{(j)}, A_1^{(j)}, A_2^{(j)}, \cdots, A_{p-1}^{(j)}\big)$ is $\omega + 1$. In view of this, by (6.3.16) and using the fact that $i_1 = 0$, we see that the codeword $c(x) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)$ is of the

form

$$\begin{aligned} c \;=\; \Big(&A_0^{(1)}, \underbrace{0,0,\cdots,0,0}_{i_2-1}, A_0^{(2)}, \cdots\cdots, A_0^{(r-1)}, \underbrace{0,0,\cdots,0}_{i_r-i_{r-1}-1}, A_0^{(r)}, \underbrace{0,0,\cdots,0}_{p^{s-1}-i_r-1},\\ &A_1^{(1)}, \underbrace{0,0,\cdots,0,0}_{i_2-1}, A_1^{(2)}, \cdots\cdots, A_1^{(r-1)}, \underbrace{0,0,\cdots,0}_{i_r-i_{r-1}-1}, A_1^{(r)}, \underbrace{0,0,\cdots,0}_{p^{s-1}-i_r-1},\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &A_{p-2}^{(1)}, \underbrace{0,0,\cdots,0}_{i_2-1}, A_{p-2}^{(2)}, \cdots\cdots, A_{p-2}^{(r-1)}, \underbrace{0,0,\cdots,0}_{i_r-i_{r-1}-1}, A_{p-2}^{(r)}, \underbrace{0,0,\cdots,0}_{p^{s-1}-i_r-1},\\ &A_{p-1}^{(1)}, \underbrace{0,0,\cdots,0}_{i_2-1}, A_{p-1}^{(2)}, \cdots\cdots, A_{p-1}^{(r-1)}, \underbrace{0,0,\cdots,0}_{i_r-i_{r-1}-1}, A_{p-1}^{(r)}, \underbrace{0,0,\cdots,0}_{p^{s-1}-i_r-1}\Big). \end{aligned}$$

As $w_b(c(x)) < p^s$, the codeword $c(x)$ has a cyclic run of 0 of length at least b. So we will apply Theorem 6.2.1(b) to prove the assertion (6.3.15) in this case. For this, let $\mathfrak{B}_c$ be a minimal partition of the set $\mathcal{K}_c$ (as defined in Theorem 6.2.1(b)) into subsets of consecutive indices modulo p^s, and let $B_1, B_2, \cdots, B_{L_c}$ be all the distinct parts of the partition $\mathfrak{B}_c$. Now by Theorem 6.2.1(b), we see that

$$w_b(c(x)) \;=\; L_c(b-1) + \sum_{\ell=1}^{L_c} |B_\ell|. \tag{6.3.18}$$

When $L_c \geq \omega + 2$, by (6.3.18), we have

$$w_b(c(x)) \;=\; L_c(b-1) + \sum_{\ell=1}^{L_c} |B_\ell| \;\geq\; L_c(b-1) + L_c \;\geq\; (\omega+2)b.$$

So from now on, we assume that $L_c \leq \omega + 1$. Next let us define

$$d_\ell \;=\; |\{j \in \mathbb{Z} : 0 \leq j \leq p-1,\; jp^{s-1} \in B_\ell\}|$$

for $1 \leq \ell \leq L_c$, and let

$$\mathfrak{F}_c \;=\; \{u \in \mathbb{Z} : 1 \leq u \leq L_c,\; d_u > 0\}.$$

One can easily observe that

$$1 \leq |\mathfrak{F}_c| \leq L_c \text{ and } |B_u| \geq 1 + (d_u - 1)p^{s-1} \text{ for each } u \in \mathfrak{F}_c. \quad (6.3.19)$$

Further, since the Hamming weight of the vector $\left(A_0^{(1)}, A_1^{(1)}, A_2^{(1)}, \cdots, A_{p-1}^{(1)}\right)$ is $\omega + 1$, we must have

$$\sum_{u \in \mathfrak{F}_c} d_u \geq \omega + 1. \quad (6.3.20)$$

When $L_c > |\mathfrak{F}_c|$, by (6.3.18)-(6.3.20) and using the fact that $L_c \leq \omega + 1$, we see that

$$\begin{aligned} w_b(c(x)) &= L_c(b-1) + \sum_{u \in \mathfrak{F}_c} |B_u| + \sum_{\substack{\ell=1 \\ \ell \notin \mathfrak{F}_c}}^{L_c} |B_\ell| \\ &\geq L_c(b-1) + \Big(\sum_{u \in \mathfrak{F}_c} d_u - |\mathfrak{F}_c| \Big) p^{s-1} + |\mathfrak{F}_c| + L_c - |\mathfrak{F}_c| \\ &\geq bL_c + (\omega + 1 - |\mathfrak{F}_c|)p^{s-1} \geq bL_c + (\omega + 2 - L_c)p^{s-1} \\ &\geq bL_c + (\omega + 2 - L_c)b = (\omega + 2)b, \end{aligned}$$

which proves the assertion (6.3.15) in this case.

From this point on, we assume that $|\mathfrak{F}_c| = L_c$. Here we have

$$d_\ell \geq 1,\ d_1 + d_2 + \cdots + d_{L_c} \geq \omega + 1 \text{ and } |B_\ell| \geq 1 + (d_\ell - 1)p^{s-1} \text{ for } 1 \leq \ell \leq L_c. \quad (6.3.21)$$

Now we shall distinguish the following two cases: (i) $d_1 + d_2 + \cdots + d_{L_c} \geq \omega + 2$ and (ii) $d_1 + d_2 + \cdots + d_{L_c} = \omega + 1$.

(i) When $d_1 + d_2 + \cdots + d_{L_c} \geq \omega + 2$, by (6.3.18), (6.3.21) and using the fact that $L_c \leq \omega + 1$, we get

$$\begin{aligned} w_b(c(x)) &= L_c(b-1) + \sum_{\ell=1}^{L_c} |B_\ell| \\ &\geq (d_1 + d_2 + \cdots + d_{L_c} - L_c)p^{s-1} + L_c b \geq (\omega + 2)b. \end{aligned}$$

(ii) Next let $d_1 + d_2 + \cdots + d_{L_c} = \omega + 1$. In this case, we assert that

$$\sum_{\ell=1}^{L_c} |B_\ell| \ \geq \ (\tau+1)L_c + (\omega + 1 - L_c)p^{s-1}. \tag{6.3.22}$$

To prove the assertion (6.3.22), we first recall that $d_\ell = |\{j : 0 \leq j \leq p-1, \ jp^{s-1} \in B_\ell\}|$. Now we observe that for each ℓ, the part B_ℓ of the partition $\mathfrak{B}_c$ can be expressed as

$$B_\ell \ = \ \{\upsilon_\ell p^{s-1}, \upsilon_\ell p^{s-1} + 1, \cdots, (\upsilon_\ell + d_\ell - 1)p^{s-1}\} \cup T_\ell \cup S_\ell,$$

where υ_ℓ is an integer satisfying $0 \leq \upsilon_\ell \leq p-1$, the set T_ℓ is either empty or of the form $\{(\upsilon_\ell - 1)p^{s-1} + i_{a_\ell}, (\upsilon_\ell - 1)p^{s-1} + i_{a_\ell} + 1, \cdots, \upsilon_\ell p^{s-1} - 1\}$ with a_ℓ as an integer satisfying $a_\ell \in \{2, 3, \cdots, r\}$ and $A^{(a_\ell)}_{\upsilon_\ell - 1}$ as non-zero, and the set S_ℓ is either empty or of the form $\{(\upsilon_\ell + d_\ell - 1)p^{s-1} + 1, (\upsilon_\ell + d_\ell - 1)p^{s-1} + 2, \cdots, (\upsilon_\ell + d_\ell - 1)p^{s-1} + i_{b_\ell}\}$ with b_ℓ as an integer satisfying $b_\ell \in \{2, 3, \cdots, r\}$ and $A^{(b_\ell)}_{\upsilon_\ell + d_\ell - 1}$ as non-zero. Further, since the Hamming weight of the vector $\left(A^{(1)}_0, A^{(1)}_1, A^{(1)}_2, \cdots, A^{(1)}_{p-1}\right)$ is $\omega + 1$ and $d_1 + d_2 + \cdots + d_{L_c} = \omega + 1$, we see that if $ep^{s-1} \in B_\ell$ for some integers e and ℓ satisfying $0 \leq e \leq p-1$ and $1 \leq \ell \leq L_c$, then we must have $A^{(1)}_e \neq 0$. Now as $\upsilon_\ell p^{s-1}, (\upsilon_\ell + 1)p^{s-1}, \cdots, (\upsilon_\ell + d_\ell - 1)p^{s-1} \in B_\ell$, we note that $A^{(1)}_{\upsilon_\ell}, A^{(1)}_{\upsilon_\ell + 1}, \cdots, A^{(1)}_{\upsilon_\ell + d_\ell - 1}$ all are non-zero.

Next for $2 \leq t \leq r$, let us define $\mathfrak{L}_t = |\{y \in \mathbb{Z} : 0 \leq y \leq p-1, \ yp^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} (T_\ell \cup S_\ell)\}|$. Further, for $2 \leq t \leq r$, we note that

$$\begin{aligned}
&\{i \in \mathbb{Z} : 0 \leq i \leq p-1, \ ip^{s-1} + i_t \ \in \bigcup_{\ell=1}^{L_c} \big(B_\ell \setminus (T_\ell \cup S_\ell)\big)\} \\
&\quad = \bigcup_{\ell=1}^{L_c} \{\upsilon_\ell p^{s-1} + i_t, (\upsilon_\ell + 1)p^{s-1} + i_t, \cdots, (\upsilon_\ell + d_\ell - 2)p^{s-1} + i_t\}.
\end{aligned}$$

Now for $2 \leq t \leq r$, as the Hamming weight of the vector $\Big(A_0^{(t)}, A_1^{(t)}, A_2^{(t)}, \cdots, A_{p-1}^{(t)}\Big)$ is $\omega + 1$, we get

$$\begin{aligned}
\omega + 1 &\leq |\{i \in \mathbb{Z} : 0 \leq i \leq p-1,\ ip^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} B_\ell\}| \\
&= |\{i \in \mathbb{Z} : 0 \leq i \leq p-1,\ ip^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} \big(B_\ell \setminus (T_\ell \cup S_\ell)\big)\}| \\
&\quad + \mathfrak{L}_t \\
&= \sum_{\ell=1}^{L_c} (d_\ell - 1) + \mathfrak{L}_t \ = \ \omega + 1 - L_c + \mathfrak{L}_t.
\end{aligned}$$

From this, we obtain $\mathfrak{L}_t \geq L_c$ for $2 \leq t \leq r$. Now for each ℓ, we note that $|B_\ell| = (d_\ell - 1)p^{s-1} + 1 + |T_\ell| + |S_\ell|$. This gives

$$\begin{aligned}
\sum_{\ell=1}^{L_c} |B_\ell| &= \sum_{\ell=1}^{L_c} \big((d_\ell - 1)p^{s-1} + 1\big) + \sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big) \\
&= (\omega + 1 - L_c)p^{s-1} + L_c + \sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big). \quad (6.3.23)
\end{aligned}$$

In view of this, we see that to prove the assertion (6.3.22), it is enough to show that

$$\sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big) \ \geq \ \tau L_c.$$

Towards this, for $2 \leq t \leq r$, let k_t be the number of non-empty sets S_ℓ satisfying $b_\ell = t$. Note that $|S_\ell| = i_t$ for each non-empty set S_ℓ satisfying $b_\ell = t$. From this, we see that

$$\sum_{\ell=1}^{L_c} |S_\ell| \ = \ \sum_{t=2}^{r} k_t i_t. \quad (6.3.24)$$

Now we proceed to count non-empty sets T_ℓ satisfying $a_\ell = t$, where $2 \leq t \leq r$. For this, let m_t be the number of non-empty sets T_ℓ satisfying $a_\ell = t$ for $2 \leq t \leq r$. Note that $|T_\ell| = p^{s-1} - i_t$ for each non-empty set T_ℓ satisfying $a_\ell = t$. Further, we observe that $m_2 = \mathfrak{L}_2 - k_2 - k_3 - \cdots - k_r$ and $m_u = \mathfrak{L}_u - m_2 - m_3 - \cdots - m_{u-1} - k_u - k_{u+1} - \cdots - k_r$ for $3 \leq u \leq r$.

This implies that $m_u = \mathfrak{L}_u - \mathfrak{L}_{u-1} + k_{u-1}$ for $3 \leq u \leq r$. From this, it follows that

$$\sum_{\ell=1}^{L_c} |T_\ell| = \sum_{t=2}^{r} m_t\big(p^{s-1} - i_t\big) = \big(\mathfrak{L}_2 - k_2 - k_3 - \cdots - k_r\big)\big(p^{s-1} - i_2\big) + \sum_{u=3}^{r} \big(\mathfrak{L}_u - \mathfrak{L}_{u-1} + k_{u-1}\big)\big(p^{s-1} - i_u\big). \tag{6.3.25}$$

By (6.3.24) and (6.3.25) and using the facts that $\mathfrak{L}_r \geq L_c$ and that $0 = i_1 < i_2 < i_3 < \cdots < i_r < p^{s-1}$, we obtain

$$\begin{aligned}
\sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big) &= \sum_{t=2}^{r} k_t i_t + \big(\mathfrak{L}_2 - k_2 - k_3 - \cdots - k_r\big)\big(p^{s-1} - i_2\big) \\
&\quad + \sum_{u=3}^{r} \big(\mathfrak{L}_u - \mathfrak{L}_{u-1} + k_{u-1}\big)\big(p^{s-1} - i_u\big) \\
&= \big(L_c - k_2 - k_3 - \cdots - k_r\big)\big(p^{s-1} - i_2\big) \\
&\quad + \sum_{t=2}^{r-1} \Big(\big(\mathfrak{L}_{t+1} - \mathfrak{L}_t\big)\big(p^{s-1} - i_{t+1}\big)\Big) \\
&\quad + \big(\mathfrak{L}_2 - L_c\big)\big(p^{s-1} - i_2\big) + k_r i_r \\
&\quad + \sum_{t=2}^{r-1} k_t\big(p^{s-1} - i_{t+1} + i_t\big) \\
&\geq \sum_{t=2}^{r-1} k_t\big(p^{s-1} - i_{t+1} + i_t\big) + \big(\mathfrak{L}_r - L_c\big)\big(p^{s-1} - i_r\big) \\
&\quad + k_r i_r + \big(L_c - k_2 - k_3 - \cdots - k_r\big)\big(p^{s-1} - i_2\big) \\
&\geq \big(L_c - k_2 - k_3 - \cdots - k_r\big)\big(p^{s-1} - i_2\big) \\
&\quad + \sum_{t=2}^{r-1} k_t\big(p^{s-1} - i_{t+1} + i_t\big) + k_r i_r.
\end{aligned} \tag{6.3.26}$$

Now we claim that $g_j(\lambda_0^{p^{s-1}}) \neq 0$ for $1 \leq j \leq r$. For, if $g_k(\lambda_0^{p^{s-1}}) = 0$ for some integer k satisfying $1 \leq k \leq r$, then $x - \lambda_0$ divides $g_k(x^{p^{s-1}})$ in $\mathbb{F}_{p^m}[x]$. This implies that $x^{i_k}(x-\lambda_0)^{\omega p^{s-1}} g_k(x^{p^{s-1}}) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+1)$. By Theorem 2.0.8, we note that $d_H(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+1)) = \omega + 2$. This implies that $\omega + 2 \leq w_H\big(x^{i_w}(x-\lambda_0)^{\omega p^{s-1}} g_k(x^{p^{s-1}})\big)$. This is a contradiction, as we

have assumed that $w_H\big(x^{i_j}(x-\lambda_0)^{\omega p^{s-1}} g_j(x^{p^{s-1}})\big) = \omega + 1$ for $1 \leq j \leq r$.

Therefore $g_j(\lambda_0^{p^{s-1}}) \neq 0$ for $1 \leq j \leq r$. This, by Lemma 6.3.1, implies that $i_r \geq \tau$, $p^{s-1} - i_2 \geq \tau$ and $p^{s-1} - i_{t+1} + i_t \geq \tau$ for $2 \leq t \leq r-1$. This further implies, by (6.3.26), that $\sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big) \geq \tau L_c$. From this and by (6.3.23), the assertion (6.3.22) follows immediately. Finally, by (6.3.18) and (6.3.22), we get

$$\begin{aligned} w_b(c(x)) &= L_c(b-1) + \sum_{\ell=1}^{L_c} |B_\ell| \\ &\geq L_c(b+\tau) + (\omega + 1 - L_c)p^{s-1} \\ &\geq \min\{\omega p^{s-1} + b + \tau, (\omega+1)(b+\tau)\}, \end{aligned}$$

which proves the assertion (6.3.15).

By (6.3.14) and (6.3.15), we get the desired result in this case.

II. Next let $b \leq \tau \leq p^{s-1} - 1$. Here by Lemma 6.3.4, we see that $d_b(\mathscr{C}_{\lambda_0}(s, (\omega+1)p^{s-1})) = (\omega+2)b$. Further, by case **I**, we see that

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+b-1)) = \min\{\omega p^{s-1}+b+b-1, (\omega+2)b, (\omega+1)(b+b-1)\} = (\omega+2)b.$$

From this and using the fact that

$$\begin{aligned} \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+b-1) \supseteq \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+b) \supseteq \cdots \supseteq \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+p^{s-1}-1) \\ \supseteq \mathscr{C}_{\lambda_0}(s, (\omega+1)p^{s-1}), \end{aligned}$$

we get

$$\begin{aligned} (\omega+2)b = d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+b-1)) \leq d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+b)) \leq \cdots\cdots \\ \leq d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+p^{s-1}-1)) \leq d_b(\mathscr{C}_{\lambda_0}(s, (\omega+1)p^{s-1})) = (\omega+2)b. \end{aligned}$$

This gives

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) = (\omega + 2)b = \min\{\omega p^{s-1} + b + \tau, (\omega + 2)b, (\omega + 1)(b + \tau)\}$$
$$\text{for } b \leq \tau \leq p^{s-1} - 1.$$

This completes the proof of the lemma. □

Proof of Proposition 6.3.2. It follows immediately from Lemmas 6.3.3-6.3.5. □

6.3.2 The case $b \geq p^{s-1} + 1$

Throughout this section, we assume that $p^{s-1} + 1 \leq b \leq p^s - 1$. In the following proposition, we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)$, where $0 \leq \omega \leq p - 2$ and $1 \leq \tau \leq p^{s-1}$.

Proposition 6.3.3. Let $p^{s-1} + 1 \leq b \leq p^s - 1$ be a fixed integer. For $0 \leq \omega \leq p - 2$ and $1 \leq \tau \leq p^{s-1}$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) \;=\; \min\{\omega p^{s-1} + b + \tau,\ p^s\}.$$

To prove the above proposition, we shall consider the following three cases separately: (i) $\omega = 0$ and $1 \leq \tau \leq p^{s-1}$, (ii) $1 \leq \omega \leq p - 2$ and $\tau = p^{s-1}$, and (iii) $1 \leq \omega \leq p - 2$ and $1 \leq \tau \leq p^{s-1} - 1$.

In the following lemma, we consider the case $\omega = 0$, and we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, \tau)$, where $1 \leq \tau \leq p^{s-1}$.

Lemma 6.3.6. For $1 \leq \tau \leq p^{s-1}$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, \tau)) \;=\; \min\{b + \tau, p^s\}.$$

Proof. To prove the result, we see that the codeword $(x - \lambda_0)^\tau \in \mathscr{C}_{\lambda_0}(s, \tau)$ can be expressed as $(x - \lambda_0)^\tau = \sum_{t=0}^{\tau} E_t x^t$, where $E_t = \binom{\tau}{t}(-\lambda_0)^{\tau - t}$ for $0 \leq t \leq \tau$. From this, we see that the

codeword $(x-\lambda_0)^\tau$ is of the form

$$\big(E_0, E_1, E_2, \cdots\cdots\cdots, E_{\tau-1}, E_\tau, \underbrace{0, 0, \cdots, 0}_{p^s-\tau-1}\big).$$

Now by applying Theorem 6.2.1, we get

$$w_b((x-\lambda_0)^\tau) \;=\; \min\{b+\tau, p^s\} \;=\; \begin{cases} p^s & \text{if } \tau > p^s - b; \\ b+\tau & \text{otherwise,} \end{cases}$$

which implies that

$$d_b(\mathscr{C}_{\lambda_0}(s,\tau)) \;\leq\; \min\{b+\tau, p^s\}. \tag{6.3.27}$$

Next we assert that

$$w_b(c(x)) \;\geq\; \min\{b+\tau, p^s\} \text{ for each non-zero codeword } c(x) \in \mathscr{C}_{\lambda_0}(s,\tau). \tag{6.3.28}$$

To prove this assertion, suppose, on the contrary, that there exists a non-zero codeword $d(x) \in \mathscr{C}_{\lambda_0}(s,\tau)$ satisfying $w_b(d(x)) \leq \min\{b+\tau, p^s\} - 1$. By Theorem 6.2.1(b), we have $\tau + b - 1 \geq \min\{\tau + b, p^s\} - 1 \geq w_b(d(x)) = w_H(d(x)) + e_d + L_d(b-1)$. Since $w_H(d(x)) \geq 2$, $e_d \geq 0$ and $\tau < b$, we see that $2b - 1 > \tau + b - 1 \geq 2 + L_d(b-1)$, which gives $L_d = 1$. From this, we get $\tau + b - 1 \geq w_b(d(x)) = w_H(d(x)) + e_d + (b-1)$, which implies that $w_H(d(x)) + e_d \leq \tau$. In view of this, by applying Theorem 6.2.1(b) again and using the fact that $L_d = 1$, we see that there exists an integer j such that $0 \leq j \leq p^s - 1$ and $x^j d(x) \in \mathscr{C}_{\lambda_0}(s,\tau)$ is of the form $x^j d(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_u x^u$, where $u = w_H(d(x)) + e_d - 1$, $d_i \in \mathbb{F}_{p^m}$ for $0 \leq i \leq u$ and both d_0, d_u are non-zero. Now as $w_H(d(x)) \geq 2$, $e_d \geq 0$ and $w_H(d(x)) + e_d \leq \tau$, we note that $1 \leq u \leq \tau - 1$. Therefore there exists a non-zero codeword $x^j d(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_u x^u \in \mathscr{C}_{\lambda_0}(s,\tau) = \langle (x-\lambda_0)^\tau \rangle$ satisfying deg $x^j d(x) = u \leq \tau - 1$, which is a contradiction.

Now by (6.3.27) and (6.3.28), the desired result follows immediately. □

In the following lemma, we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, (\omega+1)p^{s-1})$, where $1 \leq \omega \leq p-2$.

Lemma 6.3.7. For $1 \leq \omega \leq p-2$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})) \;=\; \min\{(\omega+1)p^{s-1}+b,\; p^s\}.$$

Proof. To prove the result, we see that the codeword $(x-\lambda_0)^{(\omega+1)p^{s-1}} \in \mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})$ can be expressed as $(x-\lambda_0)^{(\omega+1)p^{s-1}} = \sum_{t=0}^{\omega+1} W_t x^{tp^{s-1}}$, where $W_t = \binom{\omega+1}{t}(-\lambda_0)^{(\omega+1-t)p^{s-1}} \neq 0$ for $0 \leq t \leq \omega+1$. This implies that the codeword $(x-\lambda_0)^{(\omega+1)p^{s-1}}$ is of the form

$$\big(W_0, \underbrace{0,0,\cdots,0}_{p^{s-1}-1}, W_1, \underbrace{0,0,\cdots,0}_{p^{s-1}-1}, W_2, \cdots\cdots\cdots, W_\omega, \underbrace{0,0,\cdots,0}_{p^{s-1}-1}, W_{\omega+1}, \underbrace{0,0,0,\cdots,0,0}_{p^s-(\omega+1)p^{s-1}-1}\big).$$

Now by applying Theorem 6.2.1, we see that

$$\begin{aligned} w_b((x-\lambda_0)^{(\omega+1)p^{s-1}}) \;&=\; \begin{cases} p^s & \text{if } b > p^s-(\omega+1)p^{s-1}; \\ (\omega+1)p^{s-1}+1+b-1 & \text{otherwise} \end{cases} \\ &=\; \min\{(\omega+1)p^{s-1}+b,\; p^s\}, \end{aligned}$$

which implies that

$$d_b(\mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})) \;\leq\; \min\{(\omega+1)p^{s-1}+b,\; p^s\}. \tag{6.3.29}$$

Next we assert that

$$\begin{aligned} w_b(c(x)) \;\geq\; \min\{(\omega+1)p^{s-1}+b,\; p^s\} \text{ for each non-zero codeword} \\ c(x) \in \mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1}). \end{aligned} \tag{6.3.30}$$

To prove the above assertion, suppose, on the contrary, that there exists a non-zero codeword $e(x)(\neq 0) \in \mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})$ satisfying $w_b(e(x)) \leq \min\{(\omega+1)p^{s-1}+b,\; p^s\}-1$. Then the codeword $e(x) \in \mathscr{C}_{\lambda_0}(s,(\omega+1)p^{s-1})$ can be uniquely written as $e(x) = (x-\lambda_0)^{(\omega+1)p^{s-1}} f(x)$, where $f(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$ and deg $f(x) < p^s-(\omega+1)p^{s-1}$. Further, we observe that the polynomial $f(x) \in \mathbb{F}_{p^m}[x]$ can be uniquely expressed as $f(x) = x^{i_1} f_1(x^{p^{s-1}}) + x^{i_2} f_2(x^{p^{s-1}}) + \cdots + x^{i_r} f_r(x^{p^{s-1}})$, where $0 \leq i_1 < i_2 < \cdots < i_r < p^{s-1}$ and

$f_j(x^{p^{s-1}})$ is a non-zero polynomial in $x^{p^{s-1}}$ over $\mathbb{F}_{p^m}$ for $1 \leq j \leq r$. This implies that

$$w_H(e(x)) \;=\; \sum_{j=1}^{r} w_H\big(x^{i_j}(x-\lambda_0)^{(\omega+1)p^{s-1}} f_j(x^{p^{s-1}})\big).$$

Using this and by applying Lemma 6.2.1, we see that

$$w_b(e(x)) \;\geq\; w_b(x^{i_1}(x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})). \tag{6.3.31}$$

Further, as $w_b(x^j e(x)) = w_b(e(x))$ for each integer $j \geq 0$, without any loss of generality, we can assume that $i_1 = 0$. By Theorem 2.0.8, we note that $w_H((x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})) \geq \omega+2$. Now let us take $d(x) = (x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}})$, and let us write

$$d(x) \;=\; (x-\lambda_0)^{(\omega+1)p^{s-1}} f_1(x^{p^{s-1}}) \;=\; A_0^{(1)} + A_1^{(1)} x^{p^{s-1}} + \cdots + A_{p-1}^{(1)} x^{p^{s-1}(p-1)},$$

where $A_t^{(1)} \in \mathbb{F}_{p^m}$ for $0 \leq t \leq p-1$ and the Hamming weight of the vector $\Big(A_0^{(1)}, A_1^{(1)}, A_2^{(1)}, \cdots, A_{p-1}^{(1)}\Big)$ is at least $\omega+2$.

By (6.3.31) and using the fact that $i_1 = 0$, we see that $w_b(d(x)) \leq w_b(e(x)) < p^s$, so we can apply Theorem 6.2.1(b) to determine the b-symbol weight of $d(x)$. For this, let $\mathfrak{B}_d$ be a minimal partition of the set $\mathcal{K}_d$ (as defined in Theorem 6.2.1(b)) into subsets of consecutive indices modulo p^s, and let $B_1, B_2, \cdots, B_{L_d}$ be all the distinct parts of the partition $\mathfrak{B}_d$. For $1 \leq i \leq L_d$, let us define

$$s_i \;=\; |\{j : 0 \leq j \leq p-1,\; jp^{s-1} \in B_i\}|, \text{ and let } \mathfrak{F}_d \;=\; \{u : 1 \leq u \leq L_d,\; s_u > 0\}.$$

One can easily observe that $|B_u| \geq 1 + (s_u - 1)p^{s-1}$ for each $u \in \mathfrak{F}_d$. Further, since the Hamming weight of the vector $\big(A_0^{(1)}, A_1^{(1)}, A_2^{(1)}, \cdots, A_{p-1}^{(1)}\big)$ is at least $\omega+2$, we have $\sum\limits_{u \in \mathfrak{F}_d} s_u \geq \omega+2$. In view of this and by applying Theorem 6.2.1(b), we get

$$\begin{aligned} w_b(d(x)) \;&=\; L_d(b-1) + \sum_{\ell=1}^{L_d} |B_\ell| = L_d(b-1) + \sum_{u \in \mathfrak{F}_d} |B_u| + \sum_{\substack{\ell=1 \\ \ell \notin \mathfrak{F}_d}}^{L_d} |B_\ell| \\ &\geq\; L_d(b-1) + \Big(\sum_{u \in \mathfrak{F}_d} s_u - |\mathfrak{F}_d|\Big)p^{s-1} + |\mathfrak{F}_d| + L_d - |\mathfrak{F}_d| \end{aligned}$$

$$\begin{aligned} &\geq bL_d + (\omega + 2 - |\mathfrak{F}_d|)p^{s-1} = (\omega+1)p^{s-1} + b + b(L_d - 1) + (1 - |\mathfrak{F}_d|)p^{s-1} \\ &\geq (\omega+1)p^{s-1} + b + (L_d - |\mathfrak{F}_d|)p^{s-1} \ \geq \ (\omega+1)p^{s-1} + b. \end{aligned}$$

This, by (6.3.31), implies that

$$(\omega+1)p^{s-1}+b-1 \geq \min\{(\omega+1)p^{s-1}+b, p^s\}-1 \geq w_b(e(x)) \geq w_b(d(x)) \geq (\omega+1)p^{s-1}+b,$$

which is a contradiction. This proves the assertion (6.3.30).

Now the desired result follows immediately from (6.3.29) and (6.3.30). □

In the following lemma, we determine the b-symbol distance of the code $\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)$, where $1 \leq \tau \leq p^{s-1}-1$ and $1 \leq \omega \leq p-2$.

Lemma 6.3.8. For $1 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-1}-1$, we have

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)) \ = \ \min\{\omega p^{s-1} + b + \tau, \ p^s\}.$$

Proof. To prove this, we see that the codeword $(x-\lambda_0)^{\omega p^{s-1}+\tau} \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)$ can be expressed as $(x-\lambda_0)^{\omega p^{s-1}+\tau} = \sum_{t=0}^{\omega}\sum_{u=0}^{\tau} W_u^{(t)} x^{u+tp^{s-1}}$, where $W_u^{(t)} = \binom{\omega}{t}\binom{\tau}{u}(-\lambda_0)^{(\omega-t)p^{s-1}+\tau-u}$ for $0 \leq u \leq \tau$ and $0 \leq t \leq \omega$. This implies that the codeword $(x-\lambda_0)^{\omega p^{s-1}+\tau}$ is of the form

$$\Big(W_0^{(0)}, W_1^{(0)}, \cdots, W_\tau^{(0)}, \underbrace{0, 0, \cdots, 0}_{p^{s-1}-\tau-1}, W_0^{(1)}, W_1^{(1)}, \cdots, W_\tau^{(1)}, \underbrace{0, 0, \cdots, 0}_{p^{s-1}-\tau-1}, \cdots\cdots, W_0^{(\omega-1)},$$
$$W_1^{(\omega-1)}, \cdots, W_\tau^{(\omega-1)}, \underbrace{0, 0, \cdots, 0}_{p^{s-1}-\tau-1}, W_0^{(\omega)}, W_1^{(\omega)}, \cdots, W_\tau^{(\omega)}, \underbrace{0, 0, 0, \cdots, 0, 0}_{p^s-\omega p^{s-1}-\tau-1}\Big).$$

Now by applying Theorem 6.2.1, we see that

$$\begin{aligned} w_b((x-\lambda_0)^{\omega p^{s-1}+\tau}) &= \min\{\omega p^{s-1} + b + \tau, \ p^s\} \\ &= \begin{cases} \omega p^{s-1} + \tau + 1 + b - 1 & \text{if } \tau \leq p^s - \omega p^{s-1} - b; \\ p^s & \text{otherwise,} \end{cases} \end{aligned}$$

which implies that

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) \ \leq \ \min\{\omega p^{s-1} + b + \tau, \ p^s\}. \tag{6.3.32}$$

Next we assert that

$$w_b(c(x)) \ \geq \ \min\{\omega p^{s-1}+b+\tau, \ p^s\} \ \text{ for each non-zero codeword } \ c(x) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau). \tag{6.3.33}$$

To prove the above assertion, let $c(x) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1}+\tau)$ be a non-zero codeword satisfying $w_b(c(x)) < p^s$. Then the codeword $c(x) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)$ can be uniquely written as $c(x) = (x - \lambda_0)^{\omega p^{s-1}+\tau} f(x)$, where $f(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$ and deg $f(x) < p^s - \omega p^{s-1} - \tau$. If we take $g(x) = (x - \lambda_0)^{\tau} f(x)$, then the codeword $c(x)$ can be rewritten as $c(x) = (x - \lambda_0)^{\omega p^{s-1}} g(x)$, where $g(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$, $\tau \leq$ deg $g(x) < p^s - \omega p^{s-1}$ and $(x - \lambda_0)^{\tau}$ divides $g(x)$ in $\mathbb{F}_{p^m}[x]$. We further observe that the polynomial $g(x) = (x - \lambda_0)^{\tau} f(x)$ can be uniquely expressed as $g(x) = x^{i_1} g_1(x^{p^{s-1}}) + x^{i_2} g_2(x^{p^{s-1}}) + \cdots + x^{i_r} g_r(x^{p^{s-1}})$, where $0 \leq i_1 < i_2 < \cdots < i_r < p^{s-1}$ and $g_\ell(x^{p^{s-1}})$ is a non-zero polynomial in $x^{p^{s-1}}$ over $\mathbb{F}_{p^m}$ for $1 \leq \ell \leq r$. This implies that

$$w_H(c(x)) \ = \ \sum_{j=1}^{r} w_H\big(x^{i_j}(x - \lambda_0)^{\omega p^{s-1}} g_j(x^{p^{s-1}})\big). \tag{6.3.34}$$

Further, as $w_b(x^e c(x)) = w_b(c(x))$ for each integer $e \geq 0$, without any loss of generality, we can assume that $i_1 = 0$. By Theorem 2.0.8, we note that

$$w_H(x^{i_\ell}(x - \lambda_0)^{\omega p^{s-1}} g_\ell(x^{p^{s-1}})) \ \geq \ \omega + 1 \ \text{ for } \ 1 \leq \ell \leq r.$$

For $1 \leq \ell \leq r$, we can write $x^{i_\ell}(x - \lambda_0)^{\omega p^{s-1}} g_\ell(x^{p^{s-1}}) = x^{i_\ell}\big\{A_0^{(\ell)} + A_1^{(\ell)} x^{p^{s-1}} + \cdots + A_{p-1}^{(\ell)} x^{p^{s-1}(p-1)}\big\}$, where $A_t^{(\ell)} \in \mathbb{F}_{p^m}$ for $0 \leq t \leq p-1$ and the Hamming weight of the vector $\mathfrak{A}_\ell = \big(A_0^{(\ell)}, A_1^{(\ell)}, A_2^{(\ell)}, \cdots, A_{p-1}^{(\ell)}\big)$ is at least $\omega + 1$. In view of this, by (6.3.34) and using the fact that $i_1 = 0$, we see that the codeword $c(x) \in \mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)$ is of the form

$$c \ = \ \Big(A_0^{(1)}, \underbrace{0, 0, \cdots, 0, 0}_{i_2-1}, A_0^{(2)}, \underbrace{0, 0, \cdots, 0, 0}_{i_3-i_2-1}, A_0^{(3)}, \cdots, A_0^{(r-1)}, \underbrace{0, 0, \cdots, 0}_{i_r-i_{r-1}-1}, A_0^{(r)}, \underbrace{0, 0, \cdots, 0}_{p^{s-1}-i_r-1},$$

$$A_1^{(1)}, \underbrace{0,0,\cdots,0,0}_{i_2-1}, A_1^{(2)}, \underbrace{0,0,\cdots,0,0}_{i_3-i_2-1}, A_1^{(3)}, \cdots, A_1^{(r-1)}, \underbrace{0,0,\cdots,0}_{i_r-i_{r-1}-1}, A_1^{(r)}, \underbrace{0,0,\cdots,0}_{p^{s-1}-i_r-1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$A_{p-2}^{(1)}, \underbrace{0,0,\cdots,0}_{i_2-1}, A_{p-2}^{(2)}, \underbrace{0,0,\cdots,0}_{i_3-i_2-1}, A_{p-2}^{(3)}, \cdots, A_{p-2}^{(r-1)}, \underbrace{0,0,\cdots,0}_{i_r-i_{r-1}-1}, A_{p-2}^{(r)}, \underbrace{0,0,\cdots,0}_{p^{s-1}-i_r-1},$$
$$A_{p-1}^{(1)}, \underbrace{0,0,\cdots,0}_{i_2-1}, A_{p-1}^{(2)}, \underbrace{0,0,\cdots,0}_{i_3-i_2-1}, A_{p-1}^{(3)}, \cdots, A_{p-1}^{(r-1)}, \underbrace{0,0,\cdots,0}_{i_r-i_{r-1}-1}, A_{p-1}^{(r)}, \underbrace{0,0,\cdots,0}_{p^{s-1}-i_r-1}\Big).$$

Since $w_b(c(x)) < p^s$, we will apply Theorem 6.2.1(b) to prove the assertion (6.3.33). For this, let $\mathfrak{B}_c$ be a minimal partition of the set $\mathcal{K}_c$ (as defined in Theorem 6.2.1(b)) into subsets of consecutive indices modulo p^s, and let $B_1, B_2, \cdots, B_{L_c}$ be all the distinct parts of the partition $\mathfrak{B}_c$. Now by Theorem 6.2.1(b), we see that

$$w_b(c(x)) \;=\; L_c(b-1) + \sum_{\ell=1}^{L_c} |B_\ell|. \tag{6.3.35}$$

Next let us define

$$d_\ell = |\{j : 0 \le j \le p-1,\ jp^{s-1} \in B_\ell\}| \ \text{ for } \ 1 \le \ell \le L_c,$$

and let

$$\mathfrak{F}_c = \{u : 1 \le u \le L_c,\ d_u > 0\}.$$

One can easily observe that

$$1 \le |\mathfrak{F}_c| \le L_c \ \text{ and } \ |B_u| \;\ge\; 1 + (d_u - 1)p^{s-1} \ \text{ for each } \ u \in \mathfrak{F}_c. \tag{6.3.36}$$

Further, since the Hamming weight of the vector $\mathfrak{A}_1 = \left(A_0^{(1)}, A_1^{(1)}, A_2^{(1)}, \cdots, A_{p-1}^{(1)}\right)$ is at least $\omega + 1$, we have

$$\sum_{u \in \mathfrak{F}_c} d_u \;\ge\; \omega + 1. \tag{6.3.37}$$

Now when $L_c > |\mathfrak{F}_c|$, by (6.3.35)-(6.3.37) and using the fact that $\tau \leq p^{s-1} - 1$, we get

$$\begin{aligned} w_b(c(x)) &= L_c(b-1) + \sum_{u \in \mathfrak{F}_c} |B_u| + \sum_{\substack{\ell=1 \\ \ell \notin \mathfrak{F}_c}}^{L_c} |B_\ell| \\ &\geq L_c(b-1) + (\sum_{u \in \mathfrak{F}_c} d_u - |\mathfrak{F}_c|)p^{s-1} + |\mathfrak{F}_c| + L_c - |\mathfrak{F}_c| \\ &\geq bL_c + (\omega + 1 - |\mathfrak{F}_c|)p^{s-1} \\ &\geq (\omega+1)p^{s-1} + b + (L_c - 1 - |\mathfrak{F}_c|)p^{s-1} \\ &\geq \omega p^{s-1} + b + \tau, \end{aligned}$$

which proves the assertion (6.3.33) in this case.

From this point on, we assume that $|\mathfrak{F}_c| = L_c$. Here we have

$$d_1 + d_2 + \cdots + d_{L_c} \geq \omega + 1,\ d_\ell \geq 1 \text{ and } |B_\ell| \geq 1 + (d_\ell - 1)p^{s-1} \text{ for } 1 \leq \ell \leq L_c. \tag{6.3.38}$$

Now we shall distinguish the following two cases: **I.** $d_1 + d_2 + \cdots + d_{L_c} \geq \omega + 2$ and **II.** $d_1 + d_2 + \cdots + d_{L_c} = \omega + 1$.

I. When $d_1 + d_2 + \cdots + d_{L_c} \geq \omega + 2$, by (6.3.35), (6.3.38) and using the fact that $\tau \leq p^{s-1} - 1$, we see that

$$\begin{aligned} w_b(c(x)) &= L_c(b-1) + \sum_{\ell=1}^{L_c} |B_\ell| \\ &\geq L_c(b-1) + (d_1 + d_2 + \cdots + d_{L_c} - L_c)p^{s-1} + L_c \\ &\geq (\omega+1)p^{s-1} + b + (L_c - 1)(b - p^{s-1}) \\ &\geq \omega p^{s-1} + b + \tau, \end{aligned}$$

which proves the assertion (6.3.33) in this case.

II. Next let $d_1 + d_2 + \cdots + d_{L_c} = \omega + 1$. This implies that $w_H((x-\lambda_0)^{\omega p^{s-1}} g_1(x^{p^{s-1}})) = \omega + 1$. Here we assert that

$$\sum_{\ell=1}^{L_c} |B_\ell| \geq \tau + L_c + (\omega + 1 - L_c)p^{s-1}. \tag{6.3.39}$$

To prove the assertion (6.3.39), we first recall that $d_\ell = |\{j : 0 \leq j \leq p-1,\ jp^{s-1} \in B_\ell\}|$. Now we observe that for $1 \leq \ell \leq L_c$, the part B_ℓ of the partition $\mathfrak{B}_c$ is of the form

$$B_\ell \ = \ \{\upsilon_\ell p^{s-1}, \upsilon_\ell p^{s-1}+1, \cdots, (\upsilon_\ell + d_\ell - 1)p^{s-1}\} \cup T_\ell \cup S_\ell,$$

where υ_ℓ is an integer satisfying $0 \leq \upsilon_\ell \leq p-1$, the set T_ℓ is either empty or of the form $\{(\upsilon_\ell - 1)p^{s-1} + i_{a_\ell}, (\upsilon_\ell - 1)p^{s-1} + i_{a_\ell} + 1, \cdots, \upsilon_\ell p^{s-1} - 1\}$ with a_ℓ as an integer satisfying $a_\ell \in \{2, 3, \cdots, r\}$ and $A^{(a_\ell)}_{\upsilon_\ell - 1}$ as non-zero, and the set S_ℓ is either empty or of the form $\{(\upsilon_\ell + d_\ell - 1)p^{s-1} + 1, (\upsilon_\ell + d_\ell - 1)p^{s-1} + 2, \cdots, (\upsilon_\ell + d_\ell - 1)p^{s-1} + i_{b_\ell}\}$ with b_ℓ as an integer satisfying $b_\ell \in \{2, 3, \cdots, r\}$ and $A^{(b_\ell)}_{\upsilon_\ell + d_\ell - 1}$ as non-zero. For $1 \leq \ell \leq L_c$, it is easy to see that

$$|T_\ell| \ = \ p^{s-1} - i_{a_\ell} \ \text{ if } \ T_\ell \neq \emptyset \quad \text{and} \quad |S_\ell| \ = \ i_{b_\ell} \ \text{ if } \ S_\ell \neq \emptyset. \tag{6.3.40}$$

Further, for each ℓ, we note that $|B_\ell| = (d_\ell - 1)p^{s-1} + 1 + |T_\ell| + |S_\ell|$. This implies that

$$\begin{aligned} \sum_{\ell=1}^{L_c} |B_\ell| \ &= \ \sum_{\ell=1}^{L_c} \big((d_\ell - 1)p^{s-1} + 1\big) + \sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big) \\ &= \ L_c + (\omega + 1 - L_c)p^{s-1} + \sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big). \end{aligned} \tag{6.3.41}$$

In view of this, we see that to prove the assertion (6.3.39), it is enough to show that

$$\sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big) \ \geq \ \tau. \tag{6.3.42}$$

To prove this, for $2 \leq t \leq r$, let us define

$$\mathcal{M}_t \ = \ |\{y \in \mathbb{Z} : 0 \leq y \leq p-1,\ yp^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} T_\ell\}|$$

and

$$\mathcal{N}_t \ = \ |\{y \in \mathbb{Z} : 0 \leq y \leq p-1,\ yp^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} S_\ell\}|.$$

Further, for $2 \leq t \leq r$, we note that

$$\begin{aligned}&\{i \in \mathbb{Z} : 0 \leq i \leq p-1,\ ip^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} \big(B_\ell \setminus (T_\ell \cup S_\ell)\big)\}\\ &= \bigcup_{\ell=1}^{L_c} \{\upsilon_\ell p^{s-1} + i_t, (\upsilon_\ell + 1)p^{s-1} + i_t, \cdots, (\upsilon_\ell + d_\ell - 2)p^{s-1} + i_t\}.\end{aligned}$$

Now for $2 \leq t \leq r$, we observe that

$$\begin{aligned}w_H(\mathfrak{A}_t) &= w_H(\big(A_0^{(t)}, A_1^{(t)}, A_2^{(t)}, \cdots, A_{p-1}^{(t)}\big))\\ &\leq |\{i \in \mathbb{Z} : 0 \leq i \leq p-1,\ ip^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} B_\ell\}|\\ &= |\{i \in \mathbb{Z} : 0 \leq i \leq p-1,\ ip^{s-1} + i_t \in \bigcup_{\ell=1}^{L_c} \big(B_\ell \setminus (T_\ell \cup S_\ell)\big)\}|\\ &\quad + \mathcal{M}_t + \mathcal{N}_t\\ &= \sum_{\ell=1}^{L_c}(d_\ell - 1) + \mathcal{M}_t + \mathcal{N}_t \ = \ \omega + 1 - L_c + \mathcal{M}_t + \mathcal{N}_t. \qquad (6.3.43)\end{aligned}$$

Since $w_H(\mathfrak{A}_t) \geq \omega + 1$, we get $\mathcal{M}_t + \mathcal{N}_t \geq L_c$ for $2 \leq t \leq r$. Further, for $2 \leq t \leq r$, we note that

$$\begin{aligned}\mathcal{M}_t &= |\{\ell \in \mathbb{Z} : 1 \leq \ell \leq L_c, T_\ell \neq \emptyset \text{ and } a_\ell \leq t\}| \text{ and}\\ \mathcal{N}_t &= |\{\ell \in \mathbb{Z} : 1 \leq \ell \leq L_c, S_\ell \neq \emptyset \text{ and } b_\ell \geq t\}|.\end{aligned} \qquad (6.3.44)$$

This implies that $\mathcal{M}_t \leq L_c$ and $\mathcal{N}_t \leq L_c$ for $2 \leq t \leq r$. Now we shall consider the following two cases separately:

A. There exists an integer h satisfying $2 \leq h \leq r$ and $w_H(\mathfrak{A}_h) \geq \omega + 2$.

B. $w_H(\mathfrak{A}_j) = \omega + 1$ for $2 \leq j \leq r$.

A. Suppose that there exists an integer h satisfying $2 \leq h \leq r$ and $w_H(\mathfrak{A}_h) \geq \omega + 2$. In this case, by (6.3.43), we observe that $\mathcal{M}_h + \mathcal{N}_h \geq L_c + 1$. Since $\mathcal{M}_h \leq L_c$ and $\mathcal{N}_h \leq L_c$, we must have $\mathcal{M}_h \geq 1$ and $\mathcal{N}_h \geq 1$. From this and by (6.3.44), we observe that there exist integers u, v satisfying $1 \leq u, v \leq L_c$, $a_u \leq h$ and $b_v \geq h$. This, by (6.3.40), gives $|T_u| + |S_v| = p^{s-1} - i_{a_u} + i_{b_v} \geq p^{s-1} - i_h + i_h \geq \tau$,

which implies that $\sum_{\ell=1}^{L_c}\Big(|T_\ell|+|S_\ell|\Big)\geq\tau$.

B. Now suppose that $w_H(\mathfrak{A}_j)=\omega+1$ for $2\leq j\leq r$. In this case, we have $w_H\big(x^{i_j}(x-\lambda_0)^{\omega p^{s-1}}g_j(x^{p^{s-1}})\big)=\omega+1$ for $1\leq j\leq r$. Now we claim that $g_j(\lambda_0^{p^{s-1}})\neq 0$ for $1\leq j\leq r$. For, if $g_w(\lambda_0^{p^{s-1}})=0$ for some integer w satisfying $1\leq w\leq r$, then $x-\lambda_0$ divides $g_w(x^{p^{s-1}})$ in $\mathbb{F}_{p^m}[x]$. This implies that $x^{i_w}(x-\lambda_0)^{\omega p^{s-1}}g_w(x^{p^{s-1}})\in\mathscr{C}_{\lambda_0}(s,\omega p^{s-1}+1)$. By Theorem 2.0.8, we note that $d_H(\mathscr{C}_{\lambda_0}(s,\omega p^{s-1}+1))=\omega+2$. This implies that $\omega+2\leq w_H\big(x^{i_w}(x-\lambda_0)^{\omega p^{s-1}}g_w(x^{p^{s-1}})\big)$. This is a contradiction, as $w_H\big(x^{i_j}(x-\lambda_0)^{\omega p^{s-1}}g_j(x^{p^{s-1}})\big)=\omega+1$ for $1\leq j\leq r$.

This shows that $g_j(\lambda_0^{p^{s-1}})\neq 0$ for $1\leq j\leq r$. This, by Lemma 6.3.1, implies that $i_r\geq\tau$, $p^{s-1}-i_2\geq\tau$ and $p^{s-1}-i_{t+1}+i_t\geq\tau$ for $2\leq t\leq r-1$. Now let us consider the following two cases separately: **(i)** $T_1=\emptyset$ and **(ii)** $T_1\neq\emptyset$.

(i) Let us first assume that $T_1=\emptyset$. In this case, if either $S_1=\emptyset$ or $S_1\neq\emptyset$ and $b_1<r$, then by (6.3.44), we have $\mathcal{M}_r\leq L_c-1$ and $\mathcal{N}_r\leq L_c-1$. This implies that $\mathcal{M}_r\geq 1$ and $\mathcal{N}_r\geq 1$, as $\mathcal{N}_r+\mathcal{M}_r\geq L_c$. From this and by (6.3.44), we observe that there exists an integer v satisfying $1\leq v\leq L_c$ and $b_v\geq r$. As $b_v\leq r$, by (6.3.40), we get $|S_v|=i_{b_v}=i_r\geq\tau$. This gives $\sum_{\ell=1}^{L_c}\Big(|T_\ell|+|S_\ell|\Big)\geq|S_v|\geq\tau$.

On the other hand, when $S_1\neq\emptyset$ and $b_1=r$, by (6.3.40), we get $\sum_{\ell=1}^{L_c}\Big(|T_\ell|+|S_\ell|\Big)\geq|S_1|=i_r\geq\tau$.

(ii) Now let us assume that $T_1\neq\emptyset$. In this case, if $a_1=2$, then by (6.3.40), we have $\sum_{\ell=1}^{L_c}\Big(|T_\ell|+|S_\ell|\Big)\geq|T_1|=p^{s-1}-i_2\geq\tau$. Next assume that $a_1>2$. Here if $S_1\neq\emptyset$ and $b_1\geq a_1-1$, then by (6.3.40) again, we get

$$\sum_{\ell=1}^{L_c}\Big(|T_\ell|+|S_\ell|\Big)\geq|T_1|+|S_1|=p^{s-1}-i_{a_1}+i_{b_1}\geq p^{s-1}-i_{a_1}+i_{a_1-1}\geq\tau.$$

On the other hand, when either $S_1=\emptyset$ or $S_1\neq\emptyset$ and $b_1<a_1-1$, then by (6.3.44), we get $\mathcal{M}_{a_1-1}\leq L_c-1$ and $\mathcal{N}_{a_1-1}\leq L_c-1$. This

implies that $\mathcal{M}_{a_1-1} \geq 1$ and $\mathcal{N}_{a_1-1} \geq 1$, as $\mathcal{M}_{a_1-1} + \mathcal{N}_{a_1-1} \geq L_c$. From this and by (6.3.44), we observe that there exist integers u, v satisfying $1 \leq u, v \leq L_c$, $a_u \leq a_1 - 1$ and $b_v \geq a_1 - 1$. This, by (6.3.40) again, gives $|T_u| + |S_v| = p^{s-1} - i_{a_u} + i_{b_v} \geq p^{s-1} - i_{a_1-1} + i_{a_1-1} \geq \tau$, which implies that $\sum_{\ell=1}^{L_c} \Big(|T_\ell| + |S_\ell|\Big) \geq \tau$.

This completes the proof of the assertion (6.3.42).

Now by (6.3.41) and (6.3.42), the asssertion (6.3.39) follows immediately. Furthermore, by (6.3.35) and (6.3.39), we see that

$$w_b(c(x)) \;=\; L_c(b-1) + \sum_{\ell=1}^{L_c} |B_\ell| \;\geq\; bL_c + \tau + (\omega + 1 - L_c)p^{s-1} \;\geq\; \omega p^{s-1} + b + \tau,$$

which proves the assertion (6.3.33) in this case.

Now by (6.3.32) and (6.3.33), the desired result follows immediately. □

Proof of Proposition 6.3.3. It follows immediately from Lemmas 6.3.6-6.3.8. □

Proof of Theorem 6.3.2. For $0 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-1}$, by applying Propositions 6.3.2 and 6.3.3, we get

$$d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) = \begin{cases} \min\{\omega p^{s-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\} \\ \quad \text{if} \;\; 2 \leq b \leq p^{s-1}; \\ \min\{\omega p^{s-1} + b + \tau, p^s\} \quad \text{if} \;\; p^{s-1} < b < p^s. \end{cases} \tag{6.3.45}$$

Further, for $1 \leq k \leq s-1$, $0 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-k-1}$, by Proposition 6.3.1, we see that

$$d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) = \begin{cases} p^k d_b(\mathscr{C}_{\lambda_0}(s-k, \omega p^{s-k-1} + \tau)) \\ \quad \text{if} \;\; 2 \leq b \leq p^{s-k} - 1; \\ p^s \quad \text{if} \;\; p^{s-k} \leq b < p^s. \end{cases} \tag{6.3.46}$$

Now on taking $k = s-1$ in (6.3.46) and by applying Theorem 6.3.1, we get

$$d_b(\mathscr{C}_{\lambda_0}(s, p^s - p + \omega + 1)) = \begin{cases} p^{s-1}\min\{\omega + b + 1, p\} & \text{if } 2 \le b \le p-1; \\ p^s & \text{if } p \le b < p^s. \end{cases}$$

Finally, for $1 \le k \le s-2$, $0 \le \omega \le p-2$ and $1 \le \tau \le p^{s-k-1}$, by (6.3.45) and (6.3.46), we obtain

$$d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) = \begin{cases} p^k \min\{\omega p^{s-k-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\} \\ \quad \text{if } 2 \le b \le p^{s-k-1}; \\ p^k \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\} \\ \quad \text{if } p^{s-k-1} < b < p^{s-k}; \\ p^s \quad \text{if } p^{s-k} \le b < p^s. \end{cases}$$

This completes the proof of the theorem. □

Remark 6.3.2. By Theorems 6.3.1 and 6.3.2, we see that b-symbol distances of λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ depend only on b, p and s, and are independent of the choice of λ and m. In fact, one can show that each non-trivial λ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$ is equivalent to a non-trivial cyclic code of length p^s over $\mathbb{F}_{p^m}$ as follows:

For $1 \le \nu \le p^s - 1$, let us define a map $\psi_{\lambda_0} : \mathscr{C}_{\lambda_0}(s, \nu) \to \mathscr{C}_1(s, \nu)$ as

$$\psi_{\lambda_0}\big((x-\lambda_0)^\nu f(x)\big) = (\lambda_0 x - \lambda_0)^\nu f(\lambda_0 x) = (x-1)^\nu \lambda_0^\nu f(\lambda_0 x) \in \mathscr{C}_1(s, \nu)$$

for each codeword $(x-\lambda_0)^\nu f(x) \in \mathscr{C}_{\lambda_0}(s, \nu)$, (note that each non-zero codeword $c(x) \in \mathscr{C}_{\lambda_0}(s, \nu)$ can be uniquely expressed as $c(x) = (x-\lambda_0)^\nu f(x)$, where $f(x)(\neq 0) \in \mathbb{F}_{p^m}[x]$ and deg $f(x) < p^s - \nu$). One can easily observe that the map ψ_{λ_0} is a ring isomorphism and that $w_b(c(x)) = w_b(\psi_{\lambda_0}(c(x)))$ for each $c(x) \in \mathscr{C}_{\lambda_0}(s, \nu)$. From this, it follows that the codes $\mathscr{C}_{\lambda_0}(s, \nu)$ and $\mathscr{C}_1(s, \nu)$ are equivalent, and that $d_b(\mathscr{C}_{\lambda_0}(s, \nu)) = d_b(\mathscr{C}_1(s, \nu))$ for $1 \le \nu \le p^s - 1$. □

Remark 6.3.3. Theorem 3.11 of Sun et al. [77] and Theorem 24 of Dinh et al. [24] follow from Theorems 6.3.1 and 6.3.2 as special cases when $b = 2$. □

6.4 Determination of MDS b-symbol constacyclic codes of length p^s over $\mathbb{F}_{p^m}$

Ding et al. [28, Th. 2.5] showed that an MDS b-symbol code $\mathcal{C}$ of length N over $\mathbb{F}_{p^m}$ satisfying $d_b(\mathcal{C}) < N$ is also an MDS $(b+1)$-symbol code for each integer $b \geq 2$. However, the converse is not true in general, which we illustrate in the following example.

Example 6.4.1. Let $p = 5$, $s = 2$, $m = 1$ and $\lambda = 1$. Consider the cyclic code $\mathscr{C}_1(2,3) = \langle (x-1)^3 \rangle$ of length 25 over $\mathbb{F}_5$. By Theorems 2.0.8 and 6.3.2, we see that $|\mathscr{C}_1(2,3)| = 5^{22}$, $d_2(\mathscr{C}_1(2,3)) = 4$ and $d_3(\mathscr{C}_1(2,3)) = 6$. Now by (6.2.2), we see that the code $\mathscr{C}_1(2,3)$ is an MDS 3-symbol code, but not an MDS 2-symbol (symbol-pair) code. □

In this section, we shall apply Theorems 2.0.8, 6.3.1 and 6.3.2 to determine all MDS b-symbol constacyclic codes of length p^s over $\mathbb{F}_{p^m}$, where b is an integer satisfying $2 \leq b \leq p^s - 1$. For this, we recall, by Theorem 2.0.8, that for each non-zero $\lambda \in \mathbb{F}_{p^m}$, there exists $\lambda_0 \in \mathbb{F}_{p^m}$ satisfying $\lambda = \lambda_0^{p^s}$, and that all the distinct λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ are given by $\mathscr{C}_{\lambda_0}(s,\nu) = \langle (x-\lambda_0)^\nu \rangle$, where $0 \leq \nu \leq p^s$. We also recall that an MDS b-symbol code has to be non-zero. Further, one can easily see that the code $\mathscr{C}_{\lambda_0}(s,0) = \langle 1 \rangle$ is an MDS b-symbol code. In the following theorem, we determine all non-trivial MDS b-symbol constacyclic codes of length p^s over $\mathbb{F}_{p^m}$, where $s \geq 1$ and $2 \leq b \leq p^s - 1$.

Theorem 6.4.1. Let $\lambda = \lambda_0^{p^s}$, where λ_0 is a non-zero element of $\mathbb{F}_{p^m}$. All the distinct non-trivial MDS b-symbol λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ are given by

$$\mathscr{C}_{\lambda_0}(s,\nu) \;=\; \langle (x-\lambda_0)^\nu \rangle,$$

where

- $1 \leq \nu \leq p^s - b$ when $s \geq 1$ and $p^{s-1} + 1 \leq b \leq p^s - 1$.
- $\nu \in \{p^s - b, 1, 2, \cdots, b\} \bigcup \left(\bigcup_{\omega} \{(\omega+1)p^{s-1} - b, (\omega+1)p^{s-1} - b + 1, (\omega+1)p^{s-1} - b + 2, \cdots, (\omega+1)b\} \right)$ when $s \geq 2$ and $2 \leq b \leq p^{s-1} - 1$. Here the union $\bigcup_{\omega}$ runs over all integers ω satisfying $1 \leq \omega \leq p-2$ and $(\omega+2)b - (\omega+1)p^{s-1} \geq 0$.

- $1 \leq \nu \leq (p-1)p^{s-1}$ when $s \geq 2$ and $b = p^{s-1}$.

Proof. To prove the result, we note, by Theorem 2.0.8, that $|\mathscr{C}_{\lambda_0}(s,\nu)| = p^{m(p^s-\nu)}$. From this and by (6.2.2), we see that the code $\mathscr{C}_{\lambda_0}(s,\nu)$ is an MDS b-symbol code if and only if $p^{m(p^s-\nu)} = |\mathscr{C}_{\lambda_0}(s,\nu)| = p^{m(p^s-d_b(\mathscr{C}_{\lambda_0}(s,\nu))+b)}$, which holds if and only if

$$\nu \;=\; d_b(\mathscr{C}_{\lambda_0}(s,\nu)) - b. \tag{6.4.1}$$

When $s = 1$, we have $2 \leq b \leq p-1$. Further, by Theorem 6.3.1, we note that $d_b(\mathscr{C}_{\lambda_0}(1,\nu)) = \min\{\nu+b,\ p\}$ for $1 \leq \nu \leq p-1$. From this and by (6.4.1), we see that the code $\mathscr{C}_{\lambda_0}(1,\nu)$ is an MDS b-symbol code if and only if $d_b(\mathscr{C}_{\lambda_0}(1,\nu)) = \nu + b$, which holds if and only if $\nu \leq p-b$. Therefore all the distinct non-trivial MDS b-symbol λ-constacyclic codes of length p over $\mathbb{F}_{p^m}$ are given by $\langle (x-\lambda_0)^\nu \rangle$, where $\nu \in \{1, 2, \cdots, p-b\}$.

From now on, throughout the proof, we assume that $s \geq 2$. By Remark 6.3.1, we see that each integer $\nu \in \{1, 2, \cdots, p^s-1\}$ can be uniquely written as $\nu = p^s - p^{s-k} + \omega p^{s-k-1} + \tau$, where $0 \leq k \leq s-1$, $1 \leq \tau \leq p^{s-k-1}$ and $0 \leq \omega \leq p-2$. Now we shall distinguish the following three cases: **A.** $p^{s-1}+1 \leq b \leq p^s-1$, **B.** $2 \leq b \leq p^{s-1}-1$, and **C.** $b = p^{s-1}$.

A. First of all, let $p^{s-1}+1 \leq b \leq p^s-1$. Here by Theorem 6.3.2, we see that

$$d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) \;=\; p^k \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\}, \tag{6.4.2}$$

where $0 \leq k \leq s-1$, $1 \leq \tau \leq p^{s-k-1}$ and $0 \leq \omega \leq p-2$. Now we shall consider the following two cases separately: (i) $k \geq 1$ and (ii) $k = 0$.

(i) First let $k \geq 1$. Here we note that $\omega p^{s-k-1} + b + \tau \geq p^{s-1} + 2 > p^{s-k}$. Now by (6.4.2), we see that $d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) = p^s$, which implies that

$$\begin{aligned} \nu - d_b(\mathscr{C}_{\lambda_0}(s,\nu)) + b \;&=\; p^s - d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) \\ &\quad -p^{s-k} + \omega p^{s-k-1} + \tau + b \\ &=\; \omega p^{s-k-1} + \tau + b - p^{s-k} \;>\; 0. \end{aligned}$$

From this and by (6.4.1), we see that the code $\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)$ is not an MDS b-symbol code.

(ii) Next let $k = 0$. Here we have $\nu = \omega p^{s-1} + \tau$, where $1 \leq \tau \leq p^{s-1}$ and $0 \leq \omega \leq p-2$. Further, by (6.4.2), we see that

$$\begin{aligned} \nu - d_b(\mathscr{C}_{\lambda_0}(s,\nu)) + b &= \omega p^{s-1} + \tau - d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) + b \\ &= \omega p^{s-1} + b + \tau - \min\{\omega p^{s-1} + b + \tau, p^s\}. \end{aligned}$$

From this, we note that $\omega p^{s-1} + \tau - d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) + b = 0$ if and only if $\tau \leq p^s - \omega p^{s-1} - b$ and $0 \leq \omega \leq p-2$.

On combining the above cases (i) and (ii), we see that when $s \geq 2$ and $p^{s-1} + 1 \leq b \leq p^s - 1$, all the distinct non-trivial MDS b-symbol λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ are given by $\langle (x - \lambda_0)^\nu \rangle$, where $1 \leq \nu \leq p^s - b$.

B. Next let $2 \leq b \leq p^{s-1} - 1$. Let k be an integer satisfying $0 \leq k \leq s-1$. Now according to whether the integer k satisfies $b \leq p^{s-k-1}$ or $b \geq p^{s-k-1} + 1$, we shall consider the following two cases separately.

(i) Let k be an integer satisfying $0 \leq k \leq s-1$ and $b \leq p^{s-k-1}$. As $b \leq p^{s-k-1}$, we have $k \leq s-2$. Next we note, by Theorem 6.3.2, that
$d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau))$

$$= p^k \min\{\omega p^{s-k-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\},$$

where $1 \leq \tau \leq p^{s-k-1}$ and $0 \leq \omega \leq p-2$. We also observe that $\omega p^{s-k-1} + b + \tau \leq p^{s-k}$ and the equality holds if and only if $\omega = p-2$ and $\tau = b = p^{s-k-1}$. Further, we see that

$$\begin{aligned} \nu - d_b(\mathscr{C}_{\lambda_0}(s,\nu)) + b &= b - d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) \\ &\quad + p^s - p^{s-k} + \omega p^{s-k-1} + \tau \\ &= (p^k - 1)(p^{s-k} - \omega p^{s-k-1} - \tau - b) + \omega p^{s-1} \end{aligned}$$

$$-p^k \min\{\omega p^{s-k-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\}$$
$$+\tau p^k + bp^k.$$

Now first let $1 \leq k \leq s-2$. Here we observe that $p^s - p^{s-k} + \omega p^{s-k-1} + \tau - d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau) + b = 0$ if and only if $p^{s-k} = \omega p^{s-k-1} + \tau + b$ and $\omega p^{s-k-1} + \tau + b = \min\{\omega p^{s-k-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\}$, which holds if and only if $\omega = p-2$ and $\tau = b = p^{s-k-1}$. From this and by (6.4.1), we see that the code $\mathscr{C}_{\lambda_0}(s, p^s - b)$ is an MDS b-symbol code when $1 \leq k \leq s-2$ and $b = p^{s-k-1}$.

Next let $k = 0$. Here we see that $\omega p^{s-1} + \tau - d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau) + b = 0$ if and only if $\omega p^{s-1} + \tau + b = \min\{\omega p^{s-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\}$, which holds if and only if $\tau \leq b$ when $\omega = 0$, while $p^{s-1} - b \leq \tau \leq \omega b + b - \omega p^{s-1}$ when $1 \leq \omega \leq p-2$ satisfies $(\omega+2)b - (\omega+1)p^{s-1} \geq 0$.

(ii) Let k be an integer satisfying $0 \leq k \leq s-1$ and $b \geq p^{s-k-1}+1$. As $b \leq p^{s-1}-1$, we must have $k \geq 1$. Further, by Theorem 6.3.2, we have $d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) = p^k \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\}$. This gives

$$\begin{aligned}
\nu - d_b(\mathscr{C}_{\lambda_0}(s,\nu)) + b &= b - d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) \\
&\quad + p^s - p^{s-k} + \omega p^{s-k-1} + \tau \\
&= p^k\Big(\omega p^{s-k-1} + \tau + b - \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\}\Big) \\
&\quad + (p^k - 1)(p^{s-k} - \omega p^{s-k-1} - \tau - b).
\end{aligned}$$

We further observe that $p^s - p^{s-k} + \omega p^{s-k-1} + \tau - d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau) + b = 0$ if and only if $p^{s-k} = \omega p^{s-k-1} + \tau + b = \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\}$. This, by (6.4.1), shows that the code $\mathscr{C}_{\lambda_0}(s, \nu)$ is an MDS b-symbol code if and only if $\nu = p^s - b$ when $1 \leq k \leq s-1$ and $b \geq p^{s-k-1} + 1$.

Now by (6.4.1) and on combining the above two cases, part **B** follows immediately.

C. Next let $b = p^{s-1}$. Here also, we shall distinguish the following two cases: (i) $k \geq 1$ and (ii) $k = 0$.

(i) First let $k \geq 1$. In this case, by Theorem 6.3.2, we note that $d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) = p^k \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\}$, where $1 \leq \tau \leq p^{s-k-1}$ and $0 \leq \omega \leq p-2$. Further, we observe that $\omega p^{s-k-1} + b + \tau \geq p^{s-1} + 1 > p^{s-k}$. This implies that $d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) = p^s$. From this, we see that

$$\begin{aligned} \nu - d_b(\mathscr{C}_{\lambda_0}(s,\nu)) + b &= b - d_b(\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)) \\ &\quad + p^s - p^{s-k} + \omega p^{s-k-1} + \tau \\ &= \omega p^{s-k-1} + \tau + b - p^{s-k} > 0. \end{aligned}$$

This, by (6.4.1), implies that the code $\mathscr{C}_{\lambda_0}(s, p^s - p^{s-k} + \omega p^{s-k-1} + \tau)$ is not an MDS b-symbol code.

(ii) Next let $k = 0$. Here we have $\nu = \omega p^{s-1} + \tau$, where $1 \leq \tau \leq p^{s-1}$ and $0 \leq \omega \leq p-2$. Further, by Theorem 6.3.2, we note that $d_b(\mathscr{C}_{\lambda_0}(s, \omega p^{s-1} + \tau)) = \min\{\omega p^{s-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\} = \omega p^{s-1} + \tau + b$. This, by (6.4.1), implies that the code $\langle (x-\lambda_0)^{\omega p^{s-1}+\tau} \rangle$ is an MDS b-symbol code if and only if $1 \leq \tau \leq p^{s-1}$ and $0 \leq \omega \leq p-2$.

This shows that when $b = p^{s-1}$, the code $\mathscr{C}_{\lambda_0}(s, \nu)$ is an MDS b-symbol code if and only if $1 \leq \nu \leq (p-1)p^{s-1}$.

This completes the proof of the theorem. □

To illustrate the above result, we determine all non-trivial MDS b-symbol cyclic codes of length 25 over $\mathbb{F}_5$ as follows:

Example 6.4.2. Let $p = 5$, $s = 2$, $m = 1$ and $\lambda = 1$. Here we note that $2 \leq b \leq 24$. By applying Theorem 6.4.1, we see that all the distinct non-trivial MDS b-symbol cyclic codes of length 25 over $\mathbb{F}_5$ are given by $\langle (x-1)^\nu \rangle$, where

- $1 \leq \nu \leq 25 - b$ when $6 \leq b \leq 24$.

- $\nu \in \{1, 2, 23\}$ when $b = 2$.
- $\nu \in \{1, 2, 3, 22\}$ when $b = 3$.
- $\nu \in \{1, 2, 3, 4, 6, 7, 8, 11, 12, 16, 21\}$ when $b = 4$.
- $1 \leq \nu \leq 20$ when $b = 5$. □

Remark 6.4.1. Theorem 26 of Dinh et al. [24] follows from Theorem 6.4.1 as a special case when $b = 2$. □

6.5 b-Symbol distances of constacyclic codes of length p^s over finite commutative chain rings

In this section, we shall determine b-symbol distances of all constacyclic codes of length p^s over the finite commutative chain ring $\mathcal{R}$, and identify all MDS b-symbol codes within this class of codes. To do this, we first relate the b-symbol distance of a non-zero linear code $\mathcal{C}$ of an arbitrary length over $\mathcal{R}$ with that of $\text{Tor}_{e-1}(\mathcal{C})$ in the following theorem. We also derive a necessary and sufficient condition under which the linear code $\mathcal{C}$ is an MDS b-symbol code.

Theorem 6.5.1. Let $\mathcal{C}$ be a linear code of an arbitrary length N over $\mathcal{R}$. Then the following hold.

(a) We have $d_b(\mathcal{C}) = d_b(\text{Tor}_{e-1}(\mathcal{C}))$.

(b) The code $\mathcal{C}$ is an MDS b-symbol code if and only if $\text{Tor}_0(\mathcal{C}) = \text{Tor}_{e-1}(\mathcal{C})$ and $\text{Tor}_{e-1}(\mathcal{C})$ is an MDS b-symbol code of length N over $\overline{\mathcal{R}}$.

Proof. (a) To prove the result, let us consider the subcode $\mathcal{C}_{e-1} = \{\gamma^{e-1}c : \gamma^{e-1}c \in \mathcal{C}\}$ of $\mathcal{C}$. It is easy to see that $\text{Tor}_{e-1}(\mathcal{C}) = \{\overline{c} : \gamma^{e-1}c \in \mathcal{C}_{e-1}\}$ and $d_b(\mathcal{C}_{e-1}) = d_b(\text{Tor}_{e-1}(\mathcal{C}))$. This implies that

$$d_b(\text{Tor}_{e-1}(\mathcal{C})) = d_b(\mathcal{C}_{e-1}) \geq d_b(\mathcal{C}). \tag{6.5.1}$$

Next we observe that

$$w_b(Q) \geq w_b(\gamma Q) \text{ for each } Q \in \mathcal{C}. \tag{6.5.2}$$

Further, for any non-zero codeword $Q \in \mathcal{C}$, there exists an integer i satisfying $0 \leq i \leq e-1$ and $Q \in \langle \gamma^i \rangle^N \setminus \langle \gamma^{i+1} \rangle^N$. Now by (6.5.2), we get

$$w_b(Q) \geq w_b(\gamma Q) \geq w_b(\gamma^2 Q) \geq \cdots \geq w_b(\gamma^{e-1-i} Q). \tag{6.5.3}$$

Since $Q \in \langle \gamma^i \rangle^N \setminus \langle \gamma^{i+1} \rangle^N$, we note that $\gamma^{e-1-i}Q$ is a non-zero codeword of $\mathcal{C}$ and that $\gamma^{e-1-i}Q \in \langle \gamma^{e-1} \rangle^N$, which implies that $\gamma^{e-1-i}Q (\neq 0) \in \mathcal{C}_{e-1}$. This further implies that $w_b(\gamma^{e-1-i}Q) \geq d_b(\mathcal{C}_{e-1}) = d_b(\text{Tor}_{e-1}(\mathcal{C}))$. From this and by (6.5.3), we obtain

$$w_b(Q) \geq d_b(\text{Tor}_{e-1}(\mathcal{C})) \text{ for each } Q \in \mathcal{C} \setminus \{0\},$$

which implies that

$$d_b(\mathcal{C}) \geq d_b(\text{Tor}_{e-1}(\mathcal{C})).$$

Using this and by (6.5.1), the desired result follows.

(b) To prove this, by Theorem 2.0.7, we see that for $0 \leq i \leq e-1$, the ith torsion code $\text{Tor}_i(\mathcal{C})$ of $\mathcal{C}$ is a linear code of length N over $\overline{\mathcal{R}}$, $|\text{Tor}_i(\mathcal{C})| = p^{m \times \dim(\text{Tor}_i(\mathcal{C}))}$ and $|\mathcal{C}| = \prod_{i=0}^{e-1} |\text{Tor}_i(\mathcal{C})|$. Further, by part (a), we note that $d_b(\mathcal{C}) = d_b(\text{Tor}_{e-1}(\mathcal{C}))$. From this and by (6.2.2), we see that the code $\mathcal{C}$ is an MDS b-symbol code if and only if $\prod_{i=0}^{e-1} |\text{Tor}_i(\mathcal{C})| = |\mathcal{C}| = p^{me(p^s - d_b(\mathcal{C})+b)}$, which holds if and only if

$$\dim(\text{Tor}_0(\mathcal{C})) + \dim(\text{Tor}_1(\mathcal{C})) + \cdots + \dim(\text{Tor}_{e-1}(\mathcal{C})) = e\left(p^s - d_b(\text{Tor}_{e-1}(\mathcal{C})) + b\right). \tag{6.5.4}$$

Further, by Theorem 2.0.7(b), we note that

$$\text{Tor}_0(\mathcal{C}) \subseteq \text{Tor}_1(\mathcal{C}) \subseteq \cdots \subseteq \text{Tor}_{e-1}(\mathcal{C}). \tag{6.5.5}$$

Now by applying Theorem 6.2.2 (the Singleton-type bound) for the code $\mathrm{Tor}_{e-1}(\mathcal{C})$ over $\overline{\mathcal{R}}$, we get

$$p^{m\times \dim(\mathrm{Tor}_{e-1}(\mathcal{C}))} = |\mathrm{Tor}_{e-1}(\mathcal{C})| \leq p^{m(p^s - d_b(\mathrm{Tor}_{e-1}(\mathcal{C}))+b)},$$

which implies that $\dim(\mathrm{Tor}_{e-1}(\mathcal{C})) \leq p^s - d_b(\mathrm{Tor}_{e-1}(\mathcal{C}))+b$. From this and by (6.5.5), we see that

$$\dim(\mathrm{Tor}_0(\mathcal{C})) \leq \dim(\mathrm{Tor}_1(\mathcal{C})) \leq \cdots \leq \dim(\mathrm{Tor}_{e-1}(\mathcal{C})) \leq p^s - d_b(\mathrm{Tor}_{e-1}(\mathcal{C})) + b. \tag{6.5.6}$$

This further implies that $\dim(\mathrm{Tor}_0(\mathcal{C})) + \dim(\mathrm{Tor}_1(\mathcal{C})) + \cdots + \dim(\mathrm{Tor}_{e-1}(\mathcal{C})) \leq e\,(p^s - d_b(\mathrm{Tor}_{e-1}(\mathcal{C})) + b)$ and that the equality holds if and only if

$$\dim(\mathrm{Tor}_0(\mathcal{C})) = \dim(\mathrm{Tor}_1(\mathcal{C})) = \cdots = \dim(\mathrm{Tor}_{e-1}(\mathcal{C})) = p^s - d_b(\mathrm{Tor}_{e-1}(\mathcal{C})) + b.$$

From this, the desired result follows immediately.

□

It is worth mentioning that Norton and Sălăgean [66, Th. 4.2(ii)] proved the corresponding equality "$d_H(\mathcal{C}) = d_H(\mathrm{Tor}_{e-1}(\mathcal{C}))$" for the Hamming metric by using the concept of support of a linear code. The same idea could be extended to provide an alternate proof for Theorem 6.5.1(a).

Now we will apply Theorem 6.5.1 to determine b-symbol distances of all constacyclic codes of length p^s over the finite commutative chain ring $\mathcal{R}$. For this, from now on, let η be a unit in $\mathcal{R}$. By Theorem 2.0.6(c), the unit $\eta \in \mathcal{R}$ can be uniquely written as $\eta = \theta + \gamma\delta_1 + \gamma^2\delta_2 + \cdots + \gamma^{e-1}\delta_{e-1}$, where $\theta, \delta_1, \delta_2, \cdots, \delta_{e-1} \in \mathcal{T}$ and $\theta \neq 0$. Further, by Theorem 2.0.6(b), we see that there exists $\eta_0 \in \mathcal{T} \setminus \{0\}$ satisfying $\theta = \eta_0^{p^s}$. Recall that an η-constacyclic code $\mathcal{C}$ of length p^s over $\mathcal{R}$ is an ideal of the quotient ring $\mathcal{R}_\eta = \mathcal{R}[x]/\langle x^{p^s} - \eta\rangle$. Moreover, by Theorem 5.2.3(a), we see that the ith torsion code $\mathrm{Tor}_i(\mathcal{C})$ of $\mathcal{C}$ is an ideal of the ring $\overline{\mathcal{R}}[x]/\langle x^{p^s} - \overline{\eta}_0^{p^s}\rangle$ and is given by $\mathrm{Tor}_i(\mathcal{C}) = \langle (x - \overline{\eta}_0)^{T_i}\rangle$ for $0 \leq i \leq e-1$, where

T_i is an integer satisfying $0 \leq T_i \leq p^s$ for each i. Recall that $\mathcal{C} = \{0\}$ when $T_{e-1} = p^s$, while $\mathcal{C} = \langle 1 \rangle = \mathcal{R}_\eta$ when $T_0 = 0$. Here also, when $\mathcal{C} = \{0\}$, we have $d_b(\mathcal{C}) = 0$.

In the following theorem, we determine b-symbol distances of all non-zero η-constacyclic codes of length p^s over $\mathcal{R}$.

Theorem 6.5.2. Let $\eta = \eta_0^{p^s} + \gamma\delta_1 + \cdots + \gamma^{e-1}\delta_{e-1}$, where $\eta_0, \delta_1, \cdots, \delta_{e-1} \in \mathcal{T}$ and $\eta_0 \neq 0$. Let $\mathcal{C}$ be a non-zero η-constacyclic code of length p^s over $\mathcal{R}$ with $\text{Tor}_{e-1}(\mathcal{C}) = \langle (x - \overline{\eta}_0)^{T_{e-1}} \rangle$, where $0 \leq T_{e-1} < p^s$.

(a) When $T_{e-1} = 0$, we have $d_b(\mathcal{C}) = b$.

(b) Let $1 \leq T_{e-1} \leq p^s - 1$.

(i) When $s = 1$, we have $d_b(\mathcal{C}) = \min\{T_{e-1} + b,\ p\}$.

(ii) When $s \geq 2$, the integer T_{e-1} can be uniquely expressed as $T_{e-1} = p^s - p^{s-k} + \omega p^{s-k-1} + \tau$, where $0 \leq k \leq s-1$, $0 \leq \omega \leq p-2$ and $1 \leq \tau \leq p^{s-k-1}$. Furthermore, the b-symbol distance of the code $\mathcal{C}$ is given by

$$d_b(\mathcal{C}) = \begin{cases} p^k \min\{\omega p^{s-k-1} + b + \tau, (\omega+2)b, (\omega+1)(b+\tau)\} \text{ if } 2 \leq \\ b \leq p^{s-k-1}; \\ p^k \min\{\omega p^{s-k-1} + b + \tau, p^{s-k}\} \text{ if } p^{s-k-1} + 1 \leq b \leq p^s - 1. \end{cases}$$

Proof. It follows immediately from Theorems 6.3.1, 6.3.2 and 6.5.1(a) and Remark 6.3.1. □

Remark 6.5.1. One can show that for a unit $\eta = \eta_0^{p^s} + \gamma\delta_1 + \cdots + \gamma^{e-1}\delta_{e-1} \in \mathcal{R}$, an η-constacyclic code of length p^s over $\mathcal{R}$ is equivalent to some $(\eta_0^{-p^s}\eta)$-constacyclic code of length p^s over $\mathcal{R}$ as follows: Define a map $\Theta_{\eta_0} : \mathcal{R}[x]/\langle x^{p^s} - \eta \rangle \to \mathcal{R}[x]/\langle x^{p^s} - \eta_0^{-p^s}\eta \rangle$ as $\Theta_{\eta_0}(c(x)) = c(\eta_0 x)$ for each $c(x) \in \mathcal{R}[x]/\langle x^{p^s} - \eta \rangle$. One can easily observe that the map Θ_{η_0} is a ring isomorphism and that $w_b(c(x)) = w_b(\Theta_{\eta_0}(c(x)))$ for each $c(x) \in \mathcal{R}[x]/\langle x^{p^s} - \eta \rangle$. From this, it follows that an η-constacyclic code $\mathcal{C}$ of length p^s over $\mathcal{C}$ is equivalent to the $(\eta_0^{-p^s}\eta)$-constacyclic code $\Theta_{\eta_0}(\mathcal{C})$ of length p^s over $\mathcal{R}$ and that $d_b(\mathcal{C}) = d_b(\Theta_{\eta_0}(\mathcal{C}))$. □

Now we will apply Theorems 6.5.1 and 6.5.2 to determine all MDS b-symbol constacyclic

codes of length p^s over $\mathcal{R}$. Towards this, we first observe that Theorem 2.5 of Ding et al. [28] can be similarly extended to codes over finite commutative rings, which is stated as follows:

Theorem 6.5.3. Let $2 \leq b < N$ be fixed. Let $\mathcal{C}$ be an MDS b-symbol code of length N over a finite commutative ring R. If $d_b(\mathcal{C}) < N$, then $\mathcal{C}$ is also an MDS $(b+1)$-symbol code with $d_{b+1}(\mathcal{C}) = d_b(\mathcal{C}) + 1$.

However, the converse of the above theorem is not true in general, which is illustrated in the following example.

Example 6.5.1. Let $\mathcal{R} = \mathbb{F}_5 + \gamma\mathbb{F}_5$, where $\gamma^2 = 0$. Consider the cyclic code $\mathscr{D}_1 = \langle (x-1)^3 \rangle$ of length 25 over $\mathcal{R}$. By Theorems 5.2.3 and 6.5.2, we see that $|\mathscr{D}_1| = 5^{44}$, $d_2(\mathscr{D}_1) = 4$ and $d_3(\mathscr{D}_1) = 6$. Now by (6.2.2), we observe that the code $\mathscr{D}_1$ is an MDS 3-symbol code, but not an MDS 2-symbol (symbol-pair) code. □

Now we proceed to determine all MDS b-symbol constacyclic codes of length p^s over $\mathcal{R}$. For this, we first note that an MDS b-symbol code has to be non-zero and that the code $\langle 1 \rangle = \mathcal{R}_\eta$ is an MDS b-symbol code. In the following theorem, we list all non-trivial MDS b-symbol constacyclic codes of length p^s over $\mathcal{R}$.

Theorem 6.5.4. Let $\eta = \eta_0^{p^s} + \gamma\delta_1 + \gamma^2\delta_2 + \cdots + \gamma^{e-1}\delta_{e-1}$, where $\eta_0, \delta_1, \delta_2, \cdots, \delta_{e-1} \in \mathcal{T}$ and $\eta_0 \neq 0$.

(a) When $\delta_1 \neq 0$ and $2 \leq b \leq p^s - 1$, there does not exist any non-trivial MDS b-symbol η-constacyclic code of length p^s over $\mathcal{R}$.

(b) When $\delta_1 = 0$, all the distinct non-trivial MDS b-symbol η-constacyclic codes of length p^s over $\mathcal{R}$ are given by

$$\langle (x-\eta_0)^{T_0} + \gamma(x-\eta_0)^{t_{1,0}} g_{1,0}(x) + \gamma^2(x-\eta_0)^{t_{2,0}} g_{2,0}(x) + \cdots\cdots + \gamma^{e-1}(x-\eta_0)^{t_{e-1,0}} g_{e-1,0}(x) \rangle$$

with the ith-torsional degree as T_0 for $0 \leq i \leq e-1$, $0 \leq t_{j,0} < T_0$ if $g_{j,0}(x) \neq 0$, and $g_{j,0}(x) \in \mathcal{T}[x]$ is either 0 or a unit in $\mathcal{R}_\eta$ satisfying deg $g_{j,0}(x) < T_0 - t_{j,0}$ for $1 \leq j \leq e-1$, where

- $1 \leq T_0 \leq p^s - b$ when $s \geq 1$ and $p^{s-1} + 1 \leq b \leq p^s - 1$.
- $T_0 \in \{p^s - b, 1, 2, \cdots, b\} \bigcup \left(\bigcup_{\omega} \{(\omega+1)p^{s-1} - b, (\omega+1)p^{s-1} - b + 1, (\omega+1)p^{s-1} - b + 2, \cdots, (\omega+1)b\} \right)$ when $s \geq 2$ and $2 \leq b \leq p^{s-1} - 1$. Here the union $\bigcup_{\omega}$ runs over all integers ω satisfying $1 \leq \omega \leq p-2$ and $(\omega+2)b - (\omega+1)p^{s-1} \geq 0$.
- $1 \leq T_0 \leq (p-1)p^{s-1}$ when $s \geq 2$ and $b = p^{s-1}$.

Proof. Let $\mathcal{C}$ be a non-trivial η-constacyclic code of length p^s over $\mathcal{R}$ with $\text{Tor}_i(\mathcal{C}) = \langle (x - \overline{\eta}_0)^{T_i} \rangle$, where $0 \leq T_i \leq p^s$ for $0 \leq i \leq e-1$. Here we must have $T_0 \geq 1$ and $T_{e-1} < p^s$. Now by applying Theorems 5.2.3(a) and 6.5.1(b), we see that the code $\mathcal{C}$ is an MDS b-symbol code if and only if $\text{Tor}_0(\mathcal{C}) = \text{Tor}_{e-1}(\mathcal{C})$ and $\text{Tor}_{e-1}(\mathcal{C})$ is an MDS b-symbol $\overline{\eta}_0^{p^s}$-constacyclic code of length p^s over $\overline{\mathcal{R}}$, which, by Theorem 5.2.3(c) and by (6.2.2), holds if and only if

$$1 \leq T_0 = T_1 = \cdots = T_{e-1} < p^s \tag{6.5.7}$$

and $\text{Tor}_{e-1}(\mathcal{C})$ is an MDS b-symbol code. Now we shall distinguish the following two cases: (i) $\delta_1 \neq 0$ and (ii) $\delta_1 = 0$.

(i) First let $\delta_1 \neq 0$. Here we see, by Remark 5.2.2, that $\mathcal{C} = \langle (x - \lambda_0)^{T_k} \rangle = \langle (x - \lambda_0)^{T_k}, \gamma^{k+1}, \cdots, \gamma^{e-1} \rangle$ for some $0 \leq k \leq e-1$, and that $T_{k+1} = T_{k+2} = \cdots = T_{e-1} = 0$. From this and by (6.5.7), part (a) follows.

(ii) When $\delta_1 = 0$, by (6.5.7) and by applying Theorems 5.2.4 and 6.4.1, the desired result follows immediately.

□

To illustrate the above result, we determine all non-trivial MDS b-symbol constacyclic codes of length p^s over the finite commutative chain ring $\mathbb{F}_{p^m} + \gamma\mathbb{F}_{p^m}$ with $\gamma^2 = 0$, as follows:

Example 6.5.2. Let $\mathcal{R} = \mathbb{F}_{p^m} + \gamma\mathbb{F}_{p^m}$, where $\gamma^2 = 0$. Here we note that $\mathcal{T} = \mathbb{F}_{p^m}$. Further, by Theorem 2.0.6, each unit η in $\mathcal{R}$ can be uniquely expressed as $\eta = \eta_0^{p^s} + \gamma\delta_1$, where

$\eta_0, \delta_1 \in \mathbb{F}_{p^m}$ and $\eta_0 \neq 0$. When $\delta_1 \neq 0$, by Theorem 6.5.4(a), there does not exist any non-trivial MDS b-symbol η-constacyclic code of length p^s over $\mathcal{R}$.

When $\delta_1 = 0$, by Theorem 5.2.4, all the distinct non-zero η-constacyclic codes of length p^s over $\mathcal{R}$ are given by $\langle f_0(x), f_1(x)\rangle$, where $f_0(x) = (x-\eta_0)^{T_0} + \gamma(x-\eta_0)^{t_{1,0}} g_{1,0}(x)$ if $1 \leq T_0 < p^s$, $f_0(x) = 0$ if $T_0 = p^s$, $f_0(x) = 1$ if $T_0 = 0$ and $f_1(x) = \gamma(x-\eta_0)^{T_1}$, where $0 \leq T_1 \leq T_0 \leq p^s$, $0 \leq t_{1,0} < T_1$ provided $g_{1,0}(x) \neq 0$, and $g_{1,0}(x) \in \mathbb{F}_{p^m}[x]$ is either 0 or a unit in $\mathcal{R}_\eta$ satisfying deg $g_{1,0}(x) < T_1 - t_{1,0}$. Further, when $1 \leq T_0 < p^s$ and $g_{1,0}(x) \neq 0$, one can easily show that $p^s - T_0 + t_{1,0} \geq T_1$. From this and by applying Theorem 6.5.4(b), all the distinct non-trivial MDS b-symbol η-constacyclic codes of length p^s over $\mathcal{R}$ are given by

$$\langle (x-\eta_0)^{T_0} + \gamma(x-\eta_0)^{t_{1,0}} g_{1,0}(x)\rangle$$

with $\max\{0, 2T_0 - p^s\} \leq t_{1,0} < T_0$ if $g_{1,0}(x) \neq 0$, and $g_{1,0}(x)$ as either 0 or of the form $\sum_{j=0}^{T_0 - t_{1,0} - 1} A_j (x-\eta_0)^j$, $A_j \in \mathbb{F}_{p^m}$ for $0 \leq j \leq T_0 - t_{1,0} - 1$ and $A_0 \neq 0$, where

- $1 \leq T_0 \leq p^s - b$ when $s \geq 1$ and $p^{s-1} + 1 \leq b \leq p^s - 1$.
- $T_0 \in \{p^s - b, 1, 2, \cdots, b\} \bigcup \left(\bigcup_{\omega} \{(\omega+1)p^{s-1} - b, (\omega+1)p^{s-1} - b + 1, (\omega+1)p^{s-1} - b + 2, \cdots, (\omega+1)b\} \right)$ when $s \geq 2$ and $2 \leq b \leq p^{s-1} - 1$. Here the union $\bigcup_{\omega}$ runs over all integers ω satisfying $1 \leq \omega \leq p-2$ and $(\omega+2)b - (\omega+1)p^{s-1} \geq 0$.
- $1 \leq T_0 \leq (p-1)p^{s-1}$ when $s \geq 2$ and $b = p^{s-1}$. □

Chapter 7

Depth distributions of constacyclic codes over finite commutative chain rings and roulette games

7.1 Introduction

The purpose of this chapter is two-fold. First of all, we shall study depths of codewords of all repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over a finite commutative chain ring $\mathcal{R}$, where α is a non-zero element of the Teichmüller set of $\mathcal{R}$, γ is a generator of the maximal ideal of $\mathcal{R}$ and β is a unit in $\mathcal{R}$. As an application, we shall explicitly determine depth distributions of all repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$. Secondly, we shall propose two new turn-based two player roulette games and provide positional winning strategies for these games in terms of depths of words over a finite commutative ring with unity R. We shall also discuss the feasibility of these winning strategies by applying our results on depths of codewords of repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$.

This chapter is organized as follows: In Section 7.2, we state some preliminaries that are needed to prove our main results. In Section 7.3, we study depths of codewords of all repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$, where α is a non-zero element of the Teichmüller set of $\mathcal{R}$ and β is a unit in $\mathcal{R}$. We also explicitly determine depth distributions of all repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$. In Section 7.4, we propose two new turn-based two player roulette games and provide positional winning strategies for these games in terms of depths of words over a finite commutative ring with unity R.

7.2 Some preliminaries

Let R be a finite commutative ring with unity, N be a positive integer, and let R^N be the R-module consisting of all N-tuples over R. Elements of R^N are called words of length N over R. A word in R^N is said to be a repeated word if all its components are equal, otherwise it is called a non-repeated word. The derivative $D : R^N \to R^{N-1}$ is defined as

$$D(a_0, a_1, \cdots, a_{N-1}) = (a_1 - a_0, a_2 - a_1, \cdots, a_{N-1} - a_{N-2})$$

for each $(a_0, a_1, \cdots, a_{N-1}) \in R^N$. The depth of a vector $a \in R^N$, denoted by depth(a), is defined as the smallest integer i (if it exists) satisfying $0 \leq i \leq N-1$ and $D^i(a) = (0, 0, \cdots, 0) \in R^{N-i}$. If no such integer i exists (i.e., $D^{N-1}(a) \neq 0$), then the depth of the vector a is defined to be N. It is easy to see that depth$(a) = i$ if and only if $D^{i-1}(a) = (r, r, \cdots, r) \in R^{N-i+1}$ for some $r(\neq 0) \in R$. Further, note that depth$(a) = 0$ if and only if $a = (0, 0, \cdots, 0) \in R^N$.

Definition 7.2.1. [32] Let $\mathcal{C}$ be a code of length N over R (i.e., a subset of R^N). For $0 \leq \rho \leq N$, let $\mathcal{D}_\rho(\mathcal{C})$ denote the number of codewords in $\mathcal{C}$ having the depth as ρ. Then the depth distribution and the depth spectrum of the code $\mathcal{C}$ are defined as follows:

- The depth distribution of the code $\mathcal{C}$ is defined as the list

$$\mathcal{D}_0(\mathcal{C}) = 1, \mathcal{D}_1(\mathcal{C}), \mathcal{D}_2(\mathcal{C}), \cdots, \mathcal{D}_N(\mathcal{C}).$$

- The depth spectrum of the code $\mathcal{C}$ is defined as the set

$$\text{Depth}(\mathcal{C}) = \{i : 1 \leq i \leq N \text{ and } \mathcal{D}_i(\mathcal{C}) \neq 0\}.$$

Recall that for a unit $\lambda \in R$, the study of λ-constacyclic codes of length N over R is equivalent to the study of ideals of the quotient ring $R[x]/\langle x^N - \lambda \rangle$. Now the derivative of $c(x) = c_0 + c_1 x + \cdots + c_{N-1}x^{N-1} \in R[x]/\langle x^N - \lambda \rangle$ is defined as the derivative of the vector $c = (c_0, c_1, \cdots, c_{N-1}) \in R^N$. In view of this, the depth of an element

$c(x) = c_0 + c_1x + \cdots + c_{N-1}x^{N-1} \in R[x]/\langle x^N - \lambda\rangle$, denoted by depth$(c(x))$, is defined as the depth of the vector $c = (c_0, c_1, \cdots, c_{N-1}) \in R^N$. Now the following proposition is useful in the determination of derivatives of non-zero codewords of λ-constacyclic codes.

Proposition 7.2.1. [62] Let $0 \leq i \leq N-1$ be fixed. For $c(x) \in R[x]/\langle x^N - \lambda\rangle$, let us write $(1-x)^i c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{N-1}x^{N-1}$ modulo $x^N - \lambda$. Then the ith derivative $D^i(c(x))$ of the element $c(x)$ is given by

$$D^i(c(x)) \ = \ (c_i, c_{i+1}, \cdots, c_{N-1}),$$

i.e., $D^i(c(x))$ appears as the last $N-i$ coefficients of the polynomial $(1-x)^i c(x)$ modulo $x^N - \lambda$.

From now on, throughout this chapter, let $\mathcal{R}$ be a finite commutative chain ring with unity, and let γ be a generator of the maximal ideal of $\mathcal{R}$. Let $\overline{\mathcal{R}} = \mathcal{R}/\langle\gamma\rangle$ be the residue field of $\mathcal{R}$. Let e be the nilpotency index of γ, and let $\mathcal{T}$ be the Teichmüller set of $\mathcal{R}$. As $\overline{\mathcal{R}}$ is a finite field, we assume that $\overline{\mathcal{R}} \simeq \mathbb{F}_{p^m}$ for some prime p and positive integer m, where $\mathbb{F}_{p^m}$ is the finite field of order p^m. Now by Theorem 2.0.6(c), we see that a unit $\lambda \in \mathcal{R}$ can be written as $\lambda = \alpha + \gamma\beta$, where $\alpha(\neq 0) \in \mathcal{T}$ is uniquely fixed and $\beta \in \{0\} \cup (\mathcal{R} \setminus \langle\gamma^{e-1}\rangle)$. Further, for each positive integer s, by Theorem 2.0.6(b), we see that there exists $\alpha_0(\neq 0) \in \mathcal{T}$ satisfying $\alpha = \alpha_0^{p^s}$, which implies that $\lambda = \alpha_0^{p^s} + \gamma\beta$.

From this point on, we assume that $\lambda = \alpha_0^{p^s} + \gamma\beta$, where $\alpha_0(\neq 0) \in \mathcal{T}$ and β is a unit in $\mathcal{R}$.

From now on, we shall follow the same notations as in Section 7.2. In the following section, we shall study depths of codewords of λ-constacyclic codes of length p^s over $\mathcal{R}$, where p is a prime number, s is a positive integer, and $\lambda = \alpha_0^{p^s} + \gamma\beta$ with $\alpha_0(\neq 0) \in \mathcal{T}$ and β a unit in $\mathcal{R}$. As a consequence, we shall determine depth distributions of all λ-constacyclic codes of length p^s over $\mathcal{R}$.

7.3 Depths of codewords of λ-constacyclic codes of length p^s over $\mathcal{R}$

Etzion [32, Th. 1] showed that non-zero codewords of a k-dimensional linear code $\mathcal{C}$ over a finite field attain k distinct non-zero depth values and that any k non-zero codewords of $\mathcal{C}$ with distinct depths form a basis of the code. Using this result, Luo et al. [58, Prop. 8] showed that depth distributions of linear codes over arbitrary finite fields are completely determined by their depth spectra. As linear codes over finite commutative chain rings are not free modules in general, we note that Theorem 1 of Etzion [32] and the technique employed to prove Proposition 8 of Luo et al. [58] can not be extended to study depths of codewords of linear codes over finite commutative chain rings and to determine their depth distributions. So we need to follow a new and different approach to study depths of non-zero codewords of λ-constacyclic codes of length p^s over $\mathcal{R}$, and to determine their depth distributions.

In order to study depths of codewords of all λ-constacyclic codes of length p^s over $\mathcal{R}$, we first recall, by Theorem 5.2.1(c), that all the distinct non-zero λ-constacyclic codes of length p^s over $\mathcal{R}$ are given by $\mathcal{C}_{\ell,u} = \langle \gamma^\ell (x-\alpha_0)^u \rangle$, where $0 \leq \ell \leq e-1$ and $0 \leq u < p^s$. The following lemma plays a key role in studying depths of codewords of λ-constacyclic codes of length p^s over $\mathcal{R}$.

Lemma 7.3.1. Let $\lambda = \alpha_0^{p^s} + \gamma\beta$, where $\alpha_0 (\neq 0) \in \mathcal{T}$ and β is a unit in $\mathcal{R}$. Let $\mathcal{C}_{\ell,u} = \langle \gamma^\ell (x-\alpha_0)^u \rangle$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$, where $0 \leq \ell \leq e-1$ and $0 \leq u < p^s$. Then each codeword $C(x) \in \mathcal{C}_{\ell,u}$ can be uniquely expressed as

$$C(x) = c_0 + c_1(x-\alpha_0) + \cdots + c_{u-1}(x-\alpha_0)^{u-1} + c_u(x-\alpha_0)^u + c_{u+1}(x-\alpha_0)^{u+1} + \cdots + c_{p^s-1}(x-\alpha_0)^{p^s-1},$$

where $c_0, c_1, \cdots, c_{u-1} \in \langle \gamma^{\ell+1} \rangle$ and $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle \gamma^\ell \rangle$.

Proof. It follows immediately from Lemma 5.5.1. □

Now we shall distinguish the following two cases: (i) $\alpha_0 = 1$ and (ii) $\alpha_0 \neq 1$.

7.3.1 The case $\alpha_0 = 1$

Throughout this section, we assume that $\alpha_0 = 1$. Here we have $\lambda = 1 + \gamma\beta$, where β is a unit in $\mathcal{R}$. Further, for $1 \leq k \leq p^s - 1$, $0 \leq i \leq p^s - 1$ and $0 \leq t \leq p^s - 1$, let $\mathcal{Q}_{i,k}^{(t)}$ denote the coefficient of x^t in $(x-1)^{p^s-k+i}$ modulo $x^{p^s} - \lambda$. We first make the following observation.

Lemma 7.3.2. Let $1 \leq k \leq p^s - 1$ be fixed.

(a) For $k \leq i \leq p^s - 1$ and $p^s - k \leq t \leq p^s - 1$, we have $\mathcal{Q}_{i,k}^{(t)} \equiv 0 \pmod{p}$.

(b) For $0 \leq t \leq p^s - 1$, we have $\mathcal{Q}_{k-1,k}^{(t)} \equiv 1 \pmod{p}$.

Proof. (a) To prove the result, we will apply induction on $k \geq 1$.

To begin with, we note that $\mathcal{Q}_{i,1}^{(p^s-1)} = \binom{p^s-1+i}{p^s-1}(-1)^i$ for $1 \leq i \leq p^s - 1$. Further, the p-adic representation of p^s-1 is given by $p^s-1 = (p-1)+p(p-1)+\cdots+p^{s-1}(p-1)$. Since there is at least one carry when $p^s - 1$ is added to i in the base p, by applying Theorem 2.0.9, we see that

$$\mathcal{Q}_{i,1}^{(p^s-1)} \equiv \binom{p^s - 1 + i}{i}(-1)^i \equiv 0 \pmod{p} \text{ for } 1 \leq i \leq p^s - 1.$$

Thus the result holds when $k = 1$.

Next we assume that $2 \leq j \leq p^s - 1$ is a fixed integer and that the result holds for $k = j - 1$. That is, we have $\mathcal{Q}_{i,j-1}^{(t)} \equiv 0 \pmod{p}$ for $j - 1 \leq i \leq p^s - 1$ and $p^s - j + 1 \leq t \leq p^s - 1$. Here we have to show that

$$\mathcal{Q}_{i,j}^{(t)} \equiv 0 \pmod{p} \quad \text{for} \quad j \leq i \leq p^s - 1 \quad \text{and} \quad p^s - j \leq t \leq p^s - 1. \tag{7.3.1}$$

For this, we observe that

$$\begin{aligned}\mathcal{Q}_{i,j-1}^{(0)} + \mathcal{Q}_{i,j-1}^{(1)}x + \cdots + \mathcal{Q}_{i,j-1}^{(p^s-1)}x^{p^s-1} &= (x-1)^{p^s-j+1+i} \\ &= (x-1)(x-1)^{p^s-j+i} = (x-1)\left(\mathcal{Q}_{i,j}^{(0)} + \mathcal{Q}_{i,j}^{(1)}x + \cdots + \mathcal{Q}_{i,j}^{(p^s-1)}x^{p^s-1}\right).\end{aligned}$$

This implies that

$$\begin{aligned}\mathcal{Q}_{i,j-1}^{(p^s-j+1)} &= \mathcal{Q}_{i,j}^{(p^s-j)} - \mathcal{Q}_{i,j}^{(p^s-j+1)}, \\ \mathcal{Q}_{i,j-1}^{(p^s-j+2)} &= \mathcal{Q}_{i,j}^{(p^s-j+1)} - \mathcal{Q}_{i,j}^{(p^s-j+2)}, \\ \cdots\cdots &\ \cdots\ \cdots\cdots\cdots \\ \mathcal{Q}_{i,j-1}^{(p^s-2)} &= \mathcal{Q}_{i,j}^{(p^s-3)} - \mathcal{Q}_{i,j}^{(p^s-2)}, \\ \mathcal{Q}_{i,j-1}^{(p^s-1)} &= \mathcal{Q}_{i,j}^{(p^s-2)} - \mathcal{Q}_{i,j}^{(p^s-1)}.\end{aligned}$$

In view of this and by the induction hypothesis, we see that to prove (7.3.1), it is enough to prove that

$$\mathcal{Q}_{i,j}^{(p^s-1)} = \binom{p^s-j+i}{p^s-1}(-1)^{i-j+1} \equiv 0 \pmod p \quad \text{for} \quad j \le i \le p^s-1.$$

Since the p-adic representation of p^s-1 is $p^s-1 = (p-1)+p(p-1)+\cdots+p^{s-1}(p-1)$, there is at least one carry when p^s-1 is added to $i-j+1$ in the base p. This, by applying Theorem 2.0.9 again, implies that

$$\mathcal{Q}_{i,j}^{(p^s-1)} = \binom{p^s-j+i}{p^s-1}(-1)^{i-j+1} \equiv 0 \pmod p.$$

This competes the proof of part (a).

(b) To prove this, let $0 \le t \le p^s-1$ be fixed. We note that $\mathcal{Q}_{k-1,k}^{(t)} = \binom{p^s-1}{t}(-1)^{p^s-1-t}$. Let us write $t = t_0 + pt_1 + \cdots + p^{s-1}t_{s-1}$, where $0 \le t_i \le p-1$ for $0 \le i \le s-1$. As the p-adic representation of p^s-1 is given by

$$p^s-1 = (p-1) + p(p-1) + \cdots + p^{s-1}(p-1),$$

by applying Theorem 2.0.10, we get

$$\binom{p^s-1}{t} \equiv \binom{p-1}{t_0}\binom{p-1}{t_1}\cdots\binom{p-1}{t_{s-1}} \pmod{p}. \tag{7.3.2}$$

Further, one can easily observe that $\binom{p-1}{j} \equiv (-1)^j \pmod{p}$ for each integer j satisfying $0 \leq j \leq p-1$. Using this and by (7.3.2), we obtain

$$\mathcal{Q}_{k-1,k}^{(t)} = \binom{p^s-1}{t}(-1)^{p^s-1-t} \equiv (-1)^{p^s-1-t_1(p-1)-t_2(p^2-1)-\cdots-t_{s-1}(p^{s-1}-1)}$$
$$\equiv 1 \pmod{p},$$

which proves (b).

□

In the following theorem, we provide a method to determine codewords with a prescribed depth in a λ-constacyclic code of length p^s over $\mathcal{R}$, where $\lambda = 1+\gamma\beta$ with β a unit in $\mathcal{R}$.

Theorem 7.3.1. Let $\lambda = 1+\gamma\beta$, where β is a unit in $\mathcal{R}$. Let $\mathcal{C}_{\ell,u} = \langle \gamma^\ell (x-1)^u \rangle$ be a λ-constacyclic code of length p^s over $\mathcal{R}$, where $0 \leq \ell \leq e-1$ and $0 \leq u < p^s$. Further, let $C(x) \in \mathcal{C}_{\ell,u}$ be a non-zero codeword with the unique representation as

$$C(x) = c_0 + c_1(x-1) + \cdots + c_{u-1}(x-1)^{u-1} + c_u(x-1)^u + \cdots + c_{p^s-1}(x-1)^{p^s-1},$$

where $c_0, c_1, \cdots, c_{u-1} \in \langle \gamma^{\ell+1} \rangle$ and $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle \gamma^\ell \rangle$. Then the following hold.

(a) For $1 \leq k \leq p^s-1$, the depth of the codeword $C(x) \in \mathcal{C}_{\ell,u}$ is p^s-k+1 if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the following matrix equation for some non-zero $\tau \in \langle \gamma^{\ell+1} \rangle$ when $k \leq u$ and for some non-zero $\tau \in \langle \gamma^\ell \rangle$ when $k > u$:

$$\begin{bmatrix} 1 & \mathcal{Q}_{1,k}^{(p^s-k)} & \mathcal{Q}_{2,k}^{(p^s-k)} & \cdots & \mathcal{Q}_{k-2,k}^{(p^s-k)} & \mathcal{Q}_{k-1,k}^{(p^s-k)} \\ 0 & 1 & \mathcal{Q}_{2,k}^{(p^s-k+1)} & \cdots & \mathcal{Q}_{k-2,k}^{(p^s-k+1)} & \mathcal{Q}_{k-1,k}^{(p^s-k+1)} \\ 0 & 0 & 1 & \cdots & \mathcal{Q}_{k-2,k}^{(p^s-k+2)} & \mathcal{Q}_{k-1,k}^{(p^s-k+2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \mathcal{Q}_{k-1,k}^{(p^s-2)} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} -c_0 \\ -c_1 \\ -c_2 \\ \vdots \\ -c_{k-2} \\ \tau - c_{k-1} \end{bmatrix}$$

$$= \begin{bmatrix} \tau(\mathcal{Q}_{k-1,k}^{(p^s-k)} - 1) + \sum_{j=k}^{p^s-1} c_j \mathcal{Q}_{j,k}^{(p^s-k)} \\ \tau(\mathcal{Q}_{k-1,k}^{(p^s-k+1)} - 1) + \sum_{j=k}^{p^s-1} c_j \mathcal{Q}_{j,k}^{(p^s-k+1)} \\ \tau(\mathcal{Q}_{k-1,k}^{(p^s-k+2)} - 1) + \sum_{j=k}^{p^s-1} c_j \mathcal{Q}_{j,k}^{(p^s-k+2)} \\ \vdots \\ \tau(\mathcal{Q}_{k-1,k}^{(p^s-2)} - 1) + \sum_{j=k}^{p^s-1} c_j \mathcal{Q}_{j,k}^{(p^s-2)} \\ \sum_{j=k}^{p^s-1} c_j \mathcal{Q}_{j,k}^{(p^s-1)} \end{bmatrix}. \tag{7.3.3}$$

(b) The depth of the codeword $C(x) \in \mathcal{C}_{\ell,u}$ is 1 if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the following matrix equation:

$$\begin{bmatrix} 1 & \mathcal{Q}^{(1)}_{1,p^s-1} & \mathcal{Q}^{(1)}_{2,p^s-1} & \cdots & \mathcal{Q}^{(1)}_{p^s-4,p^s-1} & \mathcal{Q}^{(1)}_{p^s-3,p^s-1} & \mathcal{Q}^{(1)}_{p^s-2,p^s-1} \\ 0 & 1 & \mathcal{Q}^{(2)}_{2,p^s-1} & \cdots & \mathcal{Q}^{(2)}_{p^s-4,p^s-1} & \mathcal{Q}^{(2)}_{p^s-3,p^s-1} & \mathcal{Q}^{(2)}_{p^s-2,p^s-1} \\ 0 & 0 & 1 & \cdots & \mathcal{Q}^{(3)}_{p^s-4,p^s-1} & \mathcal{Q}^{(3)}_{p^s-3,p^s-1} & \mathcal{Q}^{(3)}_{p^s-2,p^s-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \mathcal{Q}^{(p^s-3)}_{p^s-3,p^s-1} & \mathcal{Q}^{(p^s-3)}_{p^s-2,p^s-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 & \mathcal{Q}^{(p^s-2)}_{p^s-2,p^s-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -c_0 \\ -c_1 \\ -c_2 \\ \vdots \\ -c_{p^s-4} \\ -c_{p^s-3} \\ -c_{p^s-2} \end{bmatrix} = \begin{bmatrix} c_{p^s-1}\mathcal{Q}^{(1)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{Q}^{(2)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{Q}^{(3)}_{p^s-1,p^s-1} \\ \vdots \\ c_{p^s-1}\mathcal{Q}^{(p^s-3)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{Q}^{(p^s-2)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{Q}^{(p^s-1)}_{p^s-1,p^s-1} \end{bmatrix}. \tag{7.3.4}$$

Proof. (a) To prove the result, we recall that $\text{depth}(C(x)) = p^s - k + 1$ if and only if $D^{p^s-k}(C(x)) = (d, d, \cdots, d) \in \mathcal{R}^k$ for some $d(\neq 0) \in \mathcal{R}$. From this and by Proposition 7.2.1, we see that $\text{depth}(C(x)) = p^s - k + 1$ if and only if the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x)$ are equal to d modulo $x^{p^s} - \lambda$, where d is a non-zero element of $\mathcal{R}$.

First of all, we assume that the depth of $C(x) \in \mathcal{C}_{\ell,u}$ is $p^s - k + 1$. This implies that the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x) \in \mathcal{C}_{\ell,u}$ are equal to $d(\neq 0) \in \mathcal{R}$. From this, it follows that $c_0, c_1, \cdots, c_{p^s-1}$ satisfy (7.3.3) with $\tau = (-1)^{p^s-k}d$. Further, by Lemma 7.3.2, we see that $\mathcal{Q}^{(t)}_{k-1,k} \equiv 1 \pmod{p}$ and

$\mathcal{Q}_{i,k}^{(t)} \equiv 0 \pmod{p}$ for $k \leq i \leq p^s - 1$ and $p^s - k \leq t \leq p^s - 1$. This implies that

$$\mathcal{Q}_{k-1,k}^{(t)} - 1 \in \langle\gamma\rangle \quad \text{and} \quad \mathcal{Q}_{i,k}^{(t)} \in \langle\gamma\rangle \quad \text{for} \quad p^s - k \leq t \leq p^s - 1 \quad \text{and} \quad k \leq i \leq p^s - 1.$$

Now using the fact that $(-1)^{p^s-k}d - c_{k-1} = c_k\mathcal{Q}_{k,k}^{(p^s-1)} + \cdots + c_{p^s-1}\mathcal{Q}_{p^s-1,k}^{(p^s-1)}$ and $c_k, c_{k+1}, \cdots, c_{p^s-1} \in \langle\gamma^\ell\rangle$, we see that $(-1)^{p^s-k}d - c_{k-1} \in \langle\gamma^{\ell+1}\rangle$. From this, it follows that $d \in \langle\gamma^{\ell+1}\rangle$ when $k \leq u$ and that $d \in \langle\gamma^\ell\rangle$ when $k > u$.

Next to prove the converse part, suppose that $c_0, c_1, \cdots, c_{u-1} \in \langle\gamma^{\ell+1}\rangle$ and $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle\gamma^\ell\rangle$ satisfy the matrix equation (7.3.3) with $\tau \in \langle\gamma^{\ell+1}\rangle \setminus \{0\}$ when $k \leq u$ and with $\tau \in \langle\gamma^\ell\rangle \setminus \{0\}$ when $k > u$. Then we observe that $C(x) = c_0 + c_1(x-1) + \cdots + c_{u-1}(x-1)^{u-1} + c_u(x-1)^u + \cdots + c_{p^s-1}(x-1)^{p^s-1} \in \mathcal{C}_{\ell,u}$ and that the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x) \in \mathcal{C}_{\ell,u}$ are equal to $(-1)^{p^s-k}\tau$ modulo $x^{p^s} - \lambda$. From this, it follows that depth$(C(x)) = p^s - k + 1$. This proves (a).

(b) Working in a similar manner as in part (a) and by applying Lemma 7.3.2(a), we observe that the depth of the non-zero codeword $C(x) = c_0 + c_1(x-1) + \cdots + c_{u-1}(x-1)^{u-1} + c_u(x-1)^u + \cdots + c_{p^s-1}(x-1)^{p^s-1} \in \mathcal{C}_{\ell,u}$ is 1 if and only if the coefficients of $x, x^2, \cdots, x^{p^s-1}$ in the codeword $(1-x)C(x) \in \mathcal{C}_{\ell,u}$ are zero modulo $x^{p^s} - \lambda$, which holds if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the matrix equation (7.3.4).

□

In the following theorem, we determine depth distributions of all λ-constacyclic codes of length p^s over $\mathcal{R}$ when $\alpha_0 = 1$.

Theorem 7.3.2. Let $\lambda = 1 + \gamma\beta$, where β is a unit in $\mathcal{R}$. Let $\mathcal{C}_{\ell,u} = \langle\gamma^\ell(x-1)^u\rangle$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$, where $0 \leq \ell \leq e-1$ and $0 \leq u < p^s$. If $\mathcal{D}_\rho(\mathcal{C}_{\ell,u})$ denotes the number of codewords in $\mathcal{C}$ having the depth as ρ for $1 \leq \rho \leq p^s$, then

$$\mathcal{D}_\rho(\mathcal{C}_{\ell,u}) = \begin{cases} p^{m(e-\ell)} - 1 & \text{if } \rho = 1; \\ (p^{m(e-\ell)} - 1)p^{m(e-\ell)(\rho-1)} & \text{if } 2 \leq \rho \leq p^s - u; \\ (p^{m(e-\ell-1)} - 1)p^{m\{(e-\ell-1)(\rho-1)+p^s-u\}} & \text{if } p^s - u + 1 \leq \rho \leq p^s. \end{cases}$$

Proof. Here we need to determine the numbers $\mathcal{D}_{p^s-k+1}(\mathcal{C}_{\ell,u})$ for $1 \leq k \leq p^s$. To do this, by Lemma 7.3.1, we observe that each non-zero codeword $C(x) \in \mathcal{C}_{\ell,u}$ can be uniquely expressed as

$$C(x) = c_0 + c_1(x-1) + \cdots + c_{u-1}(x-1)^{u-1} + c_u(x-1)^u + c_{u+1}(x-1)^{u+1} + \cdots + c_{p^s-1}(x-1)^{p^s-1},$$

where $c_0, c_1, \cdots, c_{u-1} \in \langle \gamma^{\ell+1} \rangle$ and $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle \gamma^{\ell} \rangle$. Now we shall consider the following two cases separately: **(i)** $1 \leq k \leq p^s - 1$ and **(ii)** $k = p^s$.

(i) First let $1 \leq k \leq p^s - 1$ so that $2 \leq p^s - k + 1 \leq p^s$. Now by applying Theorem 7.2.1(a), we see that depth$(C(x)) = p^s - k + 1$ if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the matrix equation (7.3.3) for some non-zero $\tau \in \langle \gamma^{\ell+1} \rangle$ when $k \leq u$ and for some non-zero $\tau \in \langle \gamma^{\ell} \rangle$ when $k > u$. From this, one can easily observe that

$$\mathcal{D}_{p^s-k+1}(\mathcal{C}_{\ell,u}) = \begin{cases} (p^{m(e-\ell-1)} - 1)p^{m\{(e-\ell-1)(p^s-k)+p^s-u\}} & \text{if } 1 \leq k \leq u; \\ (p^{m(e-\ell)} - 1)p^{m(e-\ell)(p^s-k)} & \text{if } u+1 \leq k \leq p^s - 1. \end{cases}$$

(ii) Next let $k = p^s$ so that $p^s - k + 1 = 1$. Here by applying Theorem 7.2.1(b), we see that depth$(C(x)) = 1$ if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the matrix equation (7.3.4). Now using the fact that $C(x) \neq 0$ and $c_{p^s-1} \in \langle \gamma^{\ell} \rangle$, we observe that $\mathcal{D}_1(\mathcal{C}_{\ell,u}) = p^{m(e-\ell)} - 1$.

This completes the proof of the theorem. □

In the following corollary, we determine depth spectra of all λ-constacyclic codes of length p^s over $\mathcal{R}$ when $\alpha_0 = 1$.

Corollary 7.3.1. Let $\lambda = 1 + \gamma\beta$, where β is a unit in $\mathcal{R}$. Let $\mathcal{C}_{\ell,u} = \langle \gamma^{\ell}(x-1)^u \rangle$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$, where $0 \leq \ell \leq e-1$ and $0 \leq u < p^s$. Then the depth spectrum of the code $\mathcal{C}_{\ell,u}$ is given by

$$\text{Depth}(\mathcal{C}_{\ell,u}) = \begin{cases} \{1, 2, \cdots, p^s\} & \text{if } 0 \leq \ell \leq e-2; \\ \{1, 2, \cdots, p^s - u\} & \text{if } \ell = e-1. \end{cases}$$

Proof. It follows immediately from Theorem 7.3.2. □

7.3.2 The case $\alpha_0 \neq 1$

In this section, we will consider the case $\alpha_0 \neq 1$, and we will study depths of codewords and determine depth distributions of all λ-constacyclic codes of length p^s over $\mathcal{R}$. Here we assume, throughout this section, that $\lambda = \alpha_0^{p^s} + \gamma\beta$, where $\alpha_0 \in \mathcal{T} \setminus \{0, 1\}$ and β is a unit in $\mathcal{R}$. We will first fix some notations.

For $1 \leq k \leq p^s - 1$, $0 \leq w \leq p^s - 1$ and $0 \leq \ell \leq p^s - 1$, let $\mathcal{J}_{w,k}^{(\ell)} \in \mathcal{R}$ denote the coefficient of x^ℓ in $(x-1)^{p^s-k}(x-\alpha_0)^w$ modulo $x^{p^s} - \lambda$. Further, for $1 \leq k \leq p^s - 1$, let $\mathcal{A}_k$ denote the $(p^s - k) \times p^s$ matrix over $\mathcal{R}$ whose $(i,j)^{\text{th}}$ entry is $\mathcal{J}_{j-1,p^s-k}^{(k+i-1)}$ (i.e., the coefficient of x^{k+i-1} in $(x-1)^k(x-\alpha_0)^{j-1} \in \mathcal{R}_\lambda$), and let $\overline{\mathcal{A}_k}$ denote the $(p^s - k) \times p^s$ matrix over $\overline{\mathcal{R}}$ whose $(i,j)^{\text{th}}$ entry is $\overline{\mathcal{J}_{j-1,p^s-k}^{(k+i-1)}}$ for $1 \leq i \leq p^s - k$ and $1 \leq j \leq p^s$. For an integer $b \geq 1$ and $a_1, a_2, \cdots, a_b \in \overline{\mathcal{R}}$, let $\mathcal{V}(a_1, a_2, \cdots, a_b)$ denote the $b \times b$ Vandermonde matrix over $\overline{\mathcal{R}}$ whose $(i,j)^{\text{th}}$ entry is given by a_j^{i-1} for $1 \leq i, j \leq b$. Further, for a monic polynomial $f(x) \in \overline{\mathcal{R}}[x]$ of degree less than or equal to $b-2$, let $\mathcal{U}_f(a_1, a_2, \cdots, a_{b-1})$ denote the $(b-1) \times (b-1)$ matrix over $\overline{\mathcal{R}}$, defined as follows:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_{b-1} \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_{b-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{b-3} & a_2^{b-3} & a_3^{b-3} & \cdots & a_{b-1}^{b-3} \\ f(a_1) & f(a_2) & f(a_3) & \cdots & f(a_{b-1}) \end{bmatrix}.$$

To determine depth distributions of all λ-constacyclic codes of length p^s over $\mathcal{R}$, we shall first prove the following three lemmas:

Lemma 7.3.3. For an integer $b \geq 2$, let $a_1, a_2, \cdots, a_{b-1} \in \overline{\mathcal{R}}$, and let $f(x) \in \overline{\mathcal{R}}[x]$ be a monic polynomial of degree less than or equal to $b-2$. We have

$$\det \mathcal{U}_f(a_1, a_2, \cdots, a_{b-1}) = \begin{cases} 0 & \text{if } \deg f(x) \leq b-3; \\ \det \mathcal{V}(a_1, a_2, \cdots, a_{b-1}) & \text{if } \deg f(x) = b-2. \end{cases}$$

Proof. Proof is trivial. □

Lemma 7.3.4. Let $1 \leq k \leq p^s - 1$, $0 \leq \ell \leq p^s - k$, and let $a_1, a_2, \cdots, a_{k-1}$ be integers satisfying $1 \leq a_1 < a_2 < \cdots < a_{k-1} < p^s - \ell$. Further, let $\mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1})$ be the $k \times k$ matrix over $\overline{\mathcal{R}}$, whose first column is the $(\ell+1)^{\text{th}}$ column of the matrix $\overline{\mathcal{A}_{p^s-k}}$ and the j^{th} column is the $(\ell + a_{j-1} + 1)^{\text{th}}$ column of the matrix $\overline{\mathcal{A}_{p^s-k}}$ for $2 \leq j \leq k$. Then we have

$$\det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1})$$

$$= \frac{a_1 a_2 \cdots a_{k-1} \det \mathcal{V}(a_1, a_2, \cdots, a_{k-1})}{(k-1)!(k-2)! \cdots 3!2!1!} (1 - \overline{\alpha}_0)^{\{k\ell + a_1 + a_2 + \cdots + a_{k-1} - \binom{k}{2}\}}.$$

Proof. To prove the result, we will apply induction on $k \geq 1$.

When $k = 1$, we note that $\det \mathcal{B}(\ell) = \overline{\mathcal{J}_{\ell,1}^{(p^s-1)}}$, where $\mathcal{J}_{\ell,1}^{(p^s-1)}$ is the coefficient of x^{p^s-1} in the element $(x - \alpha_0)^\ell (x-1)^{p^s-1} \in \mathcal{R}_\lambda$. Further, it is easy to see that

$$\mathcal{J}_{\ell,1}^{(p^s-1)} = \sum_{\mu=0}^{\ell} (-1)^\mu \binom{p^s + \mu - 1}{p^s - 1} \binom{\ell}{\ell - \mu} (1 - \alpha_0)^{\ell - \mu}.$$

By Theorem 2.0.9, we observe that $\binom{p^s+t-1}{p^s-1} \equiv 0 \pmod{p}$ for $1 \leq t \leq \ell$, which implies that $\det \mathcal{B}(\ell) = \overline{\mathcal{J}_{\ell,1}^{(p^s-1)}} = (1 - \overline{\alpha}_0)^\ell$ in $\overline{\mathcal{R}}$. Thus the result holds when $k = 1$.

Now we assume that $2 \leq k \leq p^s - 1$ and that the result holds for $k-1$, i.e., we have

$$\det \mathcal{B}(\ell, t_1, t_2, \cdots, t_{k-2})$$

$$= \frac{t_1 t_2 \cdots t_{k-2} \det \mathcal{V}(t_1, t_2, \cdots, t_{k-2})}{(k-2)!(k-3)! \cdots 3!2!1!} (1 - \overline{\alpha}_0)^{\{(k-1)\ell + t_1 + t_2 + \cdots + t_{k-2} - \binom{k-1}{2}\}}, \tag{7.3.5}$$

where $0 \leq \ell \leq p^s - k + 1$ and $1 \leq t_1 < t_2 < \cdots < t_{k-2} < p^s - \ell$ are integers.

We assert that

$$\det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1})$$

$$= \frac{a_1 a_2 \cdots a_{k-1} \det \mathcal{V}(a_1, a_2, \cdots, a_{k-1})}{(k-1)!(k-2)! \cdots 3!2!1!} (1-\overline{\alpha}_0)^{\{k\ell + a_1 + a_2 + \cdots + a_{k-1} - \binom{k}{2}\}},$$

where $0 \leq \ell \leq p^s - k$ and $1 \leq a_1 < a_2 < \cdots < a_{k-1} < p^s - \ell$ are integers.

To prove this assertion, we first note that

$$\mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1}) = \begin{bmatrix} \overline{\mathcal{J}_{\ell,k}^{(p^s-k)}} & \overline{\mathcal{J}_{\ell+a_1,k}^{(p^s-k)}} & \overline{\mathcal{J}_{\ell+a_2,k}^{(p^s-k)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k}^{(p^s-k)}} \\ \overline{\mathcal{J}_{\ell,k}^{(p^s-k+1)}} & \overline{\mathcal{J}_{\ell+a_1,k}^{(p^s-k+1)}} & \overline{\mathcal{J}_{\ell+a_2,k}^{(p^s-k+1)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k}^{(p^s-k+1)}} \\ \overline{\mathcal{J}_{\ell,k}^{(p^s-k+2)}} & \overline{\mathcal{J}_{\ell+a_1,k}^{(p^s-k+2)}} & \overline{\mathcal{J}_{\ell+a_2,k}^{(p^s-k+2)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k}^{(p^s-k+2)}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \overline{\mathcal{J}_{\ell,k}^{(p^s-1)}} & \overline{\mathcal{J}_{\ell+a_1,k}^{(p^s-1)}} & \overline{\mathcal{J}_{\ell+a_2,k}^{(p^s-1)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k}^{(p^s-1)}} \end{bmatrix}.$$

Now for $0 \leq i \leq p^s - 1$, we see that

$$\begin{aligned} \mathcal{J}_{i,k-1}^{(0)} + \mathcal{J}_{i,k-1}^{(1)} x + \cdots + \mathcal{J}_{i,k-1}^{(p^s-1)} x^{p^s-1} &= (x-1)^{p^s-k+1}(x-\alpha_0)^i \\ &= (x-1)(x-1)^{p^s-k}(x-\alpha_0)^i \\ &= (x-1)\{\mathcal{J}_{i,k}^{(0)} + \mathcal{J}_{i,k}^{(1)} x + \cdots + \mathcal{J}_{i,k}^{(p^s-1)} x^{p^s-1}\}. \end{aligned}$$

This implies that

$$\begin{aligned} \mathcal{J}_{i,k-1}^{(p^s-k+1)} &= \mathcal{J}_{i,k}^{(p^s-k)} - \mathcal{J}_{i,k}^{(p^s-k+1)}, \\ \mathcal{J}_{i,k-1}^{(p^s-k+2)} &= \mathcal{J}_{i,k}^{(p^s-k+1)} - \mathcal{J}_{i,k}^{(p^s-k+2)}, \\ \cdots\cdots &\quad \cdots \quad \cdots\cdots\cdots\cdots \\ \mathcal{J}_{i,k-1}^{(p^s-2)} &= \mathcal{J}_{i,k}^{(p^s-3)} - \mathcal{J}_{i,k}^{(p^s-2)}, \\ \mathcal{J}_{i,k-1}^{(p^s-1)} &= \mathcal{J}_{i,k}^{(p^s-2)} - \mathcal{J}_{i,k}^{(p^s-1)}. \end{aligned}$$

In view of this and by applying suitable row operations on $\mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1})$, we obtain

$$\det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1}) = \det \begin{bmatrix} \overline{\mathcal{J}_{\ell,k-1}^{(p^s-k+1)}} & \overline{\mathcal{J}_{\ell+a_1,k-1}^{(p^s-k+1)}} & \overline{\mathcal{J}_{\ell+a_2,k-1}^{(p^s-k+1)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k-1}^{(p^s-k+1)}} \\ \overline{\mathcal{J}_{\ell,k-1}^{(p^s-k+2)}} & \overline{\mathcal{J}_{\ell+a_1,k-1}^{(p^s-k+2)}} & \overline{\mathcal{J}_{\ell+a_2,k-1}^{(p^s-k+2)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k-1}^{(p^s-k+2)}} \\ \overline{\mathcal{J}_{\ell,k-1}^{(p^s-k+3)}} & \overline{\mathcal{J}_{\ell+a_1,k-1}^{(p^s-k+3)}} & \overline{\mathcal{J}_{\ell+a_2,k-1}^{(p^s-k+2)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k-1}^{(p^s-k+3)}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \overline{\mathcal{J}_{\ell,k-1}^{(p^s-1)}} & \overline{\mathcal{J}_{\ell+a_1,k-1}^{(p^s-1)}} & \overline{\mathcal{J}_{\ell+a_2,k-1}^{(p^s-1)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k-1}^{(p^s-1)}} \\ \overline{\mathcal{J}_{\ell,k}^{(p^s-1)}} & \overline{\mathcal{J}_{\ell+a_1,k}^{(p^s-1)}} & \overline{\mathcal{J}_{\ell+a_2,k}^{(p^s-1)}} & \cdots & \overline{\mathcal{J}_{\ell+a_{k-1},k}^{(p^s-1)}} \end{bmatrix}.$$

From this, it follows that

$$\begin{aligned} &\det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1}) \\ &= (-1)^{k+1}\overline{\mathcal{J}_{\ell,k}^{(p^s-1)}} \det \mathcal{B}(\ell + a_1, a_2 - a_1, a_3 - a_1, \cdots, a_{k-1} - a_1) \\ &\quad +(-1)^{k+2}\overline{\mathcal{J}_{\ell+a_1,k}^{(p^s-1)}} \det \mathcal{B}(\ell, a_2, a_3, \cdots, a_{k-1}) \\ &\quad +(-1)^{k+3}\overline{\mathcal{J}_{\ell+a_2,k}^{(p^s-1)}} \det \mathcal{B}(\ell, a_1, a_3, a_4, \cdots, a_{k-1}) \\ &\quad +\cdots\cdots\cdots\cdots\cdots\cdots \\ &\quad +(-1)^{k+k-1}\overline{\mathcal{J}_{\ell+a_{k-2},k}^{(p^s-1)}} \det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-3}, a_{k-1}) \\ &\quad +(-1)^{k+k}\overline{\mathcal{J}_{\ell+a_{k-1},k}^{(p^s-1)}} \det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-2}). \end{aligned} \tag{7.3.6}$$

Further, for $t \in \{0, a_1, a_2, \cdots, a_{k-1}\}$, we recall that $\mathcal{J}_{\ell+t,k}^{(p^s-1)}$ is the coefficient of x^{p^s-1} in the element $(x-1)^{p^s-k}(x-\alpha_0)^{\ell+t} \in \mathcal{R}_\lambda$, so we have

$$\mathcal{J}_{\ell+t,k}^{(p^s-1)} = \sum_{\mu=0}^{\ell+t-k+1} (-1)^\mu \binom{p^s+\mu-1}{p^s-1} \binom{\ell+t}{k+\mu-1} (1-\alpha_0)^{\ell+t-k+1-\mu}.$$

Now using the fact that $\ell+t-k+1 \leq p^s-1$ and by applying Theorem 2.0.9, we observe that $\binom{p^s+i}{p^s-1} \equiv 0 \pmod p$ for $0 \leq i \leq \ell+t-k$ and $t \in \{0, a_1, a_2, \cdots, a_{k-1}\}$. This implies

that

$$\overline{\mathcal{J}_{\ell+t,k}^{(p^s-1)}} \;=\; \binom{\ell+t}{k-1}(1-\overline{\alpha}_0)^{\ell+t-k+1} \in \overline{\mathcal{R}} \quad \text{for} \quad t \in \{0, a_1, a_2, \cdots, a_{k-1}\}. \tag{7.3.7}$$

On substituting the values of $\overline{\mathcal{J}_{\ell+t,k}^{(p^s-1)}}$'s from (7.3.7) and values of the determinants from the induction hypothesis (7.3.5) in equation (7.3.6), we get

$$\begin{aligned}
&\det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1}) \\
&= \frac{(1-\overline{\alpha}_0)^{\{k\ell+a_1+a_2+\cdots+a_{k-1}-\binom{k}{2}\}}}{(k-2)!(k-3)!\cdots 3!2!1!} \\
&\quad \times \Bigg\{ (-1)^{k+1}\binom{\ell}{k-1}\prod_{j=2}^{k-1}(a_j-a_1)\det \mathcal{V}(a_2-a_1, a_3-a_1, \cdots, a_{k-1}-a_1) \\
&\qquad + (-1)^{k+2}\binom{\ell+a_1}{k-1}a_2a_3a_4\cdots a_{k-1}\det \mathcal{V}(a_2, a_3, a_4, \cdots, a_{k-1}) \\
&\qquad + (-1)^{k+3}\binom{\ell+a_2}{k-1}a_1a_3a_4\cdots a_{k-1}\det \mathcal{V}(a_1, a_3, a_4, \cdots, a_{k-1}) \\
&\qquad + \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\qquad + (-1)^{k+k-1}\binom{\ell+a_{k-2}}{k-1}a_1a_2\cdots a_{k-3}a_{k-1}\det \mathcal{V}(a_1, a_2, \cdots, a_{k-3}, a_{k-1}) \\
&\qquad + (-1)^{k+k}\binom{\ell+a_{k-1}}{k-1}a_1a_2a_3\cdots a_{k-2}\det \mathcal{V}(a_1, a_2, a_3\cdots, a_{k-2}) \Bigg\}.
\end{aligned} \tag{7.3.8}$$

Further, for $\ell + t \geq 0$, we note that

$$\binom{\ell+t}{k-1} \;=\; \sum_{\mu=0}^{k-1}\binom{\ell}{k-1-\mu}\binom{t}{\mu}.$$

Using this and by (7.3.8), we see that

$$\begin{aligned}
&\det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1}) \\
&= (-1)^{k+2} \frac{(1-\overline{\alpha}_0)^{\{k\ell+a_1+a_2+\cdots+a_{k-1}-\binom{k}{2}\}}}{(k-2)!(k-3)!\cdots 3!2!1!} \times \\
&\Bigg\{ \sum_{\mu=1}^{k-1} \binom{\ell}{k-\mu-1} \Bigg\{ \sum_{w=1}^{k-1} (-1)^{w-1} \binom{a_w}{\mu} a_1 a_2 \cdots a_{w-1} a_{w+1} a_{w+2} \cdots a_{k-1} \times \\
&\qquad \det \mathcal{V}(a_1, a_2, \cdots, a_{w-1}, a_{w+1}, a_{w+2}, \cdots, a_{k-1}) \Bigg\} \\
&\quad - \binom{\ell}{k-1} \Bigg\{ \sum_{\nu=1}^{k-1} (-1)^{\nu} a_1 a_2 \cdots a_{\nu-1} a_{\nu+1} a_{\nu+2} \cdots a_{k-1} \times \\
&\qquad \det \mathcal{V}(a_1, a_2, \cdots, a_{\nu-1}, a_{\nu+1}, a_{\nu+2}, \cdots, a_{k-1}) \\
&\qquad + \prod_{j=2}^{k-1} (a_j - a_1) \det \mathcal{V}(a_2 - a_1, a_3 - a_1, \cdots, a_{k-1} - a_1) \Bigg\} \Bigg\}.
\end{aligned}$$

This gives

$$\begin{aligned}
&\det \mathcal{B}(\ell, a_1, a_2, \cdots, a_{k-1}) \\
&= (-1)^{2k+2} \frac{(1-\overline{\alpha}_0)^{\{k\ell+a_1+a_2+\cdots+a_{k-1}-\binom{k}{2}\}}}{(k-2)!(k-3)!\cdots 3!2!1!} \\
&\quad \times \Bigg\{ \sum_{\mu=2}^{k-1} \binom{\ell}{k-1-\mu} \frac{a_1 a_2 \cdots a_{k-1}}{\mu!} \det \mathcal{U}_{f_{\mu-1}}(a_1, a_2, \cdots, a_{k-1}) \\
&\qquad + \binom{\ell}{k-2} a_1 a_2 \cdots a_{k-1} \det \mathcal{U}_1(a_1, a_2, \cdots, a_{k-1}) \Bigg\},
\end{aligned}$$

where $f_w(x) = (x-1)(x-2)\cdots(x-w)$ for $1 \leq w \leq k-2$. Now by applying Lemma 7.3.3, the desired assertion follows immediately. □

Lemma 7.3.5. For $1 \leq k \leq p^s - 1$, a $k \times k$ matrix formed by any k consecutive columns of $\mathcal{A}_{p^s-k}$ is invertible over $\mathcal{R}$.

Proof. By Lemma 7.3.4, we see that

$$\begin{aligned}
\det \mathcal{B}(\ell, 1, \cdots, k-1) &= \frac{(k-1)! \det \mathcal{V}(1, 2, \cdots, k-1)}{(k-1)!(k-2)!\cdots 3!2!1!} (1-\overline{\alpha_0})^{\{k\ell+1+2+\cdots+(k-1)-\binom{k}{2}\}} \\
&= \frac{(k-1)!(k-2)!\cdots 3!2!1!}{(k-1)!(k-2)!\cdots 3!2!1!} (1-\overline{\alpha_0})^{k\ell} = (1-\overline{\alpha_0})^{k\ell} \neq 0.
\end{aligned}$$

This implies that a $k \times k$ matrix formed by any k consecutive columns of $\overline{\mathcal{A}_{p^s-k}}$ is invertible. From this, the desired result follows immediately. □

In the following theorem, we provide a method to determine codewords with a prescribed depth in a λ-constacyclic code of length p^s over $\mathcal{R}$, where $\lambda = \alpha_0^{p^s} + \gamma\beta$ with $\alpha_0 \in \mathcal{T} \setminus \{0, 1\}$ and β a unit in $\mathcal{R}$.

Theorem 7.3.3. Let $\lambda = \alpha_0^{p^s} + \gamma\beta$, where $\alpha_0 \in \mathcal{T} \setminus \{0, 1\}$ and β is a unit in $\mathcal{R}$. Let $\mathcal{C}_{\ell,u}$ be a λ-constacyclic code of length p^s over $\mathcal{R}$, where $0 \leq \ell \leq e-1$ and $0 \leq u < p^s$. Further, let $C(x) \in \mathcal{C}_{\ell,u}$ be a non-zero codeword with the unique representation as

$$\begin{aligned} C(x) \;=\; & c_0 + c_1(x-\alpha_0) + \cdots + c_{u-1}(x-\alpha_0)^{u-1} + c_u(x-\alpha_0)^u + c_{u+1}(x-\alpha_0)^{u+1} \\ & + \cdots + c_{p^s-1}(x-\alpha_0)^{p^s-1}, \end{aligned}$$

where $c_0, c_1, \cdots, c_{u-1} \in \langle \gamma^{\ell+1} \rangle$ and $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle \gamma^{\ell} \rangle$. Then the following hold.

(a) For any integer k satisfying $1 \leq k \leq p^s - u$ and $k \leq p^s - 1$, the depth of the codeword $C(x) \in \mathcal{C}_{\ell,u}$ is $p^s - k + 1$ if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the following matrix equation for some non-zero $\tau \in \langle \gamma^{\ell} \rangle$:

$$\begin{aligned} & \begin{bmatrix} \mathcal{J}_{u,k}^{(p^s-k)} & \mathcal{J}_{u+1,k}^{(p^s-k)} & \cdots & \mathcal{J}_{u+k-2,k}^{(p^s-k)} & \mathcal{J}_{u+k-1,k}^{(p^s-k)} \\ \mathcal{J}_{u,k}^{(p^s-k+1)} & \mathcal{J}_{u+1,k}^{(p^s-k+1)} & \cdots & \mathcal{J}_{u+k-2,k}^{(p^s-k+1)} & \mathcal{J}_{u+k-1,k}^{(p^s-k+1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathcal{J}_{u,k}^{(p^s-2)} & \mathcal{J}_{u+1,k}^{(p^s-2)} & \cdots & \mathcal{J}_{u+k-2,k}^{(p^s-2)} & \mathcal{J}_{u+k-1,k}^{(p^s-2)} \\ \mathcal{J}_{u,k}^{(p^s-1)} & \mathcal{J}_{u+1,k}^{(p^s-1)} & \cdots & \mathcal{J}_{u+k-2,k}^{(p^s-1)} & \mathcal{J}_{u+k-1,k}^{(p^s-1)} \end{bmatrix} \begin{bmatrix} -c_u \\ -c_{u+1} \\ \vdots \\ -c_{u+k-2} \\ -c_{u+k-1} \end{bmatrix} \\ & = \begin{bmatrix} \tau + \sum_{i=0}^{u-1} c_i \mathcal{J}_{i,k}^{(p^s-k)} + \sum_{j=u+k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-k)} \\ \tau + \sum_{i=0}^{u-1} c_i \mathcal{J}_{i,k}^{(p^s-k+1)} + \sum_{j=u+k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-k+1)} \\ \vdots \\ \tau + \sum_{i=0}^{u-1} c_i \mathcal{J}_{i,k}^{(p^s-2)} + \sum_{j=u+k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-2)} \\ \tau + \sum_{i=0}^{u-1} c_i \mathcal{J}_{i,k}^{(p^s-1)} + \sum_{j=u+k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-1)} \end{bmatrix}. \end{aligned} \tag{7.3.9}$$

(b) For $p^s - u + 1 \leq k \leq p^s - 1$, the depth of the codeword $C(x) \in \mathcal{C}_{\ell,u}$ is $p^s - k + 1$ if and only if $c_0, c_1, \cdots, c_{p^s-1} \in \langle \gamma^{\ell+1} \rangle$ and they satisfy the following matrix equation for some non-zero $\tau \in \langle \gamma^{\ell+1} \rangle$:

$$\begin{bmatrix} 1 & \mathcal{J}_{1,k}^{(p^s-k)} & \mathcal{J}_{2,k}^{(p^s-k)} & \cdots & \mathcal{J}_{k-2,k}^{(p^s-k)} & \mathcal{J}_{k-1,k}^{(p^s-k)} \\ 0 & 1 & \mathcal{J}_{2,k}^{(p^s-k+1)} & \cdots & \mathcal{J}_{k-2,k}^{(p^s-k+1)} & \mathcal{J}_{k-1,k}^{(p^s-k+1)} \\ 0 & 0 & 1 & \cdots & \mathcal{J}_{k-2,k}^{(p^s-k+2)} & \mathcal{J}_{k-1,k}^{(p^s-k+2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \mathcal{J}_{k-1,k}^{(p^s-2)} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} -c_0 \\ -c_1 \\ -c_2 \\ \vdots \\ -c_{k-2} \\ -c_{k-1} \end{bmatrix} = \begin{bmatrix} \tau + \sum_{j=k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-k)} \\ \tau + \sum_{j=k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-k+1)} \\ \tau + \sum_{j=k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-k+2)} \\ \vdots \\ \tau + \sum_{j=k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-2)} \\ \tau + \sum_{j=k}^{p^s-1} c_j \mathcal{J}_{j,k}^{(p^s-1)} \end{bmatrix}. \tag{7.3.10}$$

(c) The depth of the codeword $C(x) \in \mathcal{C}_{\ell,u}$ is 1 if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the following matrix equation with $c_0, c_1, \cdots, c_{p^s-1} \in \langle \gamma^{\ell+1} \rangle$ when $u \geq 1$:

$$\begin{bmatrix} 1 & \mathcal{J}^{(1)}_{1,p^s-1} & \mathcal{J}^{(1)}_{2,p^s-1} & \cdots & \mathcal{J}^{(1)}_{p^s-4,p^s-1} & \mathcal{J}^{(1)}_{p^s-3,p^s-1} & \mathcal{J}^{(1)}_{p^s-2,p^s-1} \\ 0 & 1 & \mathcal{J}^{(2)}_{2,p^s-1} & \cdots & \mathcal{J}^{(2)}_{p^s-4,p^s-1} & \mathcal{J}^{(2)}_{p^s-3,p^s-1} & \mathcal{J}^{(2)}_{p^s-2,p^s-1} \\ 0 & 0 & 1 & \cdots & \mathcal{J}^{(3)}_{p^s-4,p^s-1} & \mathcal{J}^{(3)}_{p^s-3,p^s-1} & \mathcal{J}^{(3)}_{p^s-2,p^s-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \mathcal{J}^{(p^s-3)}_{p^s-3,p^s-1} & \mathcal{J}^{(p^s-3)}_{p^s-2,p^s-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 & \mathcal{J}^{(p^s-2)}_{p^s-2,p^s-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -c_0 \\ -c_1 \\ -c_2 \\ \vdots \\ -c_{p^s-4} \\ -c_{p^s-3} \\ -c_{p^s-2} \end{bmatrix} = \begin{bmatrix} c_{p^s-1}\mathcal{J}^{(1)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{J}^{(2)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{J}^{(3)}_{p^s-1,p^s-1} \\ \vdots \\ c_{p^s-1}\mathcal{J}^{(p^s-3)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{J}^{(p^s-2)}_{p^s-1,p^s-1} \\ c_{p^s-1}\mathcal{J}^{(p^s-1)}_{p^s-1,p^s-1} \end{bmatrix}. \tag{7.3.11}$$

Proof. To prove the result, we first recall, for $1 \leq k \leq p^s-1$, that $\text{depth}(C(x)) = p^s-k+1$ if and only if $D^{p^s-k}(C(x)) = (d, d, \cdots, d) \in \mathcal{R}^k$ for some $d(\neq 0) \in \mathcal{R}$. This, by Proposition 7.2.1, holds if and only if the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x) \in \mathcal{C}_{\ell,u}$ are equal to d modulo $x^{p^s} - \lambda$, where d is a non-zero element of $\mathcal{R}$.

(a) Let $1 \leq k \leq p^s - u$ and $k \leq p^s - 1$. To prove the result, we first assume that the depth of the codeword $C(x) \in \mathcal{C}_{\ell,u}$ is $p^s - k + 1$. This implies that the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x) \in \mathcal{C}_{\ell,u}$ are equal to d for some non-zero $d \in \mathcal{R}$. From this, it follows that $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the matrix equation (7.3.9) with $\tau = (-1)^{p^s-k+1}d$. Now using the fact that $(-1)^{p^s-k}d =$

$c_0\mathcal{J}_{0,k}^{(p^s-1)} + c_1\mathcal{J}_{1,k}^{(p^s-1)} + \cdots + c_{p^s-1}\mathcal{J}_{p^s-1,k}^{(p^s-1)}$ and $c_0, c_1, \cdots, c_{p^s-1} \in \langle\gamma^\ell\rangle$, we see that $d \in \langle\gamma^\ell\rangle \setminus \{0\}$.

Now to prove the converse part, suppose that $c_0, c_1, \cdots, c_{u-1} \in \langle\gamma^{\ell+1}\rangle$ and $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle\gamma^\ell\rangle$ satisfy the matrix equation (7.3.9) with $\tau \in \langle\gamma^\ell\rangle \setminus \{0\}$. Here we observe that $C(x) = c_0 + c_1(x-\alpha_0) + \cdots + c_{u-1}(x-\alpha_0)^{u-1} + c_u(x-\alpha_0)^u + \cdots + c_{p^s-1}(x-\alpha_0)^{p^s-1} \in \mathcal{C}_{\ell,u}$ and that the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x) \in \mathcal{C}_{\ell,u}$ are equal to $(-1)^{p^s-k+1}\tau$ modulo $x^{p^s} - \lambda$. From this, it follows that depth$(C(x)) = p^s - k + 1$. This completes the proof of the part (a).

(b) Next let $p^s - u + 1 \leq k \leq p^s - 1$. Here we first assume that the depth of the codeword $C(x) \in \mathcal{C}_{\ell,u}$ is p^s-k+1. This implies that the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x) \in \mathcal{C}_{\ell,u}$ are equal to d for some non-zero $d \in \mathcal{R}$. From this, it follows that $c_0, c_1, \cdots, c_{p^s-1}$ satisfy (7.3.9) with $\tau = (-1)^{p^s-k+1}d$. As $c_0, c_1, \cdots, c_{p^s-1} \in \langle\gamma^\ell\rangle$, we have $c_i = \gamma^\ell d_i$, where $d_i \in \mathcal{R}$ for $0 \leq i \leq p^s - 1$. Since $c_0, c_1, \cdots, c_{u-1} \in \langle\gamma^{\ell+1}\rangle$, we have $d_0, d_1, \cdots, d_{u-1} \in \langle\gamma\rangle$. Now using the fact that $(-1)^{p^s-k}d = c_{k-1} + c_{k+1}\mathcal{J}_{k,k}^{(p^s-1)} + \cdots + c_{p^s-1}\mathcal{J}_{p^s-1,k}^{(p^s-1)}$ and $c_{k-1}, c_k, \cdots, c_{p^s-1} \in \langle\gamma^\ell\rangle$, we see that $d \in \langle\gamma^\ell\rangle$. So we can write $(-1)^{p^s-k+1}d = \gamma^\ell g$ for some $g \in \mathcal{R}$. Now as $c_0, c_1, \cdots, c_{p^s-1}$ satisfy (7.3.9) with $\tau = (-1)^{p^s-k+1}d$, we get

$$\begin{bmatrix} 1 & \mathcal{J}_{1,k}^{(p^s-k)} & \mathcal{J}_{2,k}^{(p^s-k)} & \cdots & \mathcal{J}_{k-2,k}^{(p^s-k)} & \mathcal{J}_{k-1,k}^{(p^s-k)} \\ 0 & 1 & \mathcal{J}_{2,k}^{(p^s-k+1)} & \cdots & \mathcal{J}_{k-2,k}^{(p^s-k+1)} & \mathcal{J}_{k-1,k}^{(p^s-k+1)} \\ 0 & 0 & 1 & \cdots & \mathcal{J}_{k-2,k}^{(p^s-k+2)} & \mathcal{J}_{k-1,k}^{(p^s-k+2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \mathcal{J}_{k-1,k}^{(p^s-2)} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} -\gamma^\ell d_0 \\ -\gamma^\ell d_1 \\ -\gamma^\ell d_2 \\ \vdots \\ -\gamma^\ell d_{k-2} \\ -\gamma^\ell d_{k-1} \end{bmatrix}$$

$$= \begin{bmatrix} \gamma^\ell\Big(g + \sum_{j=k}^{p^s-1} d_j \mathcal{J}_{j,k}^{(p^s-k)}\Big) \\ \gamma^\ell\Big(g + \sum_{j=k}^{p^s-1} d_j \mathcal{J}_{j,k}^{(p^s-k+1)}\Big) \\ \gamma^\ell\Big(g + \sum_{j=k}^{p^s-1} d_j \mathcal{J}_{j,k}^{(p^s-k+2)}\Big) \\ \vdots \\ \gamma^\ell\Big(g + \sum_{j=k}^{p^s-1} d_j \mathcal{J}_{j,k}^{(p^s-2)}\Big) \\ \gamma^\ell\Big(g + \sum_{j=k}^{p^s-1} d_j \mathcal{J}_{j,k}^{(p^s-1)}\Big) \end{bmatrix}.$$

From this and using the fact that $0 \leq \ell \leq e-1$ and $d_0, d_1, \cdots, d_{u-1} \in \langle\gamma\rangle$, we obtain

$$\begin{aligned} -\overline{g} &= \overline{d_u}\,\overline{\mathcal{J}_{u,k}^{(p^s-k)}} + \overline{d_{u+1}}\,\overline{\mathcal{J}_{u+1,k}^{(p^s-k)}} + \cdots + \overline{d_{p^s-1}}\,\overline{\mathcal{J}_{p^s-1,k}^{(p^s-k)}}, && (1) \\ -\overline{g} &= \overline{d_u}\,\overline{\mathcal{J}_{u,k}^{(p^s-k+1)}} + \overline{d_{u+1}}\,\overline{\mathcal{J}_{u+1,k}^{(p^s-k+1)}} + \cdots + \overline{d_{p^s-1}}\,\overline{\mathcal{J}_{p^s-1,k}^{(p^s-k+1)}}, && (2) \\ -\overline{g} &= \overline{d_u}\,\overline{\mathcal{J}_{u,k}^{(p^s-k+2)}} + \overline{d_{u+1}}\,\overline{\mathcal{J}_{u+1,k}^{(p^s-k+2)}} + \cdots + \overline{d_{p^s-1}}\,\overline{\mathcal{J}_{p^s-1,k}^{(p^s-k+2)}}, && (3) \\ \cdots & \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ -\overline{g} &= \overline{d_u}\,\overline{\mathcal{J}_{u,k}^{(p^s-3)}} + \overline{d_{u+1}}\,\overline{\mathcal{J}_{u+1,k}^{(p^s-3)}} + \cdots + \overline{d_{p^s-1}}\,\overline{\mathcal{J}_{p^s-1,k}^{(p^s-3)}}, && (k-2) \\ -\overline{g} &= \overline{d_u}\,\overline{\mathcal{J}_{u,k}^{(p^s-2)}} + \overline{d_{u+1}}\,\overline{\mathcal{J}_{u+1,k}^{(p^s-2)}} + \cdots + \overline{d_{p^s-1}}\,\overline{\mathcal{J}_{p^s-1,k}^{(p^s-2)}}, && (k-1) \\ -\overline{g} &= \overline{d_u}\,\overline{\mathcal{J}_{u,k}^{(p^s-1)}} + \overline{d_{u+1}}\,\overline{\mathcal{J}_{u+1,k}^{(p^s-1)}} + \cdots + \overline{d_{p^s-1}}\,\overline{\mathcal{J}_{p^s-1,k}^{(p^s-1)}}. && (k) \end{aligned}$$

Next for $u \leq i \leq p^s - 1$, we observe that

$$\begin{aligned}
&\mathcal{J}_{i,k-1}^{(0)} + \mathcal{J}_{i,k-1}^{(1)} x + \cdots + \mathcal{J}_{i,k-1}^{(p^s-1)} x^{p^s-1} \\
&= (x-1)^{p^s-k+1}(x-\alpha_0)^i \\
&= (x-1)(x-1)^{p^s-k}(x-\alpha_0)^i \\
&= (x-1)\{\mathcal{J}_{i,k}^{(0)} + \mathcal{J}_{i,k}^{(1)} x + \cdots + \mathcal{J}_{i,k}^{(p^s-1)} x^{p^s-1}\},
\end{aligned}$$

which implies that

$$\begin{aligned}
\mathcal{J}_{i,k-1}^{(p^s-k+1)} &= \mathcal{J}_{i,k}^{(p^s-k)} - \mathcal{J}_{i,k}^{(p^s-k+1)}, \\
\mathcal{J}_{i,k-1}^{(p^s-k+2)} &= \mathcal{J}_{i,k}^{(p^s-k+1)} - \mathcal{J}_{i,k}^{(p^s-k+2)}, \\
\cdots\cdots &\cdots \cdots\cdots\cdots\cdots \\
\mathcal{J}_{i,k-1}^{(p^s-2)} &= \mathcal{J}_{i,k}^{(p^s-3)} - \mathcal{J}_{i,k}^{(p^s-2)}, \\
\mathcal{J}_{i,k-1}^{(p^s-1)} &= \mathcal{J}_{i,k}^{(p^s-2)} - \mathcal{J}_{i,k}^{(p^s-1)}.
\end{aligned}$$

In view of this and by subtracting the equation $(t+1)$ from the equation (t) for $1 \leq t \leq k-1$, we get

$$\left.\begin{aligned}
\overline{d_u}\ \overline{\mathcal{J}_{u,k-1}^{(p^s-k+1)}} + \overline{d_{u+1}}\ \overline{\mathcal{J}_{u+1,k-1}^{(p^s-k+1)}} + \cdots + \overline{d_{p^s-1}}\ \overline{\mathcal{J}_{p^s-1,k-1}^{(p^s-k+1)}} &= 0, \\
\overline{d_u}\ \overline{\mathcal{J}_{u,k-1}^{(p^s-k+2)}} + \overline{d_{u+1}}\ \overline{\mathcal{J}_{u+1,k-1}^{(p^s-k+2)}} + \cdots + \overline{d_{p^s-1}}\ \overline{\mathcal{J}_{p^s-1,k-1}^{(p^s-k+2)}} &= 0, \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \cdots \\
\overline{d_u}\ \overline{\mathcal{J}_{u,k-1}^{(p^s-2)}} + \overline{d_{u+1}}\ \overline{\mathcal{J}_{u+1,k-1}^{(p^s-2)}} + \cdots + \overline{d_{p^s-1}}\ \overline{\mathcal{J}_{p^s-1,k-1}^{(p^s-2)}} &= 0, \\
\overline{d_u}\ \overline{\mathcal{J}_{u,k-1}^{(p^s-1)}} + \overline{d_{u+1}}\ \overline{\mathcal{J}_{u+1,k-1}^{(p^s-1)}} + \cdots + \overline{d_{p^s-1}}\ \overline{\mathcal{J}_{p^s-1,k-1}^{(p^s-1)}} &= 0.
\end{aligned}\right\} \quad (7.3.12)$$

Further, by Lemma 7.3.5, we see that a $k-1 \times k-1$ matrix formed by any $k-1$ consecutive columns of $\mathcal{A}_{p^s-k+1}$ is invertible over $\mathcal{R}$, which implies a matrix formed by the last $k-1$ columns of $\overline{\mathcal{A}_{p^s-k+1}}$ is invertible over $\overline{\mathcal{R}}$. This further implies that the last p^s-u columns of $\overline{\mathcal{A}_{p^s-k+1}}$ are linear independent over $\overline{\mathcal{R}}$, as $p^s-u \leq k-1$.

From this and by (7.3.12), we get

$$\overline{d_u} \;=\; \overline{d_{u+1}} \;=\; \cdots \;=\; \overline{d_{p^s-1}} \;=\; 0 \;\text{ in }\; \overline{\mathcal{R}},$$

which implies that $d_u, d_{u+1}, \cdots, d_{p^s-1} \in \langle\gamma\rangle$. As $c_i = \gamma^\ell d_i$ for $u \le i \le p^s-1$, we see that $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle\gamma^{\ell+1}\rangle$. This shows that $c_0, c_1, \cdots, c_{p^s-1} \in \langle\gamma^{\ell+1}\rangle$. Now using the fact that $(-1)^{p^s-k+1}d = c_{k-1} + c_{k+1}\mathcal{J}_{k,k}^{(p^s-1)} + \cdots + c_{p^s-1}\mathcal{J}_{p^s-1,k}^{(p^s-1)}$ and $c_{k-1}, c_k, \cdots, c_{p^s-1} \in \langle\gamma^{\ell+1}\rangle$, we get $d \in \langle\gamma^{\ell+1}\rangle$.

Now to prove the converse part, suppose that $c_0, c_1, \cdots, c_{p^s-1} \in \langle\gamma^{\ell+1}\rangle$ satisfy the matrix equation (7.3.10) with $\tau \in \langle\gamma^{\ell+1}\rangle\setminus\{0\}$. From this, we observe that $C(x) = c_0 + c_1(x-\alpha_0) + \cdots + c_{u-1}(x-\alpha_0)^{u-1} + c_u(x-\alpha_0)^u + \cdots + c_{p^s-1}(x-\alpha_0)^{p^s-1} \in \mathcal{C}_{\ell,u}$ and that the coefficients of $x^{p^s-k}, x^{p^s-k+1}, \cdots, x^{p^s-1}$ in the codeword $(1-x)^{p^s-k}C(x) \in \mathcal{C}_{\ell,u}$ are equal to $(-1)^{p^s-k+1}\tau$ modulo $x^{p^s}-\lambda$. This implies that $\text{depth}(C(x)) = p^s-k+1$. This proves (b).

(c) Here working in a similar manner as in part (b), we observe that $\text{depth}(C(x)) = 1$ if and only if the coefficients of $x, x^2, \cdots, x^{p^s-1}$ in the codeword $(1-x)C(x)$ are zero modulo $x^{p^s}-\lambda$, which holds if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the matrix equation (7.3.11) with $c_0, c_1, \cdots, c_{p^s-1} \in \langle\gamma^{\ell+1}\rangle$ when $u \ge 1$.

This completes the proof of the theorem. □

In the following theorem, we determine depth distributions of all λ-constacyclic codes of length p^s over $\mathcal{R}$ when $\alpha_0 \neq 1$.

Theorem 7.3.4. Let $\lambda = \alpha_0^{p^s} + \gamma\beta$, where $\alpha_0 \in \mathcal{T}\setminus\{0,1\}$ and β is a unit in $\mathcal{R}$. Let $\mathcal{C}_{\ell,u} = \langle\gamma^\ell(x-\alpha_0)^u\rangle$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$, where $0 \le \ell \le e-1$ and $0 \le u < p^s$. If $\mathcal{D}_\rho(\mathcal{C}_{\ell,u})$ denotes the number of codewords in $\mathcal{C}$ having the depth as ρ for $1 \le \rho \le p^s$, then we have

$$\mathcal{D}_\rho(\mathcal{C}_{\ell,u}) \;=\; \begin{cases} p^{m(e-\ell-1)} - 1 & \text{if } \rho = 1 \text{ and } u \ge 1; \\ (p^{m(e-\ell-1)} - 1)p^{m(e-\ell-1)(\rho-1)} & \text{if } 2 \le \rho \le u; \\ (p^{m(e-\ell)} - 1)p^{m\{(e-\ell)(\rho-1)-u\}} & \text{if } u+1 \le \rho \le p^s. \end{cases}$$

Proof. Here we need to determine the numbers $\mathcal{D}_{p^s-k+1}(\mathcal{C}_{\ell,u})$ for $1 \leq k \leq p^s$. For this, we see, by Lemma 7.3.1, that each non-zero codeword $C(x) \in \mathcal{C}_{\ell,u}$ can be uniquely expressed as

$$C(x) = c_0 + c_1(x-\alpha_0) + \cdots + c_{u-1}(x-\alpha_0)^{u-1} + c_u(x-\alpha_0)^u + c_{u+1}(x-\alpha_0)^{u+1} + \cdots + c_{p^s-1}(x-\alpha_0)^{p^s-1},$$

where $c_0, c_1, \cdots, c_{u-1} \in \langle \gamma^{\ell+1} \rangle$ and $c_u, c_{u+1}, \cdots, c_{p^s-1} \in \langle \gamma^{\ell} \rangle$. Now we shall distinguish the following three cases: **(i)** $1 \leq k \leq p^s - u$ and $k \leq p^s - 1$ **(ii)** $p^s - u + 1 \leq k \leq p^s - 1$ and **(iii)** $k = p^s$.

(i) Let $1 \leq k \leq p^s - u$ and $k \leq p^s - 1$. Here by Theorem 7.3.3(a), we see that depth$(C(x)) = p^s - k + 1$ if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the matrix equation (7.3.9) for some non-zero $\tau \in \langle \gamma^{\ell} \rangle$. Using this and by applying Lemma 7.3.5, we obtain

$$\mathcal{D}_{p^s-k+1}(\mathcal{C}_{\ell,u}) = (p^{m(e-\ell)} - 1)p^{m\{(e-\ell-1)u+(e-\ell)(p^s-u-k)\}}.$$

(ii) Next let $p^s - u + 1 \leq k \leq p^s - 1$. Here by applying Theorem 7.3.3(b), we see that depth$(C(x)) = p^s - k + 1$ if and only if $c_0, c_1, \cdots, c_{p^s-1} \in \langle \gamma^{\ell+1} \rangle$ satisfy the matrix equation (7.3.10) for some non-zero $\tau \in \langle \gamma^{\ell+1} \rangle$. From this, we observe that

$$\mathcal{D}_{p^s-k+1}(\mathcal{C}_{\ell,u}) = (p^{m(e-\ell-1)} - 1)p^{m(e-\ell-1)(p^s-k)}.$$

(iii) Let $k = p^s$, so that we have $p^s - k + 1 = 1$. Here by applying Theorem 7.3.3(c), we see that depth$(C(x)) = 1$ if and only if $c_0, c_1, \cdots, c_{p^s-1}$ satisfy the matrix equation (7.3.11) with $c_0, c_1, \cdots, c_{p^s-1} \in \langle \gamma^{\ell+1} \rangle$ when $u \geq 1$. Now using the fact that $C(x) \neq 0$, $c_{p^s-1} \in \langle \gamma^{\ell+1} \rangle$ when $u \geq 1$ and $c_{p^s-1} \in \langle \gamma^{\ell} \rangle$ when $u = 0$, one can observe that

$$\mathcal{D}_1(\mathcal{C}_{\ell,u}) = \begin{cases} p^{m(e-\ell-1)} - 1 & \text{when } u \geq 1; \\ p^{m(e-\ell)} - 1 & \text{when } u = 0. \end{cases}$$

This completes the proof of the theorem. □

In the following corollary, we determine depth spectra of all λ-constacyclic codes of length p^s over $\mathcal{R}$ when $\alpha_0 \neq 1$.

Corollary 7.3.2. Let $\lambda = \alpha_0^{p^s} + \gamma\beta$, where $\alpha_0 \in \mathcal{T} \setminus \{0, 1\}$ and β is a unit in $\mathcal{R}$. Let $\mathcal{C}_{\ell,u} = \langle \gamma^\ell (x - \alpha_0)^u \rangle$ be a non-trivial λ-constacyclic code of length p^s over $\mathcal{R}$, where $0 \leq \ell \leq e-1$ and $0 \leq u < p^s$. Then the depth spectrum of the code $\mathcal{C}_{\ell,u}$ is given by

$$\text{Depth}(\mathcal{C}_{\ell,u}) = \begin{cases} \{1, 2, \cdots, p^s\} & \text{if } 0 \leq \ell \leq e-2; \\ \{u+1, u+2, \cdots, p^s\} & \text{if } \ell = e-1. \end{cases}$$

Proof. It follows immediately from Theorem 7.3.4. □

In the next section, we will propose two new turn-based two player roulette games and provide positional winning strategies for these games in terms of depths of words over a finite commutative ring with unity R.

7.4 Roulette games

A turn-based two player game is defined as a game played between two players in which the moves of the players are interleaved. The board games such as chess and tic-tac-toe are classical examples of turn-based two player games. A two player game is solved by providing a winning strategy for one of the players. In general, a winning strategy for a player is defined as a finite sequence of moves (i.e., a strategy) that enables the player to achieve the game target, irrespective of the moves of the opponent. Further, a winning strategy is said to be optimal if there is no other winning strategy that ensures the win for the player in a fewer number of moves. For more details, please refer to [59, 60, 85]. A winning strategy is said to be positional if it depends only on the current position of the play and not on the history of the play [18].

To define the roulette games, throughout this section, let R be a finite commutative ring with unity 1, and let $r_0 = 0, r_1, r_2, \cdots, r_{\sigma-1}$ be all the distinct elements of the ring R, where $r_0 = 0$ is the zero element of R. Here when $\sigma \geq 3$, we shall identify a roulette by a regular polygon having σ sides, which are labelled as $r_0, r_1, r_2, \cdots, r_{\sigma-1}$ cyclically in the

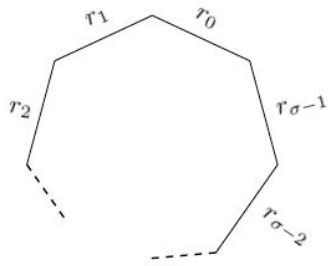

FIGURE 7.1: Roulette when $\sigma \geq 3$

anticlockwise direction (see Figure 7.1). Since a regular polygon with σ number of sides has a rotational symmetry of order σ, we assume that each roulette is free to rotate by an angle of $\frac{360^\circ}{\sigma} \times u$ in the anticlockwise direction, where $0 \leq u \leq \sigma - 1$ is an integer.

On the other hand, when $\sigma = 2$, we have $R = \mathbb{Z}_2 = \{0, 1\}$. Here we shall identify a roulette by a drinking glass. The drinking glass in the upright position corresponds to the element $0 \in \mathbb{Z}_2$, while the drinking glass in the upside down position corresponds to the element $1 \in \mathbb{Z}_2$.

7.4.1 Game 1

Consider the following game for two players, Player A and Player B, who are standing by a table. We assume that Player A is the adversary and Player B is blind. The game starts when Player B (blind) instructs Player A (the adversary) to place N drinking glasses on the table in a row, either in the upright position or in the upside down position, in such a way that not all glasses have the same orientation, where $N \geq 2$ is an integer. Player A labels these glasses as $0, 1, 2, \cdots, N-1$ from left to right. During the course of the game, Player A will keep on removing either the leftmost glass or the rightmost glass (but not both) from the row of glasses on the table before following instructions of Player B, unless all glasses on the table are in the upright position. At the same time, Player B attempts to force Player A to put all glasses on the table in the upright position by providing suitable instructions. For $\ell = 1, 2, 3, \cdots, N-1$, the ℓ-th round of the game goes in the following manner.

I. Player B provides the key $\mathbf{K}_{\ell-1} = \left(k_0^{(\ell-1)}, k_1^{(\ell-1)}, \cdots, k_{N-\ell-1}^{(\ell-1)}\right) \in \mathbb{Z}_2^{N-\ell}$ to Player A.

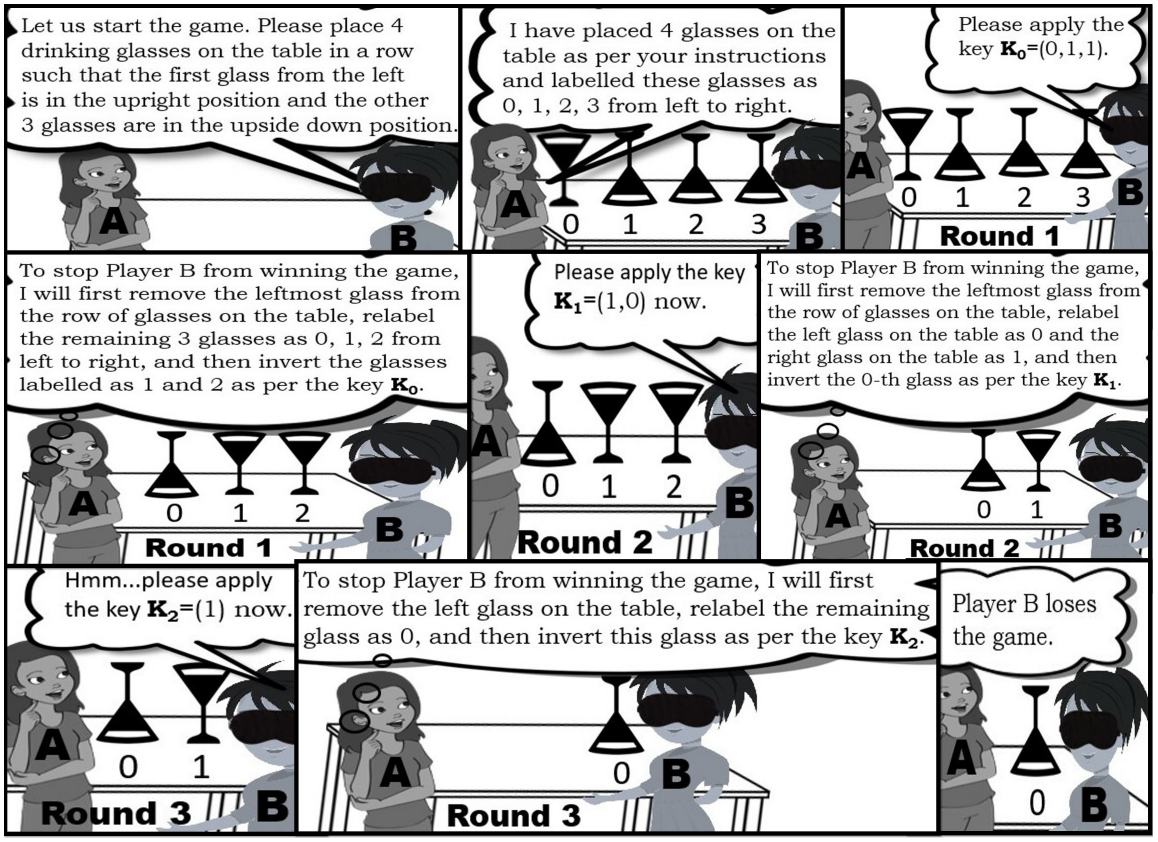

FIGURE 7.2: Example I

II. Now Player A removes either the leftmost glass or the rightmost glass (but not both) from the row of glasses on the table, relabels the remaining $N - \ell$ glasses as $0, 1, 2, \cdots, N - \ell - 1$ from left to right, and inverts these glasses as per the key $\mathbf{K}_{\ell-1}$, i.e., Player A inverts the i-glass on the table if and only if $k_i^{(\ell-1)} = 1$ for $0 \leq i \leq N - \ell - 1$. This completes the ℓ-th round.

III. Player B wins the game after the ℓ-th round if all the $N - \ell$ glasses on the table are in the upright position. Otherwise, the game continues with the $(\ell + 1)$-th round.

We say that Player B wins the game if there exists an integer ℓ satisfying $1 \leq \ell \leq N - 1$ such that all glasses on the table are in the upright position after the ℓ-th round. Otherwise, Player B loses the game. □

We illustrate this game in Figures 7.2 and 7.3. We further generalize this game for larger alphabet sizes as follows:

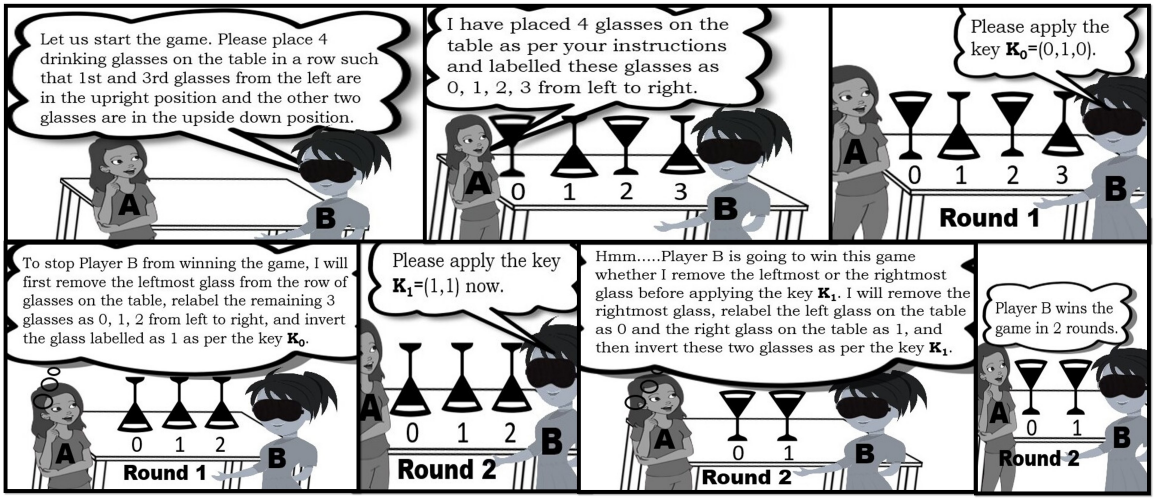

FIGURE 7.3: Example II

A generalization of Game 1 for larger alphabet sizes

Consider the following game for two players, Player A (the adversary) and Player B (blind), who are standing by a table. The game starts when Player B (blind) instructs Player A (the adversary) to place N identical roulettes on the table and to fix the orientations of these roulettes in such a way that each roulette has a side parallel to the row of roulettes and visible to both the players and that this particular side is not labelled by the same element of the ring R (i.e., these N roulettes do not have the same orientation). Further, Player A labels these N roulettes as $0, 1, 2, \cdots, N-1$ as we move from left to right. In other words, the game starts when Player B chooses a non-repeated word $W_0 = (W_0^{(0)}, W_1^{(0)}, \cdots, W_{N-1}^{(0)}) \in R^N$ (called the initial word), and instructs Player A to fix the orientations of all the N roulettes on the table in such a way that the side of the j-th roulette parallel to the row of roulettes and visible to both the players is labelled by the ring element $W_j^{(0)} \in R$ for $0 \leq j \leq N-1$.

During the course of the game, Player A has the freedom to remove either the leftmost roulette or the rightmost roulette (but not both) from the row of roulettes on the table before following the instructions of Player B, unless the side of each roulette parallel to the row of roulettes and visible to both the players is labelled by the zero element $r_0 = 0$ of the ring R. At the same time, Player B attempts to force Player A to fix positions of all the roulettes on the table in this special orientation by providing suitable instructions. Further, for $1 \leq \ell \leq N-1$, during the ℓ-th round, when Player A removes either the leftmost or the

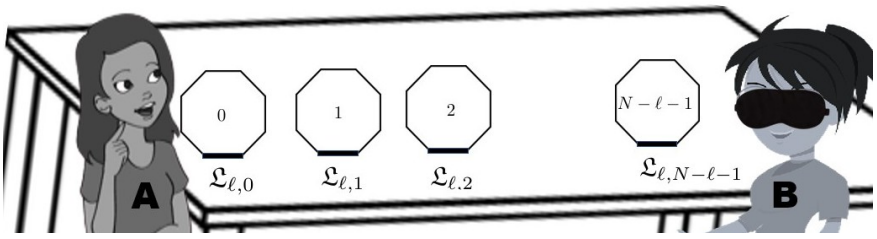

FIGURE 7.4: The ℓ-th round of Game 1

rightmost roulette from the row of roulettes on the table and relabels the remaining $N-\ell$ roulettes on the table as $0, 1, 2, \cdots, N-\ell-1$ from left to right, suppose that the side of the j-th roulette parallel to the row of roulettes and visible to both the players is labelled by the ring element $\mathfrak{L}_{\ell,j} \in R$ for $0 \leq j \leq N-\ell-1$ as shown in Figure 7.4.

Now for $\ell = 1, 2, \cdots, N-1$, the ℓ-th round of the game goes in the following manner.

I. The ℓ-th round of the game starts when Player B provides the key $\mathbf{K}_{\ell-1} = \big(k_0^{(\ell-1)}, k_1^{(\ell-1)}, \cdots, k_{N-\ell-1}^{(\ell-1)}\big) \in R^{N-\ell}$ to Player A. Thereafter, Player A removes either the rightmost or the leftmost roulette (but not both) from the row of roulettes on the table, relabels the remaining $N-\ell$ roulettes as $0, 1, 2, \cdots, N-\ell-1$ from left to right, and then rotates these roulettes in such a way that either $\mathfrak{L}_{\ell,j} = W_j^{(\ell-1)} + k_j^{(\ell-1)} = W_j^{(\ell)}$ for $0 \leq j \leq N-\ell-1$ or $\mathfrak{L}_{\ell,j} = W_{j+1}^{(\ell-1)} + k_j^{(\ell-1)} = W_j^{(\ell)}$ for $0 \leq j \leq N-\ell-1$ according as the Player A removes the rightmost or the leftmost roulette from the row of roulettes on the table. That is, Player A chooses the integer $s_{\ell-1}$ as 0 or 1 according as the Player A removes the rightmost or the leftmost roulette from the row of roulettes on the table, relabels the remaining $N-\ell$ roulettes as $0, 1, 2, \cdots, N-\ell-1$ from left to right, and then rotates these roulettes on the table in such a way that $\mathfrak{L}_{\ell,j} = W_{j+s_{\ell-1}}^{(\ell-1)} + k_j^{(\ell-1)} = W_j^{(\ell)}$ for $0 \leq j \leq N-\ell-1$. This completes the ℓ-th round.

II. Player B wins the game after the ℓ-th round if $\mathfrak{L}_{\ell,j} = 0$ for $0 \leq j \leq N-\ell-1$. Otherwise, the game continues with the $(\ell+1)$-th round.

We say that Player B wins the game if there exists an integer ℓ satisfying $1 \leq \ell \leq N-1$ such that all the roulettes on the table are positioned in such a way that $\mathfrak{L}_{\ell,j} = 0$ for $0 \leq j \leq N-\ell-1$ after the ℓ-th round. Otherwise, Player B loses the game. □

Next for a word $V = (v_0, v_1, \cdots, v_{N-1}) \in R^N$ and $1 \leq i \leq N$, let us define $[V]_i = (v_0, v_1, v_2, \cdots, v_{i-1}) \in R^i$ and $\langle V \rangle_i = (v_{N-i}, v_{N-i+1}, v_{N-i+2}, \cdots, v_{N-1}) \in R^i$. Furthermore, define a map $E : R^N \to R^N$ as $E(V) = (v_1, v_2, \cdots, v_{N-1}, v_0)$ for each $V = (v_0, v_1, v_2, \cdots, v_{N-1}) \in R^N$. Note that $D(V) = [E(V) - V]_{N-1}$ for each $V \in R^N$. We are now ready to provide a mathematical version of Game 1.

Mathematical version of Game 1

The game starts when Player B chooses a non-repeated word $W_0 = (W_0^{(0)}, W_1^{(0)}, \cdots, W_{N-1}^{(0)}) \in R^N$ (called the initial word) and instructs Player A to rotate the roulettes placed on the table in such a way that the side of the j-th roulette parallel to the row of roulettes and visible to both the players is labelled by the ring element $W_j^{(0)} \in R$ for $0 \leq j \leq N-1$. Now for $\ell = 1, 2, \cdots, N-1$, the ℓ-th round of the game goes in the following manner.

I. The ℓ-th round of the game starts when Player B provides the key $\mathbf{K}_{\ell-1} = \big(k_0^{(\ell-1)}, k_1^{(\ell-1)}, \cdots, k_{N-\ell-1}^{(\ell-1)}\big) \in R^{N-\ell}$ to Player A. Thereafter, Player A chooses the integer $s_{\ell-1}$ as 0 or 1 according as the Player A removes the rightmost or the leftmost roulette from the row of roulettes on the table, relabels the remaining $N-\ell$ roulettes as $0, 1, 2, \cdots, N-\ell-1$ from left to right, and creates the word $W_\ell \in R^{N-\ell}$ as

$$W_\ell = [E^{s_{\ell-1}}(W_{\ell-1})]_{N-\ell} + \mathbf{K}_{\ell-1} = \big(W_0^{(\ell)}, W_1^{(\ell)}, \cdots, W_{N-\ell-1}^{(\ell)}\big).$$

Player A further rotates the remaining $N-\ell$ roulettes on the table in such a way that $\mathfrak{L}_{\ell,j} = W_j^{(\ell)}$ for $0 \leq j \leq N-\ell-1$. This completes the ℓ-th round.

II. Player B wins the game after the ℓ-th round if $W_\ell = \big(W_0^{(\ell)}, W_1^{(\ell)}, \cdots, W_{N-\ell-1}^{(\ell)}\big) = (0, 0, \cdots, 0) \in R^{N-\ell}$. Otherwise, the game continues with the $(\ell+1)$-th round.

We say that Player B wins the game if there exists an integer ℓ satisfying $1 \leq \ell \leq N-1$ and $W_\ell = (0, 0, \cdots, 0) \in R^{N-\ell}$ (or equivalently, if all the roulettes on the table are positioned in such a way that $\mathfrak{L}_{\ell,j} = 0$ for $0 \leq j \leq N-\ell-1$) after the ℓ-th round. Otherwise, Player B loses the game. □

In the following theorem, we show that Player B has no positional winning strategy in Game 1 if Player B chooses an initial word $W_0 \in R^N$ of depth N.

Theorem 7.4.1. In Game 1, Player B has no positional winning strategy if Player B chooses an initial word $W_0 \in R^N$ of depth N.

Proof. Let us suppose that Player B chooses an initial word $W_0 \in R^N$ of depth N. Here we will prove that there is no positional winning strategy for Player B. For this, we will show that given any set of keys suggested by Player B, there is a strategy for Player A, which does not allow Player B to win the game.

Suppose that $\mathbf{K}_0, \mathbf{K}_1, \cdots, \mathbf{K}_{N-2}$ are the keys provided by Player B during 1st, 2nd, $\cdots$, $(N-1)$-th rounds, respectively. Now for $1 \leq \ell \leq N-2$, we assert that there exists an integer $s_{\ell-1} \in \{0,1\}$ such that the depth of the word $W_\ell = [E^{s_{\ell-1}}(W_{\ell-1})]_{N-\ell} + \mathbf{K}_{\ell-1} \in R^{N-\ell}$ is $N-\ell$.

To prove this assertion, for $1 \leq \ell \leq N-2$, let us write $D^{N-\ell-1}(W_{\ell-1}) = (e_0^{(\ell-1)}, e_1^{(\ell-1)}) \in R^2$, and let us define $U_\ell = [W_{\ell-1}]_{N-\ell} + \mathbf{K}_{\ell-1} \in R^{N-\ell}$ and $V_\ell = [E(W_{\ell-1})]_{N-\ell} + \mathbf{K}_{\ell-1} \in R^{N-\ell}$ for $1 \leq \ell \leq N-2$. Now we will apply induction on $\ell \geq 1$.

To prove the assertion for $\ell = 1$, we note that $D^{N-2}(W_0) = \left(e_0^{(0)}, e_1^{(0)}\right)$ and depth$(W_0) = N$. So we must have $e_0^{(0)} \neq e_1^{(0)}$. Next we observe that

$$D^{N-2}(U_1) = [D^{N-2}(W_0)]_1 + D^{N-2}(\mathbf{K}_0) \quad \text{and} \quad D^{N-2}(V_1) = \langle D^{N-2}(W_0)\rangle_1 + D^{N-2}(\mathbf{K}_0).$$

This implies that

$$D^{N-2}(U_1) = e_0^{(0)} + D^{N-2}(\mathbf{K}_0) \quad \text{and} \quad D^{N-2}(V_1) = e_1^{(0)} + D^{N-2}(\mathbf{K}_0).$$

Further, since $e_0^{(0)} \neq e_1^{(0)}$, both $D^{N-2}(U_1)$ and $D^{N-2}(V_1)$ can not be zero. This shows that either depth$(U_1) = N-1$ or depth$(V_1) = N-1$. Now let us choose the word W_1 as U_1 or V_1 according as depth$(U_1) = N-1$ or depth$(V_1) = N-1$. Thus the above assertion holds when $\ell = 1$.

Now let ℓ_0 be a fixed integer satisfying $2 \leq \ell_0 \leq N-2$. Suppose that the above assertion holds for $\ell = \ell_0 - 1$. That is, there exists an integer $s_{\ell_0-2} \in \{0,1\}$ such that the depth of the word $W_{\ell_0-1} = [E^{s_{\ell_0-2}}(W_{\ell_0-2})]_{N-\ell_0+1} + \mathbf{K}_{\ell_0-2} \in R^{N-\ell_0+1}$ is $N-\ell_0+1$.

Now to prove the assertion for $\ell = \ell_0$, we see that $D^{N-\ell_0-1}(W_{\ell_0-1}) = \left(e_0^{(\ell_0-1)}, e_1^{(\ell_0-1)}\right)$ and depth$(W_{\ell_0-1}) = N - \ell_0 + 1$, which implies that $e_0^{(\ell_0-1)} \neq e_1^{(\ell_0-1)}$. Further, as

$$D^{N-\ell_0-1}(U_{\ell_0}) = [D^{N-\ell_0-1}(W_{\ell_0-1})]_1 + D^{N-\ell_0-1}(\mathbf{K}_{\ell_0-1})$$

and

$$D^{N-\ell_0-1}(V_{\ell_0}) = \langle D^{N-\ell_0-1}(W_{\ell_0-1})\rangle_1 + D^{N-\ell_0-1}(\mathbf{K}_{\ell_0-1}),$$

we get

$$D^{N-\ell_0-1}(U_{\ell_0}) = e_0^{(\ell_0-1)} + D^{N-\ell_0-1}(\mathbf{K}_{\ell_0-1})$$

and

$$D^{N-\ell_0-1}(v_{\ell_0}) = e_1^{(\ell_0-1)} + D^{N-\ell_0-1}(\mathbf{K}_{\ell_0-1}).$$

As $e_0^{(\ell_0-1)} \neq e_1^{(\ell_0-1)}$, both $D^{N-\ell_0-1}(U_{\ell_0})$ and $D^{N-\ell_0-1}(V_{\ell_0})$ can not be zero. Now let us choose the word W_{ℓ_0} as U_{ℓ_0} or V_{ℓ_0} according as depth$(U_{\ell_0}) = N-\ell_0$ or depth$(V_{\ell_0}) = N-\ell_0$. This completes the proof of the assertion.

Now let us consider the scenario, in which Player A, being the adversary, chooses an integer $s_{\ell-1} \in \{0, 1\}$ such that the depth of the word $W_\ell = [E^{s_{\ell-1}}(W_{\ell-1})]_{N-\ell} + \mathbf{K}_{\ell-1} \in R^{N-\ell}$ is $N - \ell$ for $1 \leq \ell \leq N - 2$. By the above assertion, we see that such an integer $s_{\ell-1}$ always exists for $1 \leq \ell \leq N - 2$, $W_{N-2} \in R^2$ and depth$(W_{N-2}) = 2$. Now as $W_{N-2} = (W_0^{(N-2)}, W_1^{(N-2)})$, we must have $W_0^{(N-2)} \neq W_1^{(N-2)}$. From this, we see that either $[W_{N-2}]_1 + \mathbf{K}_{N-2} = W_0^{(N-2)} + \mathbf{K}_{N-2} \neq 0$ or $[E(W_{N-2})]_1 + \mathbf{K}_{N-2} = W_1^{(N-2)} + \mathbf{K}_{N-2} \neq 0$. Now Player A, being the adversary, will choose $s_{N-2} \in \{0, 1\}$ such that $W_{N-1} = [E^{s_{N-2}}(W_{N-2})]_1 + \mathbf{K}_{N-2} \neq 0$. Hence Player B loses the game.

This completes the proof of the theorem. □

In the following theorem, we show that Player B has a positional winning strategy in Game 1 if Player B chooses an initial word $W_0 \in R^N$ of depth at most $N - 1$.

Theorem 7.4.2. In Game 1, Player B has a positional winning strategy if Player B chooses an initial word $W_0 \in R^N$ satisfying depth$(W_0) \leq N - 1$.

Proof. Suppose that Player B chooses an initial word $W_0 \in R^N$ satisfying $\mathrm{depth}(W_0) = t \leq N-1$. Note that W_0 is a non-repeated word. Now the following sequence of moves is a winning strategy ($\star$) for Player B:

I. Player B provides the key $\mathbf{K}_0 = -[W_0]_{N-1} \in R^{N-1}$ to Player A. Now Player A, being the adversary, chooses the integer $s_0 = 1$ (i.e., removes the leftmost roulette from the row of roulettes on the table), creates the word $W_1 \in R^{N-1}$ as

$$W_1 = [E(W_0)]_{N-1} + \mathbf{K}_0 = [E(W_0)]_{N-1} - [W_0]_{N-1} = D(W_0),$$

relabels the remaining $N-1$ roulettes on the table as $0, 1, 2, \cdots, N-2$ from left to right, and rotates these roulettes in such a way that

$$\big(\mathfrak{L}_{1,0}, \mathfrak{L}_{1,1}, \cdots, \mathfrak{L}_{1,N-2}\big) = W_1 = D(W_0).$$

That is, Player A holds the word $W_1 = D(W_0)$ after the first round.

II. Next for $\ell = 2, 3, \cdots, N-1$ respectively, do the following steps: Assume that after the $(\ell-1)$-th round, Player A (the adversary) holds the word $W_{\ell-1} = D^{\ell-1}(W_0) \in R^{N-\ell+1}$. Thereafter, Player B provides the key $\mathbf{K}_{\ell-1} = -[D^{\ell-1}(W_0)]_{N-\ell} \in R^{N-\ell}$ to Player A. Now Player A, being the adversary, chooses the integer $s_{\ell-1} = 1$ (i.e., removes the leftmost roulette from the row of roulettes on the table), creates the word $W_\ell \in R^{N-\ell}$ as

$$W_\ell = [E(W_{\ell-1})]_{N-\ell} + \mathbf{K}_{\ell-1} = [E(D^{\ell-1}(W_0))]_{N-\ell} - [D^{\ell-1}(W_0)]_{N-\ell} = D^\ell(W_0),$$

relabels the remaining $N-\ell$ roulettes on the table as $0, 1, 2, \cdots, N-\ell-1$ from left to right, and rotates these roulettes in such a way that

$$\big(\mathfrak{L}_{\ell,0}, \mathfrak{L}_{\ell,1}, \cdots, \mathfrak{L}_{\ell,N-\ell-1}\big) = W_\ell = D^\ell(W_0).$$

That is, Player A holds the word $W_\ell = D^\ell(W_0)$ after the ℓ-th round.

Now as $\mathrm{depth}(W_0) = t \leq N-1$, we have $W_t = D^t(W_0) = (0, 0, \cdots, 0) \in R^{N-t}$. This

implies that after t rounds, all the remaining $N-t$ roulettes on the table are positioned in such a way that $\mathfrak{L}_{t,j}=0$ for $0\leq j\leq N-t-1$. Hence Player B will win the game in at most t rounds. □

Remark 7.4.1. By Theorem 7.4.1, we note that Player B will always lose Game 1 if Player B chooses an initial word $W_0\in R^N$ of depth N. On the other hand, if Player B chooses an initial word $W_0\in R^N$ of depth $t\leq N-1$, then by Theorem 7.4.2, we see that Player B will win this game in at most t rounds by following the strategy $(\star)$.

In the following theorem, we show that the winning strategy $(\star)$, provided in the proof of Theorem 7.4.2, is an optimal winning strategy for Player B in Game 1.

Theorem 7.4.3. In Game 1, suppose that Player B chooses an initial word $W_0\in R^N$ such that $\text{depth}(W_0)=t\leq N-1$. Then there is no strategy that forces a win for Player B in less than t rounds. As a consequence, the winning strategy $(\star)$, provided in the proof of Theorem 7.4.2, is an optimal winning strategy for Player B.

Proof. As $\text{depth}(W_0)=t\leq N-1$, by following the winning strategy $(\star)$ provided in the proof of Theorem 7.4.2, we see that Player B will win the game in at most t rounds.

Now to prove the result, we will show that given any set of keys provided by Player B, there is a strategy for Player A, which does not allow Player B to win the game in less than t rounds.

To do this, suppose that Player B provides the keys $\mathbf{K}_0,\mathbf{K}_1,\cdots,\mathbf{K}_{N-2}$ during 1st, 2nd, $\cdots$, $(N-1)$-th rounds, respectively. For $1\leq\ell\leq t-1$, we assert that there exists an integer $s_{\ell-1}\in\{0,1\}$ such that the depth of the word $W_\ell=[E^{s_{\ell-1}}(W_{\ell-1})]_{N-\ell}+\mathbf{K}_{\ell-1}\in R^{N-\ell}$ is at least $t-\ell$.

To prove the assertion, let us define $U_\ell=[W_{\ell-1}]_{N-\ell}+\mathbf{K}_{\ell-1}\in R^{N-\ell}$ and $V_\ell=[E(W_{\ell-1})]_{N-\ell}+\mathbf{K}_{\ell-1}\in R^{N-\ell}$ for $1\leq\ell\leq t-1$. Now we will apply induction on $\ell\geq 1$.

To prove the above assertion for $\ell=1$, we note that $\text{depth}(W_0)=t$. This implies that

$$D^{t-2}(W_0)=(d,d+f,d+2f,\cdots,d+(N-t+1)f),$$

where $d, f \in R$ and $f \neq 0$. Further, let us write $D^{t-2}(\mathbf{K}_0) = (\ell_0, \ell_1, \cdots, \ell_{N-t}) \in R^{N-t+1}$. From this, we observe that

$$\begin{aligned} D^{t-2}(U_1) &= [D^{t-2}(W_0)]_{N-t+1} + D^{t-2}(\mathbf{K}_0) \\ &= (d+\ell_0, d+f+\ell_1, d+2f+\ell_2, \cdots, d+(N-t)f+\ell_{N-t}) \end{aligned}$$

and

$$\begin{aligned} D^{t-2}(V_1) &= \langle D^{t-2}(W_0)\rangle_{N-t+1} + D^{t-2}(\mathbf{K}_0) \\ &= (d+f+\ell_0, d+2f+\ell_1, d+3f+\ell_2, \cdots, d+(N-t+1)f+\ell_{N-t}). \end{aligned}$$

Now as f is non-zero, we see that both $D^{t-2}(U_1)$ and $D^{t-2}(V_1)$ can not be zero. This implies that either depth$(U_1) \geq t-1$ or depth$(V_1) \geq t-1$. Let us choose W_1 as either U_1 or V_1, according as depth$(U_1) \geq t-1$ or depth$(V_1) \geq t-1$. Thus the result holds when $\ell = 1$.

Now we assume that $1 \leq h \leq t-2$ is a fixed integer. Suppose that the result holds for $\ell = h$. That is, there exists an integer $s_{h-1} \in \{0, 1\}$ such that the depth of the word $W_h = [E^{s_{h-1}}(W_{h-1})]_{N-h} + \mathbf{K}_{h-1} \in R^{N-h}$ is at least $t-h$. Let depth$(W_h) = d_h \geq t-h$. This implies that

$$D^{d_h-2}(W_h) = (v, v+w, v+2w, \cdots, v+(N-d_h-h+1)w),$$

where $v, w \in R$ and $w \neq 0$. Further, let us write $D^{d_h-2}(\mathbf{K}_h) = (b_0, b_1, \cdots, b_{N-d_h-h}) \in R^{N-d_h-h+1}$. From this, we observe that

$$\begin{aligned} D^{d_h-2}(U_{h+1}) &= [D^{d_h-2}(W_h)]_{N-d_h-h+1} + D^{d_h-2}(\mathbf{K}_h) \\ &= (v+b_0, v+w+b_1, \cdots, v+(N-d_h-h)w+b_{N-d_h-h}) \end{aligned}$$

and

$$\begin{aligned} D^{d_h-2}(V_{h+1}) &= \langle D^{d_h-2}(W_h)\rangle_{N-d_h-h+1} + D^{d_h-2}(\mathbf{K}_h) \\ &= (v+w+b_0, v+2w+b_1, \cdots, v+(N-d_h-h+1)w+b_{N-d_h-h}). \end{aligned}$$

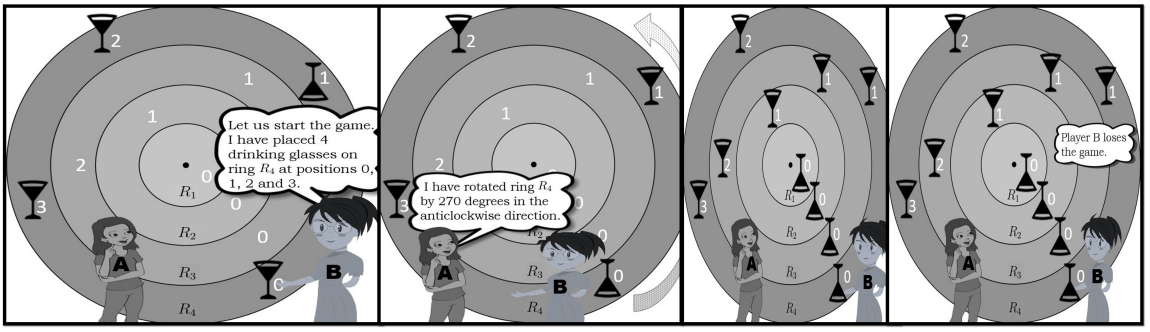

FIGURE 7.5: Example III

Since w is non-zero, both $D^{d_h-2}(U_{h+1})$ and $D^{d_h-2}(V_{h+1})$ can not be zero. This shows that either depth$(U_{h+1}) \geq d_h - 1$ or depth$(V_{h+1}) \geq d_h - 1$. Let us choose W_{h+1} as U_{h+1} or V_{h+1} according as depth$(U_{h+1}) \geq d_h - 1$ or depth$(V_{h+1}) \geq d_h - 1$. As $d_h \geq t - h$, we see that depth$(W_{h+1}) \geq d_h - 1 \geq t - h - 1$, which completes the proof of the assertion.

Now for $1 \leq \ell \leq t-1$, during the ℓ-th round, Player A, being the adversary, chooses an integer $s_{\ell-1} \in \{0, 1\}$ such that the depth of the word $W_\ell = [E^{s_{\ell-1}}(W_{\ell-1})]_{N-\ell} + \mathbf{K}_{\ell-1}$ is at least $t - \ell$. In particular, we have depth$(W_{t-1}) \geq 1$, which implies that $W_{t-1} \neq (0, 0, \cdots, 0) \in R^{N-t+1}$. This shows that given any set of keys provided by Player B, there is a strategy for Player A that does not allow Player B to win the game in less than t rounds.

This completes the proof of the theorem. □

Remark 7.4.2. In Game 1, we impose the constraint that Player B has to choose the initial word W_0 as a non-repeated word of R^N. This is because, if Player B in Game 1 chooses the initial word W_0 as a non-zero repeated-word in R^N, then by providing the key $\mathbf{K}_0 = -[W_0]_{N-1}$ in Game 1, Player B will win the game immediately after the first round. Hence Game 1 would be trivial when Player B is allowed to choose the initial word W_0 as a non-zero repeated word of R^N.

7.4.2 Game 2

Consider the following game for two players, Player A (the adversary) and Player B, who are standing by a round table. Suppose that the top of the round table is made up of N concentric rings, which are labelled as $R_1, R_2, \cdots, R_N$, as we move from the centre

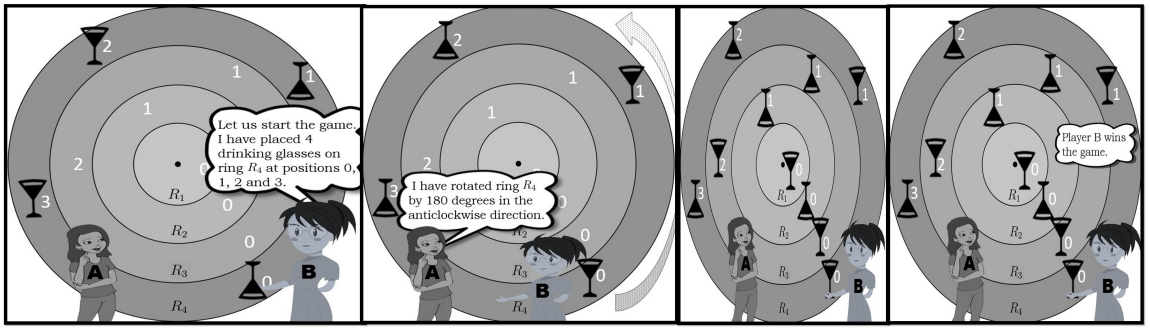

FIGURE 7.6: Example IV

of the round table towards the outermost ring. Further, suppose that the ring R_N (i.e., the outermost ring) can rotate freely by an angle of $\frac{360^\circ}{N} \times u$ in the anticlockwise direction, where $0 \leq u \leq N-1$ is an integer. For $1 \leq i \leq N$, let us mark i equidistant positions on ring R_i and label these positions as $0, 1, 2, \cdots, i-1$ in the anticlockwise direction. The game starts when Player B places N drinking glasses at each of the N equispaced positions marked on ring R_N, either in the upright position or in the upside down position, such that not all glasses have the same orientation. Thereafter, for $i = N-1, N-2, \cdots, 1$ respectively, Player A has to place i drinking glasses at each of the i equispaced positions, *viz.* $0, 1, 2, \cdots, i-1$, marked on ring R_i with a certain manipulation and by applying the following recursive rule:

For $0 \leq j \leq i-1$, a glass has to be placed at position j on ring R_i in

- the upright position if both the glasses placed at positions j and $j+1$ on ring R_{i+1} are either in the upright position or in the upside down position, (i.e., if the glasses placed at positions j and $j+1$ on ring R_{i+1} have the same orientation).
- the upside down position if one of the glasses placed at positions j and $j+1$ on ring R_{i+1} is in the upside down position and the other glass is in the upright position (i.e., if the glasses placed at positions j and $j+1$ on ring R_{i+1} have the opposite orientation).

Now Player A rotates the outermost ring (i.e. ring R_N) by an angle a multiple of $\frac{360^\circ}{N}$ in the anticlockwise direction, which leads to a cyclic permutation of the glasses placed on ring R_N. Now Player A places $N-1$ glasses on ring R_{N-1}, $N-2$ glasses on ring R_{N-2}, $\cdots$, 2 glasses on ring R_2 and 1 glass on ring R_1 (the innermost ring) by applying the above recursive rule. We say that Player B wins the game if all glasses are placed in the upright

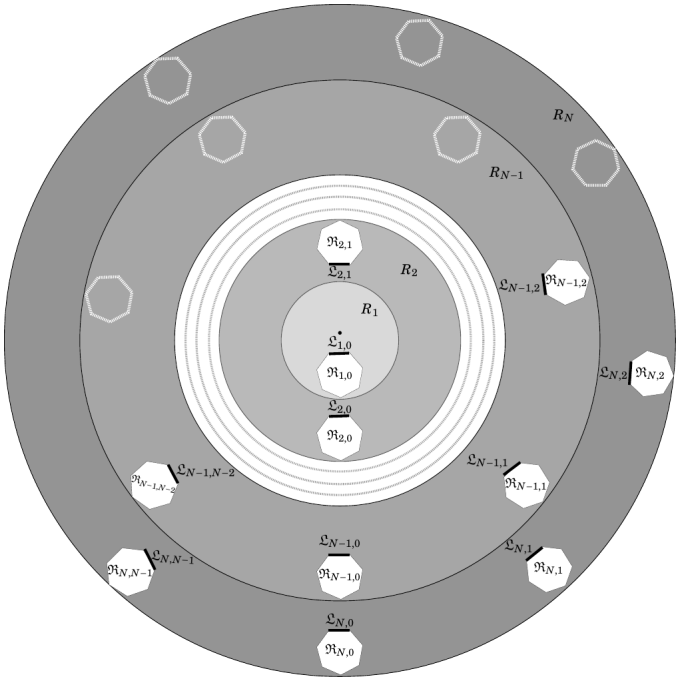

FIGURE 7.7: Illustration of Game 2

position on some ring of the tabletop. Otherwise, Player B loses the game. □

We illustrate this game in Figures 7.5 and 7.6. We further generalize this game for larger alphabet sizes as follows:

A generalization of Game 2 for larger alphabet sizes

In order to generalize this game for larger alphabet sizes, we suppose, throughout this section, that λ is a unit in R. Further, let us define the map $E_\lambda : R^N \to R^N$ as $E_\lambda(V) = (\lambda v_{N-1}, v_0, v_1, \cdots, v_{N-2})$ for each $V = (v_0, v_1, v_2, \cdots, v_{N-1}) \in R^N$. The map E_λ is called the λ-constacyclic shift operator on R^N.

Now consider the following game for two players, Player A (the adversary) and Player B, who are standing by a round table, whose top is made up of N concentric rings as shown in Figure 7.7. Suppose that these N concentric rings on the round table are labelled as $R_1, R_2, \cdots, R_N$, as we move from the centre of the round table towards the outer ring. Further, suppose that ring R_N (i.e., the outermost ring) can rotate freely by an angle of $\frac{360^\circ}{N} \times u$ in the anticlockwise direction, where $0 \leq u \leq N-1$ is an integer. For $1 \leq i \leq N$, let us mark i equidistant points on ring R_i, place i identical roulettes on each of these points

in such a way that each roulette has a side nearest to the centre and parallel to a diameter (i.e., a chord passing through the centre) of the round table and label these roulettes as $\mathfrak{R}_{i,0}, \mathfrak{R}_{i,1}, \cdots, \mathfrak{R}_{i,i-1}$ in the anticlockwise direction. For $1 \leq i \leq N$ and $0 \leq j \leq i-1$, suppose that the side of the roulette $\mathfrak{R}_{i,j}$ nearest to the centre and parallel to a diameter of the round table is labelled by the ring element $\mathfrak{L}_{i,j} \in R$. We also assume that if the side of the roulette $\mathfrak{R}_{N,j}$ nearest to the centre and parallel to a diameter of the round table is labelled by the element $a_j \in R$ for $0 \leq j \leq N-1$, then the rotation of the ring R_N by an angle of $\frac{360^\circ}{N} \times u$ gives rise to rotation of the roulettes placed on the ring R_N in such a way that

$$\begin{aligned}\big(\mathfrak{L}_{N,0}, \mathfrak{L}_{N,1}, \cdots, \mathfrak{L}_{N,N-1}\big) &= E_\lambda^u\big(a_0, a_1, \cdots, a_{N-1}\big) \\ &= (\lambda a_{N-u}, \lambda a_{N-u+1}, \cdots, \lambda a_{N-1}, a_0, a_1, \cdots, a_{N-u-1}),\end{aligned}$$

where u is an integer satisfying $0 \leq u \leq N-1$. Now we describe the game as follows:

I. The game starts when Player B chooses a non-zero word $W_0 = (a_0, a_1, \cdots, a_{N-1}) \in R^N$ when $\lambda \neq 1$, while Player B chooses a non-repeated word $W_0 = (a_0, a_1, \cdots, a_{N-1}) \in R^N$ when $\lambda = 1$. The word W_0 is called the initial word. Further, Player B fixes the orientation of the roulettes on ring R_N in such a way that $\mathfrak{L}_{N,j} = a_j \in R$ for $0 \leq j \leq N-1$. Now Player A chooses an integer u satisfying $0 \leq u \leq N-1$ and rotates ring R_N by an angle of $u \times \frac{360^\circ}{N}$, which gives rise to

$$\mathfrak{L}_{N,j} = \begin{cases} \lambda a_{N-u+j} & \text{if } 0 \leq j \leq u-1; \\ a_{N-u+j} & \text{if } u \leq j \leq N-1, \end{cases}$$

where the subscript $N-u+j$ is taken modulo N. Further, positions of the roulettes placed on rings $R_{N-1}, R_{N-2}, R_{N-3}, \cdots, R_2, R_1$ are fixed recursively by the following relation for $1 \leq j \leq N-1$:

$$\mathfrak{L}_{N-j,i} = \mathfrak{L}_{N-j+1,i+1} - \mathfrak{L}_{N-j+1,i} \quad \text{for} \quad 0 \leq i \leq N-j-1.$$

II. Player B wins the game if there exists an integer i satisfying $1 \leq i \leq N-1$ and $\mathfrak{L}_{i,j} = 0$ for $0 \leq j \leq i-1$. Otherwise, Player B loses the game. □

In order to further study this game, we now describe a mathematical version of Game 2.

Mathematical version of Game 2

I. The game starts when Player B chooses a non-zero word $W_0 = (a_0, a_1, \cdots, a_{N-1}) \in R^N$ when $\lambda \neq 1$, while Player B chooses a non-repeated word $W_0 = (a_0, a_1, \cdots, a_{N-1}) \in R^N$ when $\lambda = 1$. The word $W_0 \in R^N$ is called the initial word. Further, Player B fixes the orientation of the roulettes placed on ring R_N in such a way that $\mathfrak{L}_{N,j} = a_j$ for $0 \leq j \leq N-1$. Now Player A (the adversary) chooses an integer u satisfying $0 \leq u \leq N-1$ and rotates the ring R_N by an angle of $\frac{360^\circ}{N} \times u$, which gives rise to rotation of the roulettes placed on ring R_N in such a way that

$$\mathfrak{L}_{N,j} = \begin{cases} \lambda a_{N-u+j} & \text{if } 0 \leq j \leq u-1; \\ a_{N-u+j} & \text{if } u \leq j \leq N-1, \end{cases}$$

where the subscript $N-u+j$ is taken modulo N. That is, Player A creates the word $U_0 = E_\lambda^u(W_0)$ and rotates the ring R_N by an angle of $\frac{360^\circ}{N} \times u$, which gives rise to rotation of the N roulettes on this outermost ring (i.e., ring R_N) in such a way that

$$\left(\mathfrak{L}_{N,0}, \mathfrak{L}_{N,1}, \cdots, \mathfrak{L}_{N,N-1}\right) = U_0 = E_\lambda^u(W_0).$$

Further, Player A creates the words $U_1 \in R^{N-1}, U_2 \in R^{N-2}, \cdots, U_{N-1} \in R$ by recursively applying the following relation for $\ell = 1, 2, \cdots, N-1$ respectively:

$$U_\ell = [E(U_{\ell-1}) - U_{\ell-1}]_{N-\ell} = D(U_{\ell-1}) = D^\ell(U_0),$$

and rotates the roulettes placed on ring $R_{N-\ell}$ in such a way that

$$\left(\mathfrak{L}_{N-\ell,0}, \mathfrak{L}_{N-\ell,1}, \cdots, \mathfrak{L}_{N-\ell,N-\ell-1}\right) = U_\ell = D^\ell(U_0)$$

for $1 \leq \ell \leq N-1$.

II. Player B wins the game if there exists an integer ℓ satisfying $1 \leq \ell \leq N-1$ and $U_\ell = (0, 0, \cdots, 0) \in R^{N-\ell}$ (or equivalently, if there exists an integer ℓ such that $1 \leq \ell \leq N-1$ and all the roulettes placed on ring $R_{N-\ell}$ are positioned in such a way

that $\mathfrak{L}_{N-\ell,j} = 0$ for $0 \leq j \leq N-\ell-1$). Otherwise, Player B loses the game. □

In the following theorem, we derive a necessary and sufficient condition for Player B to have a winning strategy in Game 2.

Theorem 7.4.4. In Game 2, Player B has a winning strategy if and only if Player B chooses an initial word $W_0 \in R^N$ satisfying $\text{depth}(E_\lambda^u(W_0)) \leq N-1$ for $0 \leq u \leq N-1$.

Proof. One can easily observe that Player B wins the game if and only if Player B chooses the initial word $W_0 \in R^N$ such that W_0 and all its λ-constacyclic shifts have depths at most $N-1$. From this, the desired result follows immediately. □

Remark 7.4.3. When $\lambda = 1$, we impose the constraint that Player B has to choose the initial word W_0 as a non-repeated word of R^N. For, if Player B chooses the initial word W_0 as a non-zero repeated word of R^N, then the word W_0 and all its λ-constacyclic (i.e., cyclic) shifts have depth 1, and hence all the roulettes placed on rings $R_{N-1}, R_{N-2}, \cdots, R_2, R_1$ will have the desired orientation. Therefore, when $\lambda = 1$, Game 2 would be trivial and non-interesting if we allow Player B to choose the initial word W_0 as a non-zero repeated word of R^N.

Remark 7.4.4.

(a) One may slightly modify Games 1 and 2, and associate some monetary gain with the winning of Player B. For instance, if Player B wins after the i-th round (resp. ring R_i) in Game 1 (resp. Game 2) for some integer $1 \leq i \leq N-1$, then one may say that Player B wins the game with $1+2+\cdots+(N-i) = \frac{(N-i)(N-i+1)}{2}$ points (resp. $1+2+\cdots+i = \frac{i(i+1)}{2}$ points), and a monetary gain may be associated with the win accordingly. In such a scenario, Player B intends to win the game as early as possible for a high monetary gain.

(b) In Game 1, Player B has a positional winning strategy if and only if Player B chooses the initial word W_0 as a non-repeated word of R^N with depth at most $N-1$ (Theorems 7.4.1 and 7.4.2). Further, the positional winning strategy ($\star$), provided in the proof of Theorem 7.4.2, is an optimal winning strategy for Player B in the sense that if Player B chooses a non-repeated initial word $W_0 \in R^N$ of depth $t < N$, then Player B will win the game in at most t rounds and there is no other winning strategy for Player B that ensures the win in less than t rounds (Theorem 7.4.3). So Player B intends

to choose the initial word W_0 as a non-repeated word of R^N with a smaller depth to win the game as early as possible. By applying Theorems 7.3.1 and 7.3.3, one can determine several choices for the word $W_0 \in \mathcal{R}^{p^s}$ of a given depth $t \leq p^s$. These two theorems also establish the feasibility of the winning strategy proposed for Player B in Game 1, and also provide methods to determine several choices for the initial word $W_0 \in \mathcal{R}^{p^s}$ that ensures the win for Player B in Game 1 after a certain round.

(c) In Game 2, Player B has a winning strategy if and only if Player B chooses the initial word $W_0 \in R^N$ such that the word W_0 and all its λ-constacyclic shifts have depths at most $N-1$ (Theorem 7.4.4). Note that a word and its constacyclic shift may not have the same depth. By Corollary 7.3.1, we see that for $1 \leq u \leq p^s - 1$, each codeword $C(x)$ of the $(1+\gamma\beta)$-constacyclic code $\mathcal{C}_{e-1,u} = \langle \gamma^{e-1}(x-1)^u \rangle$ of length p^s over $\mathcal{R}$ satisfies the property that the codeword $C(x)$ and all its $(1+\gamma\beta)$-constacyclic shifts have depths at most $p^s - 1$. This establishes the feasibility of Game 2 when $N = p^s$, $R = \mathcal{R}$ and $\lambda = 1 + \gamma\beta$, and also provides several non-trivial choices for the initial word $W_0 \in \mathcal{R}^{p^s}$ satisfying the property that the word W_0 and all its $(1+\gamma\beta)$-constacyclic shifts have depths at most $p^s - 1$. That is, Player B will win Game 2 by choosing any codeword of $(1+\gamma\beta)$-constacyclic codes $\mathcal{C}_{e-1,1}, \mathcal{C}_{e-1,2}, \cdots, \mathcal{C}_{e-1,p^s-1}$ of length p^s over $\mathcal{R}$ as the initial word $W_0 \in \mathcal{R}^{p^s}$. This shows that there are several choices for the initial word $W_0 \in \mathcal{R}^{p^s}$ that ensures the win for Player B in Game 2 when $N = p^s$, $R = \mathcal{R}$ and $\lambda = 1 + \gamma\beta$ with β a unit in $\mathcal{R}$.

Chapter 8

Conclusion and future work

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. The Singleton bound is an upper bound on the size of the code in terms of the cardinality of the code alphabet, length of the code, and distance of the code. The codes that attain the Singleton bound have the highest possible value of distance for given code length, code size and alphabet size, and hence are called maximum distance separable (MDS) codes. MDS codes are optimal codes in the sense that these codes have the highest possible error-detecting and error-correcting capabilities for given code length, code size and alphabet size. Thus it is of great interest to study and find MDS codes with respect to various metrics. In this thesis, several MDS codes are obtained within the family of constacyclic codes over finite commutative chain rings with respect to Hamming, RT, symbol-pair and b-symbol metrics.

8.1 Conclusion

Below we summarize some of the main results derived in the thesis.

- All repeated-root constacyclic codes of arbitrary lengths over the Galois ring GR(p^2, m) are determined, where p is a prime and m is a positive integer. Their sizes and their dual codes are also explicitly determined. As an application, some isodual constacyclic codes over GR(p^2, m) are identified.

- All repeated-root constacyclic codes of arbitrary lengths over the chain ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ are explicitly determined, where p is a prime, m is a positive integer and $\mathbb{F}_{p^m}$ is the finite field of order p^m. Their sizes and their dual codes are determined. Some isodual codes are also identified within this class of constacyclic codes. Besides this, Hamming distances, RT distances and RT weight distributions are obtained for several constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. By applying these results, several MDS Hamming and MDS RT codes are identified within this class of codes.

- Algebraic structures of all repeated-root constacyclic codes of prime power lengths over an arbitrary finite commutative chain ring $\mathcal{R}$ are established. Their sizes, symbol-pair distances, RT distances, and RT weight distributions are explicitly determined. Necessary and sufficient conditions are derived for a repeated-root constacyclic code of prime power length over $\mathcal{R}$ to be (i) an MDS Hamming code (ii) an MDS symbol-pair code and (iii) an MDS RT code. All MDS Hamming, MDS symbol-pair and MDS RT codes belonging to this special class of constacyclic codes are listed. An algorithm to decode repeated-root constacyclic codes of prime power lengths over $\mathcal{R}$ is also presented with respect to Hamming, symbol-pair and RT metrics.

- b-Symbol distances of all repeated-root constacyclic codes of prime power lengths over finite fields are explicitly determined. Using this result, all MDS b-symbol codes belonging to this class of constacyclic codes are identified. It is also shown that the b-symbol distance of a linear code of an arbitrary length over $\mathcal{R}$ is equal to the b-symbol distance of its $(e-1)$th Torsion code. A necessary and sufficient condition for a linear code of an arbitrary length over $\mathcal{R}$ to be an MDS b-symbol code is also derived. Applying these results, b-symbol distances of all repeated-root constacyclic codes of prime power lengths over $\mathcal{R}$ are explicitly determined, and all MDS b-symbol codes belonging to this particular class of constacyclic codes over $\mathcal{R}$ are listed.

- Depths of codewords of all repeated-root $(\alpha+\gamma\beta)$-constacyclic codes of prime power lengths over a finite commutative chain ring $\mathcal{R}$ are studied, where α is a non-zero element of the Teichmüller set of $\mathcal{R}$, γ is a generator of the maximal ideal of $\mathcal{R}$ and β is a unit in $\mathcal{R}$. As a consequence, depth distributions of all repeated-root $(\alpha+\gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$ are explicitly determined.

- Two new turn-based two player roulette games are proposed and positional winning strategies for these games are discussed in terms of depths of words over a finite commutative ring with unity R. It is also shown that the winning strategy provided for Game 1 is optimal. The feasibility of these winning strategies is also discussed by applying our results on depths of codewords of repeated-root $(\alpha + \gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$.

8.2 Future work

Some of the interesting open problems in this research direction are listed below:

- It would be interesting to determine b-symbol distances of constacyclic codes of non prime power lengths over $\mathcal{R}$, and to identify MDS b-symbol codes within this class of constacyclic codes. It would also be interesting to obtain homogeneous distances of constacyclic codes over finite commutative chain rings. Another interesting problem is to provide algorithms to decode constacyclic codes over finite commutative chain rings with respect to b-symbol and homogeneous metrics.

- It would also be an interesting problem to determine dual codes of constacyclic codes over $\mathcal{R}$ and to study their duality properties.

- It would be interesting to determine depth distributions of $(\alpha+\gamma\beta)$-constacyclic codes of prime power lengths over $\mathcal{R}$ when β is a non-unit in $\mathcal{R}$, and to further determine depth distributions of constacyclic codes of non-prime power lengths over $\mathcal{R}$.

- It would be interesting to study the feasibility of winning strategies proposed for Player B in Games 1 and 2 when R is a finite commutative ring with unity (not necessarily a chain ring) and $N \geq 2$ is an arbitrary integer (not necessarily a prime power).

- Another interesting problem would be to study natural generalizations of Game 1 in which Player A (the adversary) removes any roulette among the $N - \ell + 1$ roulettes on the table (i.e., when Player A chooses the integer $s_{\ell-1} \in \{0, 1, 2, \cdots, N - \ell\}$) during the ℓ-th round for $1 \leq \ell \leq N - 1$.

Bibliography

[1] T. Abualrub and R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, *IEEE Trans. Inform. Theory* 49(9), pp. 2126-2133, Sept. 2003.

[2] M. M. Al-Ashker, Simplex codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, *Arab. J. Sci. Eng. Sect. A Sci.* 30(2), pp. 277-285, Jul. 2005.

[3] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa and M. Oura, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to Hermitian modular forms, *Abh. Math. Semin. Univ. Hambg.* 73(1), pp. 13-42, Dec. 2003.

[4] A. Batoul, K. Guenda and T. A. Gulliver, Some constacyclic codes over finite chain rings, *Adv. Math. Commun.* 10(4), pp. 683-694, Nov. 2016.

[5] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill Book Company, New York: 1968.

[6] S. R. Blackburn, T. Etzion and K. G. Paterson, Permutation polynomials, de Bruijin sequences and linear complexity, *J. Comb. Theory* 76(1), pp. 55-82, Oct. 1996.

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

[8] A. R. Calderbank, A. R. Hammons Jr., P. V. Kumar, N. J. A. Sloane and P. Sol$\acute{e}$, A linear construction for certain Kerdock and Preparata codes, *Bull. Amer. Math. Soc.* 29(2), pp. 218-222, Oct. 1993.

[9] Y. Cao, On constacyclic codes over finite chain rings, *Finite Fields Appl.* 24, pp. 124-135, Nov. 2013.

[10] 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.* 12(2), pp. 231-262, May 2018.

[11] Y. Cao, Y. Cao, H. Q. Dinh, F-W. Fu, Y. Gao, S. Sriboonchitta, Type 2 constacyclic codes over $\mathbb{F}_{2^m}/\langle u^3\rangle$ of oddly even length, *Discrete Math.* 342(2), pp. 412-426, Feb. 2019.

[12] Y. Cassuto and M. Blaum, Codes for symbol-pair read channels, *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 988-992.

[13] Y. Cassuto and M. Blaum, Codes for symbol-pair read channels, *IEEE Trans. Inf. Theory* 57(12), pp. 8011-8020, Dec. 2011.

[14] A. H. Chan, R. A. Games and E. L. Key, On the complexities of de Bruijin sequences, *J. Comb. Theory* 33(3), pp. 233-246, Nov. 1982.

[15] Y. M. Chee, L. Ji, H. M. Kiah, C. Wang and J. Yin, Maximum distance separable codes for symbol-pair read channels, *IEEE Trans. Inf. Theory* 59(11), pp. 7259-7267, Nov. 2013.

[16] B. Chen, H. Q. Dinh, H. Liu and L. Wang, Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$,, *Finite Fields Appl.* 37, pp. 108-130, Jan. 2016.

[17] B. Chen, L. Lin and H. Liu, Constacyclic symbol-pair codes: lower bounds and optimal constructions, *IEEE Trans. Inf. Theory* 63(12), pp. 7661-7666, Dec. 2017.

[18] T. Colcombet and D. Niwiski, On the positional determinacy of edge-labeled games, *Theor. Comput. Sci.* 352(1), pp. 190-196, Mar. 2006.

[19] G. Deng, On the depth spectrum of binary linear codes and their dual, *Discrete Math.* 340(4), pp. 591-595, Apr. 2017.

[20] H. Q. Dinh, Negacyclic codes of length 2^s over Galois rings, *IEEE Trans. Inf. Theory* 51(12), pp. 4252-4262, Dec. 2005.

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

[22] H. Dinh and S. R. L*ó*pez-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inf. Theory* 50(8), pp. 1728-1744, Aug. 2004.

[23] H. Q. Dinh, H. Liu, X. S. Liu and S. Sriboonchitta, On structure and distances of some classes of repeated-root constacyclic codes over Galois rings, *Finite Fields Appl.* 43, pp. 86-105, Jan. 2017.

[24] H. Q. Dinh, B. T. Nguyen, A. K. Singh and S. Sriboonchitta, On the symbol-pair distance of repeated-root constacyclic codes of prime power lengths, *IEEE Trans. Inf. Theory* 64(4), pp. 2417-2430, Apr. 2018.

[25] 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 Appl.* 43, pp. 22-41, Jan. 2017.

[26] H. Q. Dinh, L. Wang and S. Zhu, Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Finite Fields Appl.* 31, pp. 178-201, Jan. 2015.

[27] B. Ding, G. Ge, J. Zhang, T. Zhang and Y. Zhang, New constructions of MDS symbol-pair codes, *Des. Codes Cryptogr.* 86, pp. 841-859, Apr. 2018.

[28] B. Ding, T. Zhang and G. Ge, Maximum distance separable codes for b-symbol read channels, *Finite Fields Appl.* 49, pp. 180-197, Jan. 2018.

[29] S. T. Dougherty and K. Shiromoto, Maximum distance codes over rings of order 4, *IEEE Trans. Inf. Theory* 47(1), pp. 400-404, Jan. 2001.

[30] S. T. Dougherty and M. M. Skriganov, Maximum distance separable codes in the ρ metric over arbitrary alphabets *J. Algebraic Combinatorics*, 16, pp. 71-81, Jul. 2002.

[31] R. Ehrenborg and C. M. Skinner, The Blind Bartender's Problem, *J. Comb. Theory, Ser. A* 70(2), pp. 249-266, 1995.

[32] T. Etzion, The depth distribution - A new characterization for linear codes, *IEEE Trans. Inf. Theory* 43(4), pp. 1361-1363, Jul. 1997.

[33] R. A. Games and A. H. Chan, A fast algorithm for determining the complexity of binary sequences with period 2^n, *IEEE Trans. Inf. Theory* 29(1), pp. 144-166 Jan. 1983.

[34] M. Gardner, About rectangling rectangles, parodying Poe and many other pleasing problem, Mathematical Games, *Sci. Amer.* 240(2), pp. 16-24, Feb. 1979.

[35] M. Gardner, On altering the past, delaying the future and other ways of tampering with time, Mathematical Games, *Sci. Amer.* 240(3), pp. 21-30, Mar. 1979.

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

[37] M. Hirotomo, M. Takita and M. Morii, Syndrome decoding of symbol-pair codes, *Proc. IEEE Inf. Theory Workshop*, Nov. 2014, pp. 162-166.

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

[39] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, New York, 2003.

[40] J. Y. Hyun and H. K. Kim, Maximum distance separable poset codes, *Des. Codes Cryptogr.* vol. 48, pp. 247-261, Sep. 2008.

[41] X. Kai, L. Wang and S. Zhi, The depth spectrum of negacyclic codes over $\mathbb{Z}_4$, *Discrete Math.* 340(3), pp. 345-350, Mar. 2017.

[42] X. Kai, S. Zhu and P. Li, A construction of new MDS symbol-pair codes, *IEEE Trans. Inf. Theory* 61(11), pp. 5828-5834, Nov. 2015.

[43] X. Kai, S. Zhu and P. Li, New MDS symbol-pair codes from repeated-root codes, *IEEE Commun. Lett.* 22(3), pp. 462-465, Mar. 2018.

[44] H. M. Kiah, K. H. Leung and S. Ling, Cyclic codes over GR(p^2, m) of length p^k, *Finite Fields Appl.* 14(3), pp. 834-846, Jul. 2008.

[45] B. Kong, X. Zheng and H. Ma, The depth spectrums of constacyclic codes over finite chain rings, *Discrete Math.* 338(2), pp. 256-261, Feb. 2015.

[46] W. T. Laaser and L. Ramshaw, Probing the rotating table, *D. A Klarner (Ed.), The Mathematical Gardner,* Springer, Boston, MA, pp. 285-307, 1981.

[47] V. I. Levenshtein, Reconstruction of objects from a minimum number of distorted patterns, *Doklady Math.* 55(3), pp. 417-420, May 1997.

[48] V. I. Levenshtein, Efficient reconstruction of sequences, *IEEE Trans. Inf. Theory* 47(1), pp. 2-22, Jan. 2001.

[49] V. I. Levenshtein, Efficient reconstruction of sequences from their subsequences and their supersequences, *J. Combin. Theory Ser. A* 93(2), pp. 310-332, Feb. 2001.

[50] T. Lewis and S. Williard, The rotating table, *Math. Mag.* 53(3), pp. 174-179, 1980.

[51] S. Li and G. Ge, Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes, *Des. Codes Cryptogr.* 84, pp. 359-372, Sep. 2017.

[52] X. Li, Q. Yue, On the Hamming distances of repeated-root cyclic codes of length $5p^s$, arXiv:1911.07542 [cs.IT] 2019.

[53] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 2000.

[54] S. Ling and C. Xing, *Coding Theory: A first course*, Cambridge University Press, 2010.

[55] H. Liu and Y. Maouche, Some repeated-root constacyclic codes over Galois Rings, *IEEE Trans. Inf. Theory* 63(10), pp. 6247-6255, Oct. 2017.

[56] X. Liu and X. Xu, Cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Acta Math. Sci.* 34(3), pp. 829-839, May 2014.

[57] 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 Appl.* 19(3), pp. 16-38, Jan. 2013.

[58] Y. Luo, F. Fu, and V. K.-W. Wei, On the depth distribution of linear codes, *IEEE Trans. Inf. Theory* 46(6), pp. 2197-2203, Sep. 2000.

[59] V. Malvone, A. Murano and L. Sorrentino, Games with additional winning strategies, CILC'15 CEUR Workshop Proceedings, pp. 1-6, 2015.

[60] V. Malvone, A. Murano and L. Sorrentino, Additional winning strategies in reachability games, *Fundamenta Informaticae* 159, pp. 175-195, 2018.

[61] B. R. McDonald, *Finite rings with identity*, New York, USA: Marcel Dekker, 1974.

[62] C. J. Mitchell, On integer-valued rational polynomials and depth distributions of binary codes, *IEEE Trans. Inf. Theory* 44(7), pp. 3146-3150, Nov. 1998.

[63] H. Mostafanasab and E. S. Sevim, b-Symbol distance distribution of repeated-root constacylic codes, *Proc. Seminar on Algebra and its applications* Aug. 2016, pp. 1-7.

[64] A. A. Nechaev, Kerdock code in a cyclic form, *Discrete Math. Appl.* 1(4), pp. 365-384, 1991.

[65] A. A. Nechaev, *Finite rings with applications*, Handbook of Algebra 5, Elsevier/North-Holland, Amsterdam, pp. 213-320, 2008.

[66] G. H. Norton and A. Sălăgean, On the Hamming distance of linear codes over a finite chain ring, *IEEE Trans. Inf. Theory* 46(3), pp. 1060-1067, May 2000.

[67] G. H. Norton and A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, *Applicable Alg. Eng. Commun. Comput.* 10(6), pp. 489-506, Jul. 2000.

[68] M. Ozen and I. Siap, On the structure and decoding of linear codes with respect to RosenbloomTsfasman metric, *Selcuk J. Appl. Math.* 5(2), pp. 25-31, 2004.

[69] J. Quistorff, On Rosenbloom and Tsfasman's generalization of the Hamming space, *Discrete Math.* 307, pp. 2514-2524, Oct. 2007.

[70] M. Y. Rosenbloom and M.A. Tsfasman, Codes for the m-metric, *Problems Inform. Transmission* 33(1), pp. 45-52, 1997.

[71] A. Sharma , Repeated-root constacyclic codes of length $\ell^t p^s$ and their dual codes , Cryptogr. Commun. 7(2), pp. 229-255, 2015.

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

[73] T. Sidana, On depth spectra of constacyclic codes, (submitted).

[74] R. C. Singleton, Maximum distance q-ary codes, *IEEE Trans. Inform. Theory* 10(2), pp. 116-118, Apr. 1964.

[75] 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.* 34, pp. 123-138, Jul. 2015.

[76] R. Sobhani and M. Esmaeili, Cyclic and negacyclic codes over the Galois ring GR(p^2, m), *Discrete Math. Appl.* 157, pp. 2892-2903, Jul. 2009.

[77] Z. Sun, S. Zhu and L. Wang, The symbol-pair distance distribution of a class of repeated-root cyclic codes over $\mathbb{F}_{p^m}$, *Cryptogr. Commun.* 10(4), pp. 643-653, Jul. 2018.

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

[79] Z.-X. Wan, *Lectures on finite fields and Galois rings*, World Sci. Publ. Co. Inc., 2003.

[80] Y. Wu, Q. Yue, Factorizations of binomial polynomials and enumerations of LCD and self-dual constacyclic codes, *IEEE Trans. Inf. Theory* 65(3), pp. 1740-1751, Mar. 2019.

[81] E. Yaakobi, J. Bruck, and P. H. Siegel, Decoding of Cyclic codes over symbol-pair read channels, *Proc. IEEE Int. Symp. Inform. Theory*, pp. 2891-2895, 2012.

[82] E. Yaakobi, J. Bruck and P. H. Siegel, Constructions and decoding of cyclic codes over b-symbol read channels, *IEEE Trans. Inf. Theory* 62(4), pp. 1541-1551, Apr. 2016.

[83] R. B. Yehuda, T. Etzion and S. Moran, Rotating-table games and derivatives of words, *Theor. Comput. Sci.* 108(2), pp. 311-329, Feb. 1993.

[84] J. Yuan, S. Zhu, X. Kai, On depth spectra of repeated-root constacyclic codes over finite chain rings, *Discrete Math.* 343(2), 111647, Feb. 2020.

[85] M. Zeng, Y. Luo and G. Gong, Rotating-table game and construction of periodic sequences with lightweight calculation, *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1221-1225, 2012.

[86] 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.* 50, pp.1-16, Mar. 2018.

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