جامعة سيدي محمد بن عبد الله بفاس
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵙⵉⴷⵉ ⵎⵓⵃⴰⵎⵎⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ ⴰ ⴼⴰⵙ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

كلية العلوم ظهر المهراز فاس
ⵜⴰⵖⵡⵍⵎⵜ ⵏ ⵜⵣⵔⴼⵜ ⵎⴻⴷⴰⵖ ⵎⵣⵔⴰⵣ ⴼⴰⵙ
FACULTE DES SCIENCES DHAR EL MAHRAZ FES

N° d'Ordre : **/2021**

Formation Doctorale : Mathématiques et Applications (MA)

Discipline : Mathématiques

Spécialité : Algèbre

Laboratoire : Sciences mathématiques et applications

THESE DE DOCTORAT

Présentée par

LAAOUINE Jamal

Algebraic structures and distance distributions of repeated-root constacyclic codes over a class of finite commutative chain rings

Soutenue le 28 / 10 / 2021 devant le jury composé de :

Pr. Souad Wardi	***Faculté des Sciences Dhar El Mahraz - Fès***	***Présidente***
Pr. Malika Ait Ben Haddou	***Faculté des Sciences - Meknès***	***Rapporteur***
Pr. Abdelfattah Haily	***Faculté des Sciences - El Jadida***	***Rapporteur***
Pr. Mustapha Najmeddine	***ENSAM-Meknès***	***Rapporteur***
Pr. Siham Ezzouak	***Faculté des Sciences Dhar El Mahraz - Fès***	***Examinateur***
Pr. Ismail Akharraz	***Faculté des Sciences - Agadir***	**Examinateur**
Pr. Mohammed E. Charkani	***Faculté des Sciences Dhar El Mahraz - Fès***	**Directeur de thèse**
Pr. Hai Q. Dinh	***Kent State University - USA***	**Invité**
Pr. Abdulaziz Deajim	***King Khalid University, Abha - Saudi Arabia***	**Invité**

Année universitaire : 2020-2021

Université Sidi Mohamed Ben Abdellah

Faculté des Sciences Dhar El Mahraz - Fès

THÈSE

Présentée par

Jamal Laaouine

Pour l'obtention du

Doctorat en Mathématiques

FD: Mathématiques et Applications (MA)

Spécialité: Algèbre

Intitulée:

Algebraic structures and distance distributions of repeated-root constacyclic codes over a class of finite commutative chain rings

Soutenue le jeudi **28 octobre 2021** devant le jury composé de:		
Pr. Souad Wardi	Faculté des Sciences Dhar-El-Mahraz de Fès	Présidente
Pr. Mohammed Elhassani Charkani	Faculté des Sciences Dhar-El-Mahraz de Fès	Directeur
Pr. Malika Ait Ben Haddou	Faculté des Sciences de Meknès	Rapporteur
Pr. Abdelfattah Haily	Faculté des Sciences d' El Jadida	Rapporteur
Pr. Mustapha Najmeddine	Ecole Nationale Supérieure d'Arts et Métiers de Meknès	Rapporteur
Pr. Hai Q. Dinh	Kent State University, USA	Rapporteur
Pr. Siham Ezzouak	Faculté des Sciences Dhar-El-Mahraz de Fès	Examinateur
Pr. Ismail Akharraz	Faculté des Sciences d'Agadir	Examinateur
Pr. Abdulaziz Deajim	Université King Khaled d' Abha - Arabie Saoudite	Invité

À l'âme de mon père . . . God rest his soul

Dedicated to my Family . . . Especially

My Parents: Fatma Sibouss bint Ali et Mimouna

Mohammed Laaouine ben Lahcen et Meryem

My Wife: Nour-El Houda Kerrich beint Mohammed et Khadija

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. **Mohammed Elhassani Charkani**, who offered his appreciation, encouragement, continuous advice, good teaching, and lot of good ideas throughout my Ph.D. He has provided insightful discussions about the research. I thank him for the systematic guidance and great effort. His patience and kindness, his academic experience, as well as his relentless pursuit of good mathematics, have been invaluable to me.

I would like to express my sincere gratitude to **Malika Ait Ben Haddou**, **Abdelfattah Haily** and **Mustapha Najmeddine** for the time they have given to the reading and judgment of this thesis as well as to the preparation of their reports. It is with joy that I thank them for having accepted this charge. I am deeply grateful to **Hai Q. Dinh**, **Siham Ezzouak**, **Ismail Akharraz** and **Abdulaziz Deajim** for agreeing to read the manuscript and to participate in the defense of this thesis. I would like to express my sincere gratitude to **Souad Wardi** for accepted to participate in the defense of my thesis as president.

Finally, I must express my very profound gratitude to my **friends**, my **family**, especially my **parents** for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them.

Abstract

Algebraic coding theory deals with the design of error-correcting and error-detecting codes for the reliable transmission of information across noisy channel. Maximum distance separable (MDS) codes have the highest possible error-correcting capability among codes of given length and size. Thus it is of great interest to study and find MDS codes with respect to various distances (e.g. Hamming distance, symbol-pair distance, etc.).

Constacyclic codes over finite chain rings are an important class of codes from both a theoretical and practical viewpoint. The case when the code length n is divisible by the characteristic p of the residue field of a finite chain ring yields the so-called repeated-root codes. The classification of codes plays an important role in studying their structures. However, only some codes of special lengths over certain finite chain rings are classified. Let p be a prime number, s, m be positive integers, $\mathbb{F}_{p^m}$ be the finite field of order p^m, and let $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3 \rangle$ be the finite commutative chain ring with unity.

In this thesis, we study algebraic structures of repeated-root γ-constacyclic codes of length p^s over $\mathcal{R}$, that is, ideals of the ring $\mathcal{R}[x]/\langle x^{p^s} - \gamma \rangle$, where γ is a nonzero element of the field $\mathbb{F}_{p^m}$. First, we classify all γ-constacyclic codes of length p^s over $\mathcal{R}$ into 8 distinct types and obtain the number of codewords in each of those constacyclic codes. Furthermore, using their algebraic structures, the Hamming and symbol-pair distance distributions of all such codes are completely determined. As an application of these results, we identify all MDS Hamming and MDS symbol-pair codes within this class of constacyclic codes.

Keywords: Finite chain rings, constacyclic codes, repeated-root codes, Hamming distance, symbol-pair distance, MDS codes

Résumé

La théorie du codage est l'étude des méthodes permettant le transfert de l'information de façon efficace et précise. Les codes constacycliques sont une famille importante des codes linéaires. La particularité de ces codes est que leur étude se ramène à la recherche des idéaux d'un certain type d'anneaux. En effet, construire des codes constacycliques de longueur n sur un anneau fini R reviendrait à trouver les idéaux de l'anneau $\mathcal{R}[x]/\langle x^n-\lambda\rangle$, où λ est un élément inversible de R.

De plus la nature des idéaux trouvés jouent un rôle déterminant dans l'étude de certaines propriétés du code telles que la distance minimale. Cette distance minimale possède une borne, appelée borne de Singleton, qui dépend de la longueur et de la dimension du code. Les codes dont la distance minimale atteint cette borne, appelés des codes MDS, pour Maximum Distance Separable, possèdent une capacité de correction optimale. Soient p un nombre premier, s et m deux entiers positifs. Soit $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$ un anneau à chaîne fini, de corps résiduel le corps fini à p^m éléments noté $\mathbb{F}_{p^m}$.

Dans cette thèse, nous nous sommes intéressés à l'étude des codes γ-constacycliques à racines multiples de longueur p^s sur $\mathcal{R}$, autrement dit, l'étude porte sur les idéaux de $\mathcal{R}[x]/\langle x^{p^s}-\gamma\rangle$, où γ est un élément inversible de $\mathbb{F}_{p^m}$. Tout d'abord, nous classifions tous les codes γ-constacycliques de longueur p^s sur $\mathcal{R}$ en 8 types distincts et nous obtenons le nombre de mots du code dans chacun de ces codes constacycliques. De plus, en utilisant leurs structures algébriques, les distances de Hamming et paire de symboles de tous ces codes sont complètement déterminées. En application, nous identifions tous les codes MDS et de paire de symboles MDS au sein de cette classe de codes constacycliques.

Mots clés: Anneaux à chaîne finis, codes constacycliques, codes à racines multiples, distance de Hamming, distance de paire de symboles, codes MDS

Contents

Acknowledgements i

Abstract ii

Résumé iii

Contents iv

List of Notations vi

List of Publications vii

1 Introduction 1

2 Preliminary concepts 5

2.1 Finite commutative chain ring 5

2.2 Constacyclic codes over finite commutative rings with unity 7

2.3 Hamming and symbol-pair distances 9

2.3.1 Hamming distance 9

2.3.2 Symbol-pair distance 10

2.4 Constacyclic codes over $\mathbb{F}_{p^m}$ 11

2.4.1 Structure of constacyclic codes 11

2.4.2 Hamming distance 13

2.4.3 Symbol-pair distance 14

3 Repeated-root γ-constacyclic codes over the chain ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ 15

3.1 Introduction 15

3.2 Algebraic structures of repeated-root γ-constacyclic codes of length p^s over $\mathcal{R}$ 16

3.3 Some examples 35

4 Hamming distance distributions of repeated-root γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ 39

4.1 Introduction 39

4.2 Hamming distance 40

4.3 MDS codes with respect to Hamming distance 46

4.4 Some examples 56

5 Symbol-pair distance distributions of repeated-root γ-constacyclic codes of prime power lengths over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ 60

5.1 Introduction 60

5.2 Symbol-pair distance 61

5.3 Determination of MDS symbol-pair codes 71

5.4 Some examples 93

6 Conclusion and future work 97

6.1 Conclusion 97

6.2 Future work 98

Bibliography 99

List of Notations

Symbol	Meaning
$\mathbb{F}_q$	The Finite field of order q
$\mathbb{Z}_n$	The ring of integers modulo n
$\|A\|$	The cardinality of the set A
$GR(p^k, m)$	The Galois ring of characteristic p^k and cardinality p^{km}
wt_H	The Hamming weight
wt_{sp}	The symbol-pair weight
d_H	The Hamming distance
d_{sp}	The symbol-pair distance

List of Publications

1) J. Laaouine, M. E. Charkani and L. Wang, Complete classification of repeated-root σ-constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, Discrete Mathematics, vol. 344, no 6, pp. 112325, 2021.

2) J. Laaouine and M. E. Charkani, A note on "H. Q. Dinh et al., Hamming distance of repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$", Applicable Algebra in Engineering, Communication and Computing, pp. 1–7, 2021.

3) J. Laaouine, On the Hamming and Symbol-Pair Distance of Constacyclic Codes of Length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. In: International Conference on Advanced Communication Systems and Information Security. Springer, Cham, pp. 137–154, 2019.

4) J. Laaouine, On MDS symbol-pair γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^2\rangle$, International Journal of Computer Science and Applications, accepted for publication, 2020.

5) H. Q. Dinh, J. Laaouine, M. E. Charkani and S. Chinnakum, Hamming distance of constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$, IEEE Access, 2021.

6) M. E. Charkani, H. Q. Dinh, J. Laaouine and W. Yamaka, Symbol-Pair Distance of Repeated-Root Constacyclic Codes of Prime Power Lengths over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, Mathematics, 2021.

7) B. Boudine, J. Laaouine and M. E. Charkani, New quantum codes from cyclic codes over finite chain ring of length 3. Asian-European Journal of Mathematics, p. 2150175, 2021.

Chapter 1

Introduction

In the early history of coding theory, codes over finite fields were studied. Codes over finite rings have been intensively studied since 1990s due to their new role in coding theory and their successful applications. A commutative ring with identity is called a chain ring if all its ideals form a chain under inclusion. Calderbank et al. [10], Hammons et al. [31] and Nechaev [45] 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. Theoretically, constacyclic codes are the pivotal and profound part of linear codes. Constacyclic codes are generalization of cyclic codes, which form the most important and well studied class of error-correcting codes. Due to their encoding with shift registers, these codes have numerous practical applications. In recent years, there has been a great interest in study about the algebraic structure of constacyclic codes and apply to construct good codes.

Let λ be a unit of a finite commutative chain ring R. A λ-constacyclic code of length n over R can be classified as an ideal in $R[x]/\langle x^n - \lambda\rangle$. Thus the study of λ-constacyclic codes of length n over R is equivalent to the study of ideals of the ring $R[x]/\langle x^n - \lambda\rangle$. Particularly, in the case $\lambda = 1$, those λ-constacyclic codes are called cyclic codes, and when $\lambda = -1$, such λ-constacyclic codes are called negacyclic codes. When the code length n is divisible by the characteristic p of the residue field of R, the constacyclic codes are called repeated-root constacyclic codes. Otherwise, the constacyclic codes are called single-root constacyclic 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.

The structure of constacyclic codes of length n, gcd(n, p) = 1, over finite chain rings are well-known [19, 34]. However, when p divides n, the situation is quite different and classification of the corresponding codes is still incomplete. From 2003 on, special classes of repeated-root codes over certain classes of finite chain rings have been studied by numerous authors (see, for example, [1, 7, 11, 21, 47, 49]). Kiah et al. [36] determined all repeated-root cyclic codes of length p^s over Galois rings $GR(p^2, m)$ (a special finite chain ring). In a related work, Batoul et al. [6] determined the conditions that a constacyclic code is equivalent to a cyclic code.

Another type of finite chain rings is the class of finite chain rings $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$. This class of rings has been of interest because of a successful application in connections between modular lattices and linear codes over $\mathbb{F}_p + u\mathbb{F}_p$ [4]. For example, the structure of $\mathbb{F}_2 + u\mathbb{F}_2$ is interesting, because it is lying between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$ and multiplicatively analogous to $\mathbb{Z}_4$. Linear codes over $\mathbb{F}_2+u\mathbb{F}_2$ have been studied by a lot of researchers (see, for example, [2, 5, 8, 32, 48, 55]). The classification of codes plays an important role in studying their structures, but in general, it is very difficult. All constacyclic codes of length 2^s over the Galois extension rings of $\mathbb{F}_2+u\mathbb{F}_2$ are classified and their detailed structures are also established in [23]. Then in 2010, Dinh [18] classified all constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^2\rangle$. In a related work, Sobhani et al. [52] determined all $(\gamma + \alpha u^2)$-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ and their dual codes, where γ and α are nonzero elements in $\mathbb{F}_{p^m}$. Recently, Sharma and Sidana [50] studied repeated-root constacyclic codes of arbitrary lengths over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. From this point of view, describing the structure of γ-constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ might be of interest.

In **Chapter 3**, we investigate repeated-root γ-constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$, that is, ideals of the ring $\mathcal{R}_\gamma = \mathcal{R}[x]/\langle x^{p^s} - \gamma\rangle$, where γ is a nonzero element of the field $\mathbb{F}_{p^m}$. The algebraic structures of such codes are classified by categorizing the ideals of the local ring $\mathcal{R}_\gamma$ into 8 distinct types. The detailed structures of ideals in each type are provided. As an application, we obtain the number of codewords in each type of those constacyclic codes.

The metrics of constacyclic codes have very significant role in error-correcting coding theory. The most studied distance in coding theory is the Hamming distance, which is suitable for orthogonal modulated channels. Singleton [51] derived the upper bound (called the Singleton bound) on the size of an arbitrary block code with respect to the

Hamming distance. Linear codes that attain the Singleton bound are called maximum distance separable (MDS) Hamming codes. However, till now very little amount of works on computation of the Hamming distances have been done due to computational complexity. In [22] Dinh computed the Hamming distance of cyclic codes of p^s length over $\mathbb{F}_{p^m}$. Later, in [18], Dinh determined Hamming distances of all $(\alpha + u\beta)$-constacyclic codes of length of prime power over $\mathbb{F}_{p^m}[u]/\langle u^2\rangle$ using the results of [42]. In [26, 39], the Hamming distances of all γ-constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/\langle u^2\rangle$ are completely determined. Later, in [50], the Hamming distances of some repeated-root constacyclic codes of any length over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ are obtained. However, the complete Hamming distance distribution of all γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ was still left open. That motivates us to complete that task in this thesis.

In **Chapter 4**, using algebraic structures of γ-constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$, we explicitly determine their Hamming distances. As an application of these results, we identify all MDS Hamming codes within this class of constacyclic codes.

In [12, 13], Cassuto and Blaum 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 distance is called the symbol-pair distance. 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. Recently, 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 distance. In 2012, lower bound on the symbol-pair distances for binary cyclic codes are considered by Yaakobi et al. [56]. Later, Kai et al. [35] 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. [20] and Sun et al. [53] simultaneously determined symbol-pair distances of all repeated-root constacyclic codes of prime power lengths over finite fields. Later, in [26, 39], the symbol-pair distances of all repeated-root constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/\langle u^2\rangle$ are completely determined. In [27, 40], all MDS symbol-pair constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^2\rangle$ are obtained. Symbol-pair distances of γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$ have remained open, where $\gamma \in \mathbb{F}_{p^m}^*$. Motivated by that, we solved this problem in this thesis.

In **Chapter 5**, we obtain symbol-pair distances of all repeated-root γ-constacyclic codes of prime power lengths over $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3 \rangle$. Applying these results, we identify all MDS symbol-pair codes within this class of constacyclic codes.

In **Chapter 6**, we mention a brief conclusion and discuss some interesting open problems.

Chapter 2

Preliminary concepts

In this chapter we give some notations and recall some known definitions and results required for the following chapters.

2.1 Finite commutative chain ring

Rings are one of the fundamental objects of abstract algebra. They have numerous applications in number theory, cryptography, algebraic coding theory, and many other branches of mathematics.

All rings are commutative rings. An ideal I of a ring R is called principal if it is generated by a single element. A ring R is a principal ideal ring if all of its ideals are principal. R is called a local ring if R has a unique maximal ideal (consisting of all the non-units of R). Finally, a ring R is called a chain ring if all the ideals of R form a chain with respect to the inclusion relation. Typical examples of finite chain rings are the finite field $\mathbb{F}_{p^m}$ of order p^m, the integer residue ring $\mathbb{Z}_{p^k}$, the Galois ring $GR(p^k,m)$, i.e. the Galois extension of degree m of $\mathbb{Z}_{p^k}$ (cf. [33], [44]), where p is a prime and m, k are positive integers.

The following equivalence conditions are known for the class of finite commutative rings (see [19]).

Proposition 2.1 Let R be a finite ring, the following conditions are equivalent:

(i) R is a local ring and the maximal ideal of R is principal,

(ii) R is a local principal ideal ring,

(iii) R is a chain ring.

Let u be a fixed generator of the maximal ideal $\mathfrak{m}$ of a finite commutative chain ring R, i.e., $\mathfrak{m} = \langle u \rangle$. Then u is nilpotent and we denote its nilpotency index by e. The ideals of R form a chain:

$$\langle 0 \rangle = \langle u^e \rangle \subsetneq \langle u^{e-1} \rangle \subsetneq \cdots \subsetneq \langle u \rangle \subsetneq \langle u^0 \rangle = R.$$

Let $\overline{R} = R/\mathfrak{m}$ be the residue field of R modulo its maximal ideal $\mathfrak{m}$. By $^-: R[x] \to \overline{R}[x]$, we denote the natural ring homomorphism that maps $r \mapsto \bar{r} = r + \mathfrak{m}$ and the variable x to x. The following is a well known fact about finite commutative chain ring (cf. [44]).

Proposition 2.2 Let R be a finite commutative chain ring, with maximal ideal $\mathfrak{m} = \langle u \rangle$, and let e be the nilpotency u. Then

(a) For some prime p and positive integers k, m ($k \geq m$), $|R| = p^k$, $|\overline{R}| = p^m$, the characteristic of $\overline{R}$ is p, and the characteristic of R is a power of p. ($|A|$ denotes the cardinality of the set A).

(b) There is an element ζ of the multiplicative group of units of R with multiplicative order $p^m - 1$ such that any element $r \in R$ can be uniquely expressed as

$$r = r_0 + r_1 u + r_2 u^2 + \cdots + r_{e-1} u^{e-1},$$

where $r_i \in \mathcal{T}_e = \{0, 1, \zeta, \ldots, \zeta^{p^m-2}\}$ for $0 \leq i \leq e-1$. Moreover, r is a unit in R if and only if $r_0 \neq 0$.

The set $\mathcal{T}_e = \{0, 1, \zeta, \ldots, \zeta^{p^m-2}\}$ is called the Teichmüller set of R.

(c) For $i = 0, 1, \ldots, e$, $|\langle u^i \rangle| = |\overline{R}|^{e-i}$. In particular, $|R| = |\overline{R}|^e$, i.e., $k = me$.

The ring R is called a finite commutative chain ring with nilpotency index e. As $\overline{R}$ is a finite field, let us suppose that $\overline{R} \simeq \mathbb{F}_{p^m}$, where $\mathbb{F}_{p^m}$ is the finite field of order p^m. If R is of characteristic p, then $R \simeq \mathbb{F}_{p^m}[u]/\langle u^e \rangle$ (see [16], [54]).

The ring $\mathfrak{R} = \mathbb{F}_{p^m}[u]/\langle u^e \rangle$ is a local ring with maximal ideal $u\mathfrak{R} = \langle u \rangle_{\mathfrak{R}}$. That means, in light of Proposition 2.1, $\mathfrak{R}$ is a chain ring. $\mathfrak{R}$ can be viewed as $\mathfrak{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \ldots + u^{e-1}\mathbb{F}_{p^m}$, $u^e = 0$. It consists of all polynomials in $\mathbb{F}_{p^m}[u]$ of degree less than or equal to $e-1$ in indeterminate u. It is closed under p^m-ary polynomial addition and multiplication modulo u^e. The set $\mathfrak{R} \setminus \langle u \rangle_{\mathfrak{R}}$ is the set of all units of $\mathfrak{R}$, it consists of elements of the form

$$\lambda_0 + u\lambda_1 + u^2\lambda_2 + \cdots + u^{e-1}\lambda_{e-1},$$

where $\lambda_0, \lambda_1, \ldots, \lambda_{e-1} \in \mathbb{F}_{p^m}$ and $\lambda_0 \neq 0$.

More precisely, we get the following:

Proposition 2.3 ([24]) Let $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^e\rangle = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \ldots + u^{e-1}\mathbb{F}_{p^m}$. Then

(i) $\mathcal{R}$ is a chain ring with maximal ideal $\langle u\rangle_{\mathcal{R}}$, and residue field $\mathbb{F}_{p^m}$.

(ii) The ideals of $\mathcal{R}$ are $\langle u^i\rangle_{\mathcal{R}} = u^i\mathcal{R}$, $0 \le i \le e$, each ideal $\langle u^i\rangle_{\mathcal{R}}$ contains $p^{m(e-i)}$ elements.

(iii) $\mathcal{R}$ has $(p^m - 1)p^{m(e-1)}$ units, they are of the form

$$\lambda_0 + u\lambda_1 + u^2\lambda_2 + \cdots + u^{e-1}\lambda_{e-1},$$

where $\lambda_0, \lambda_1, \ldots, \lambda_{e-1} \in \mathbb{F}_{p^m}$ and $\lambda_0 \neq 0$.

2.2 Constacyclic codes over finite commutative rings with unity

The constacyclic codes play a very significant role in the theory of error-correcting codes as they are a direct generalization of the important family of cyclic codes. Codes over finite rings have been intensively studied since 1990s due to their new role in coding theory and their successful applications.

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. A code C of length n over R is a nonempty subset of R^n, and the ring R is referred to as the alphabet of the code. If this subset is also an R-submodule of R^n, then C is called linear. For a unit λ of R, the λ-constacyclic shift τ_λ on R^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \ldots, x_{n-2}).$$

A code C is said to be λ-constacyclic if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ. In the case that $\lambda = 1$, those λ-constacyclic codes are called cyclic codes, and when $\lambda = -1$, such λ-constacyclic codes are called negacyclic codes.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $R[x]/\langle x^n - \lambda\rangle$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$.

From that, the following fact is well known (cf. [33, 43]) and straightforward:

Proposition 2.4 *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of $R[x]/\langle x^n - \lambda\rangle$.*

In the light of this, the study of λ-constacyclic codes of length n over R is equivalent to the study of ideals of the quotient ring $R[x]/\langle x^n - \lambda\rangle$.

Definition 2.1 If $\mathfrak{a}, \mathfrak{b}$ are ideals of a ring A, then their ideal quotient is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

which is also an ideal. In particular, if $\mathfrak{b}$ is a principal ideal (π), we shall write $(\mathfrak{a} : \pi)$ in place of $(\mathfrak{a} : (\pi))$.

Proposition 2.5 ([3]) If $\mathfrak{a}, \mathfrak{b}$ and $\mathfrak{c}$ are ideals of a ring A. Then we have the followings:

(1) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

(2) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.

(3) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.

(4) $(\mathfrak{a} \cap \mathfrak{c} : \mathfrak{b}) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{c} : \mathfrak{b})$.

The following lemma will play an important role in studying the algebraic structures of constacyclic codes of length p^s over the ring $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$.

Lemma 2.1 *Let A and B be two commutative rings. Let $\varphi : A \longrightarrow B$ be a surjective ring homomorphism. Assume that B is a principal ideal ring and $\ker(\varphi)$ is a principal ideal $\langle\pi\rangle = \pi A$. Let I be an ideal of the ring A. Then there exists an $a \in I$ such that*

$$I = aA + \pi J,$$

where $J = (I : \pi) = \{r \in A : r\pi \in I\}$.

Proof Let $b \in B$ such that $\varphi(I) = Bb$. Let $a \in I$ such that $\varphi(a) = b$. If $x \in I$ then there exists an $w \in B$ such that $\varphi(x) = bw = \varphi(a)\varphi(v)$, where $v \in A$ and $\varphi(v) = w$. This implies that $y = x - av \in \ker(\varphi)$, which also implies that $x = av + y$ with $y \in \ker(\varphi) \cap I$. Hence, we get $I \subseteq Aa + \ker(\varphi) \cap I$, which means that $I = aA + \ker(\varphi) \cap I$. Since $\ker(\varphi) = \pi A$, we have $\ker(\varphi) \cap I = \pi J$, where $J = (I : \pi)$. Therefore, the desired result follows. □

The notion of dual codes is one of the most interesting topics in coding theory. For a linear code C over R, its dual code $C^{\perp}$ is defined as

$$C^{\perp} = \{a \in R^n : \ a \cdot c = 0, \text{ for all } c \in C\},$$

where $a \cdot c = a_0c_0 + a_1c_1 + \cdots + a_{n-1}c_{n-1}$, for $a = (a_0, a_1, \ldots, a_{n-1}) \in R^n$ and $c = (c_0, c_1, \ldots, c_{n-1}) \in C$. A code C is called self-orthogonal if $C \subseteq C^{\perp}$, and it is called self-dual if $C = C^{\perp}$.

The following result can be found in [18].

Proposition 2.6 The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.

The following proposition relates the number of codewords in a linear code of length n over R with that of its dual code.

Proposition 2.7 ([17]) Let p be a prime number and R be a finite chain ring of size p^{α}. The number of codewords in any linear code C of length n over R is p^k, for some integer $k \in \{0, 1, \ldots, \alpha n\}$. Moreover, the dual code $C^{\perp}$ has p^l codewords, where $k + l = \alpha n$, i.e., $|C| \cdot |C^{\perp}| = |R|^n$.

2.3 Hamming and symbol-pair distances

To study error-detecting and error-correcting properties of a code with respect to various communication channels, several distances (e.g. Hamming distance, symbol-pair distance, etc.) have been introduced and studied in coding theory. The most studied distance in coding theory is the Hamming distance, which is suitable for orthogonal modulated channels. 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.

2.3.1 Hamming distance

For a codeword $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in R^n$, the Hamming weight of $\mathbf{x}$, denoted by $wt_H(\mathbf{x})$, is the number of nonzero components of $\mathbf{x}$. The Hamming distance $d_H(\mathbf{x}, \mathbf{y})$ of two codewords $\mathbf{x}$ and $\mathbf{y}$ equals the number of components in which they differ, which is the Hamming weight $wt_H(\mathbf{x} - \mathbf{y})$ of $\mathbf{x} - \mathbf{y}$.

For a nonzero linear code C, the Hamming weight $wt_H(C)$ and the Hamming distance $d_H(C)$ are the same and defined as the smallest Hamming weight of nonzero codewords of C:

$$d_H(C) = \min\{wt_H(\mathbf{x}) \mid 0 \neq \mathbf{x} \in C\}.$$

The zero code is conventionally said to have Hamming distance 0.

Let C be a linear code of length n over R with Hamming distance $d_H(C)$. In [46], Norton et al. discussed the Singleton bound for R with respect to the Hamming distance $d_H(C)$ and is given as $|C| \leq |R|^{(n-d_H(C)+1)}$. Maximum Distance Separable (MDS) codes, which are classified as an important class of linear codes that meet the Singleton bound. They have high error correction capability as compared to non MDS codes. Then, C is said to be MDS code with respect to the Hamming distance if it attains the Singleton bound, i.e.,

$$|C| = |R|^{(n-d_H(C)+1)}. \tag{2.1}$$

2.3.2 Symbol-pair distance

In 2010, Cassuto and Blaum [12] introduced a new distance, called the symbol-pair distance, which is suitable for a channel whose outputs are overlapping pairs of symbols.

Let R be the code alphabet consisting of q elements. Then each element $c \in R$ is called a symbol. In symbol-pair read channels, a codeword $(c_0, c_1, \ldots, c_{n-1})$ is read as $((c_0, c_1), (c_1, c_2), \ldots, (c_{n-1}, c_0))$. A q-ary code of length n is a nonempty subset $C \subseteq R^n$. Suppose that $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ is a vector in R^n. The symbol-pair vector of $\mathbf{x}$ is defined as

$$\pi(\mathbf{x}) = ((x_0, x_1), (x_1, x_2), \ldots, (x_{n-1}, x_0)) \in (R^2)^n.$$

Hence, each vector has a unique symbol-pair vector $\pi(\mathbf{x}) \in (R, R)^n$. An important parameter of symbol-pair codes is the symbol-pair distance.

Now the natural question arises: Does there exist a relation between the symbol-pair distance of a code and its Hamming distance? Towards this, Cassuto and Blaum [12] derived such a relation and gave the definition of the symbol-pair distance as the Hamming distance over the alphabet (R, R).

Given $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$, the symbol-pair distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$d_{sp}(\mathbf{x}, \mathbf{y}) = d_H(\pi(\mathbf{x}), \pi(\mathbf{y})) = |\{i \in \mathbb{Z}_n \mid (x_i, x_{i+1}) \neq (y_i, y_{i+1})\}|,$$

where $\mathbb{Z}_n$ denotes the ring $\mathbb{Z}/n\mathbb{Z}$. The symbol-pair distance of a symbol-pair code C is defined as

$$d_{sp}(C) = \min\{d_{sp}(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

The symbol-pair weight of a vector $\mathbf{x}$ is defined as the Hamming weight of its symbol-pair vector $\pi(\mathbf{x})$:

$$wt_{sp}(\mathbf{x}) = wt_H(\pi(\mathbf{x})) = |\{i \in \mathbb{Z}_n \mid (x_i, x_{i+1}) \neq (0, 0)\}|.$$

If the code C is linear, its symbol-pair distance is equal to the minimum symbol-pair weight of nonzero codewords of C:

$$d_{sp}(C) = \min\{wt_{sp}(\mathbf{x}) \mid 0 \neq \mathbf{x} \in C\}.$$

MDS symbol-pair code has the largest minimum distance, i.e., they have the best possible error-correction capability. Hence, constructing MDS symbol-pair codes is significant in theory and practice. Singleton bound for symbol-pair code C of length n over R with symbol-pair distance $d_{sp}(C)$ is as follows: $|C| \leq |R|^{(n-d_{sp}(C)+2)}$ (see [15]). A symbol-pair code C is called an MDS symbol-pair code if it attains the singleton bound for symbol-pair codes, i.e.,

$$|C| = |R|^{(n-d_{sp}(C)+2)}. \tag{2.2}$$

2.4 Constacyclic codes over $\mathbb{F}_{p^m}$

Let p be a prime, s, m be positive integers. Let $\mathbb{F}_{p^m}$ be a finite field of order p^m. In this section, we consider all constacyclic codes of length p^s with alphabet $\mathbb{F}_{p^m}$.

2.4.1 Structure of constacyclic codes

As discussed in Section 2.2, for any invertible element γ of $\mathbb{F}_{p^m}$, γ-constacyclic codes of length p^s over a finite field $\mathbb{F}_{p^m}$ are precisely the ideals of the ring

$$\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma \rangle.$$

Since $\gamma \in \mathbb{F}_{p^m}$, we have $\gamma^{p^{tm}} = \gamma$ for any positive integer t. By applying the Division Algorithm, there exist nonnegative integers γ_q, γ_r such that $s = \gamma_q m + \gamma_r$ with $0 \leq \gamma_r \leq m-1$. Let $\gamma_0 = \gamma^{p^{(\gamma_q+1)m-s}} = \gamma^{p^{m-\gamma_r}}$. Then $\gamma_0^{p^s} = \gamma^{p^{(\gamma_q+1)m}} = \gamma$.

In 2008, Dinh [22] determined all γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ and their sizes, by showing that $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$ is a chain ring and by applying Proposition 2.1.

Theorem 2.1 (cf. [22, 3.1, 3.2, 3.3]) Let $\gamma = \gamma_0^{p^s} \in \mathbb{F}_{p^m}$, where $\gamma \neq 0$. Then we have the following:

(a) The polynomial $x - \gamma_0$ is nilpotent in $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$ with nilpotency index p^s.

(b) The ring $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$ is a finite commutative chain ring with the unique maximal ideal as $\langle x - \gamma_0\rangle$.

(c) All the distinct γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$ are precisely the ideals $\langle (x - \gamma_0)^i\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$, where $0 \leq i \leq p^s$, which forms the strictly inclusive chain

$$\langle 0\rangle = \langle (x - \gamma_0)^{p^s}\rangle \subsetneq \langle (x - \gamma_0)^{p^s-1}\rangle \subsetneq \cdots \subsetneq \langle x - \gamma_0\rangle \subsetneq \langle 1\rangle = \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle.$$

Moreover, for $0 \leq i \leq p^s$, the code $\langle (x - \gamma_0)^i\rangle$ has $p^{m(p^s-i)}$ codewords.

Now, consider the dual codes of γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}$. By Proposition 2.6, for a γ-constacyclic code $\mathcal{C}$ of length p^s over $\mathbb{F}_{p^m}$, $\mathcal{C} = \langle (x-\gamma_0)^i\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$, its dual $\mathcal{C}^\perp$ is a γ^{-1}-constacyclic code of length p^s over $\mathbb{F}_{p^m}$. That means $\mathcal{C}^\perp$ is an ideal of the chain ring $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma^{-1}\rangle$. However, in light of Proposition 2.7 and because $|\mathcal{C}| = p^{m(p^s-i)}$, then $|\mathcal{C}^\perp| = p^{mi}$. Hence, $\mathcal{C}^\perp = \langle (x - \gamma_0^{-1})^{p^s-i}\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma^{-1}\rangle$. Thus, we summarize that in the following theorem about the dual codes of γ-constacyclic codes.

Theorem 2.2 (cf. [20]) For each γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$, $\mathcal{C} = \langle (x - \gamma_0)^i\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$, where $0 \leq i \leq p^s$, its dual $\mathcal{C}^\perp$ is the γ^{-1}-constacyclic code $\mathcal{C}^\perp = \langle (x - \gamma_0^{-1})^{p^s-i}\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma^{-1}\rangle$, which contains p^{mi} codewords.

2.4.2 Hamming distance

[22], [18] proved that the Hamming distance of each γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$ is completely determined which is not depend on m. The Hamming distance of all γ-constacyclic code depends on the characteristic of $\mathbb{F}_{p^m}$ and length of the code.

Theorem 2.3 (cf. [18, 22]) Let $\mathcal{C}$ be a γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$. Then $\mathcal{C} = \langle (x-\gamma_0)^i \rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma \rangle$, for $i \in \{0,1,\ldots,p^s\}$, and its Hamming distance $\mathcal{H}_i := d_H(\mathcal{C})$ is completely determined by:

$$\mathcal{H}_i = \begin{cases} \bullet\, 1, & \text{if } i = 0, \\ \bullet\, (n+1)p^k, & \text{if } p^s - pr + (n-1)r + 1 \le i \le p^s - pr + nr, \\ & \text{where } r = p^{s-k-1},\ 1 \le n \le p-1 \text{ and } 0 \le k \le s-1, \\ \bullet\, 0, & \text{if } i = p^s. \end{cases}$$

Let $\mathcal{C} = \langle (x-\gamma_0)^i \rangle$ be a γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$, where $0 \le i \le p^s$. It is well known that $|\mathcal{C}| = p^{m(p^s-i)}$. So the dimension of code $\mathcal{C}$ is $p^s - i$. By the Singleton bound (2.1), $\mathcal{C}$ is an MDS code if and only if $p^s - i = p^s - d_H(\mathcal{C}) + 1$, i.e., $i = d_H(\mathcal{C}) - 1$. In [25], Dinh et al. identified all the MDS constacyclic codes of length p^s over $\mathbb{F}_{p^m}$.

Theorem 2.4 (cf. [25]) Let $\mathcal{C} = \langle (x-\gamma_0)^i \rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma \rangle$ be a γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$, where $i \in \{0,1,\ldots,p^s\}$. Then $\mathcal{C}$ is an MDS code if and only if one of the following conditions holds:

- If $s = 1$, then $i = \beta$ for $1 \le \beta \le p-1$, in such case, $d_H(\mathcal{C}) = \beta + 1$.
- If $s \ge 2$, then
  - $i = 0$, in such case, $d_H(\mathcal{C}) = 2$,
  - $i = 1$, in such case, $d_H(\mathcal{C}) = 2$,
  - $i = p^s - 1$, in such case, $d_H(\mathcal{C}) = p^s$.

2.4.3 Symbol-pair distance

The symbol-pair distance distribution of all constacyclic code of length p^s over $\mathbb{F}_{p^m}$ is established in [20].

Theorem 2.5 (cf. [20]) Let $\mathcal{C} = \langle (x-\gamma_0)^i \rangle, 0 \le i \le p^s$, be a γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$. Then the symbol-pair distance $\mathcal{S}_i := d_{sp}(\mathcal{C})$ of $\mathcal{C}$ is completely determined by:

$$\mathcal{S}_i = \begin{cases} \bullet\ 2, & \text{if } i = 0, \\ \bullet\ 3p^k, & \text{if } i = p^s - p^{s-k} + 1, \text{ where } 0 \le k \le s-2, \\ \bullet\ 4p^k, & \text{if } p^s - p^{s-k} + 2 \le i \le p^s - p^{s-k} + p^{s-k-1}, \\ & \text{where } 0 \le k \le s-2, \\ \bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr + \sigma r + 1 \le i \le p^s - pr + (\sigma+1)r, \\ & \text{where } r = p^{s-k-1},\ 0 \le k \le s-2 \text{ and } 1 \le \sigma \le p-2, \\ \bullet\ (\sigma+2)p^{s-1}, & \text{if } i = p^s - p + \sigma, \text{ where } 0 \le \sigma \le p-2, \\ \bullet\ p^s, & \text{if } i = p^s - 1, \\ \bullet\ 0, & \text{if } i = p^s. \end{cases}$$

By Singleton bound (2.2), $\mathcal{C}$ is an MDS symbol-pair code if and only if $p^s - i = p^s - d_{sp}(\mathcal{C}) + 2$, i.e., $i = d_{sp}(\mathcal{C}) - 2$. In [20], Dinh et al. identified all the MDS symbol-pair constacyclic codes of length p^s over $\mathbb{F}_{p^m}$.

Theorem 2.6 (cf. [20]) Let $\mathcal{C} = \langle (x-\gamma_0)^i \rangle$ be a γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$, for $i \in \{0, 1, \ldots, p^s\}$. Then $\mathcal{C}$ is an MDS symbol-pair constacyclic code if and only if one of the following conditions holds:

- If $s = 1$, then $i = \eta$ for $0 \le \eta \le p-2$, in such case, $d_{sp}(\mathcal{C}) = \eta + 2$.
- If $s \ge 2$, then
  - $i = 0$, in such case, $d_{sp}(\mathcal{C}) = 2$,
  - $i = 1$, in such case, $d_{sp}(\mathcal{C}) = 3$,
  - $i = 2$, in such case, $d_{sp}(\mathcal{C}) = 4$,
  - $s = 2$, $p = 3$, $i = 4$, in such case, $d_{sp}(\mathcal{C}) = 6$,
  - $i = p^s - 2$, in such case, $d_{sp}(\mathcal{C}) = p^s$.

Chapter 3

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

3.1 Introduction

In this chapter, we shall determine all repeated-root γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$. We shall also determine the number of codewords in each code.

For this, throughout this chapter, let p be a prime, s, m be positive integers, $\mathbb{F}_{p^m}$ be the finite field of order p^m, and denote

$$\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle.$$

The ring $\mathcal{R}$ can be expressed as $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m} = \{a + bu + cu^2 \mid a, b, c \in \mathbb{F}_{p^m}\}$, where $u^3 = 0$. It is known that $\mathcal{R}$ is a local ring with maximal ideal $\langle u\rangle = u\mathcal{R}$. Therefore, by Proposition 2.1, it is a chain ring. As discussed in Section 2.2, the γ-constacyclic codes of length p^s over $\mathcal{R}$ are ideals of the ring

$$\mathcal{R}_\gamma = \mathcal{R}[x]/\langle x^{p^s} - \gamma\rangle,$$

where γ is a nonzero element of the field $\mathbb{F}_{p^m}$.

This chapter is organized as follows: In Section 3.2, we classify all γ-constacyclic codes of length p^s over $\mathcal{R}$ into 8 distinct types and obtain the number of codewords in each of those constacyclic codes. To illustrate the results, Section 3.3 contains some examples of constacyclic codes for different values of p and s.

3.2 Algebraic structures of repeated-root γ-constacyclic codes of length p^s over $\mathcal{R}$

Recall that for any invertible element γ of $\mathbb{F}_{p^m}$, a γ-constacyclic code of length p^s over $\mathcal{R}$ is an ideal of the quotient ring $\mathcal{R}_\gamma$. Since γ is a nonzero element of the field $\mathbb{F}_{p^m}$, there exists $\gamma_0 \in \mathbb{F}_{p^m}$ such that $\gamma_0^{p^s} = \gamma$.

In this section, we will determine all γ-constacyclic codes of length p^s over $\mathcal{R}$ and the number of codewords in each code. The following fact will play an important role in our consideration later:

Lemma 3.1 The polynomial $x-\gamma_0$ is nilpotent in $\mathcal{R}_\gamma$ with nilpotency index p^s.

Proof For $1 \le i \le p^s-1$, p divides $\binom{p^s}{i}$. Since the characteristic of $\mathcal{R}$ is p, we have

$$(x-\gamma_0)^{p^s} = x^{p^s} - \gamma_0^{p^s} = x^{p^s} - \gamma.$$

The computation in $\mathcal{R}_\gamma$ gives $(x-\gamma_0)^{p^s} = 0$. Hence $x-\gamma_0$ is nilpotent of nilpotency index $\le p^s$. Since $(x-\gamma_0)^{p^s-1}$ is of degree $< p^s$, $(x-\gamma_0)^{p^s-1}$ cannot be zero in $\mathcal{R}_\gamma$. Therefore, the nilpotency index of $x-\gamma_0$ is p^s. □

Lemma 3.2 Let $f(x) \in \mathcal{R}_\gamma$. Then f(x) can be written uniquely as:

$$\begin{aligned} f(x) &= \sum_{i=0}^{p^s-1} a_i(x-\gamma_0)^i + u\sum_{i=0}^{p^s-1} b_i(x-\gamma_0)^i + u^2\sum_{i=0}^{p^s-1} c_i(x-\gamma_0)^i \\ &= a_0 + (x-\gamma_0)\sum_{i=1}^{p^s-1} a_i(x-\gamma_0)^{i-1} + u\sum_{i=0}^{p^s-1} b_i(x-\gamma_0)^i + u^2\sum_{i=0}^{p^s-1} c_i(x-\gamma_0)^i, \end{aligned}$$

where a_i, b_i and c_i are elements of $\mathbb{F}_{p^m}$. Furthermore, f(x) is invertible if and only if $a_0 \neq 0$.

Proof The representation of f(x) follows from the fact that it can be viewed as a polynomial of degree less than p^s over $\mathcal{R}$. Each coefficient d_i of f(x) is an element of $\mathcal{R}$, that can be expressed uniquely by $a_i, b_i, c_i \in \mathbb{F}_{p^m}$ as $d_i = a_i + ub_i + u^2c_i$. Expressing f(x) in this representation, the last assertion follows from the fact that u and $x-\gamma_0$ are both nilpotent in $\mathcal{R}_\gamma$. □

Proposition 3.1 The ring $\mathcal{R}_\gamma$ is a local ring with maximal ideal $\langle x-\gamma_0, u\rangle$, but it is not a chain ring.

Proof By Lemma 3.2, the ideal $\langle x-\gamma_0, u\rangle$ is precisely the set of non-invertible elements of $\mathcal{R}_\gamma$. Hence, $\mathcal{R}_\gamma$ is a local ring with the maximal ideal $\langle x-\gamma_0, u\rangle$. Here we will show that the ideal $\langle x-\gamma_0, u\rangle$ is not principal, for which it is enough to show that $u \notin \langle x-\gamma_0\rangle$ and $(x-\gamma_0) \notin \langle u\rangle$. For, if $u \in \langle x-\gamma_0\rangle$, then there exist polynomials $f_1(x)$ and $f_2(x) \in \mathcal{R}[x]$ such that $u = (x-\gamma_0)f_1(x) + (x^{p^s}-\gamma)f_2(x)$ in $\mathcal{R}[x]$. However, this is impossible because plugging in $x = \gamma_0$ yields $u = 0$. On the other hand, $(x-\gamma_0) \notin \langle u\rangle$, because $x-\gamma_0$ has nilpotency index p^s and $u^3 = 0$. Thus, $\langle x-\gamma_0, u\rangle$ is not a principal ideal of $\mathcal{R}_\gamma$, implying that $\mathcal{R}_\gamma$ is not a chain ring according to Proposition 2.1. □

Let μ be the map from $\mathcal{R}_\gamma = \mathcal{R}[x]/\langle x^{p^s}-\gamma\rangle$ to $\mathbb{F}_{p^m}[x]/\langle x^{p^s}-\gamma\rangle$ given by $\mu(f(x)) = f(x) \bmod u$. Clearly, μ is a surjective ring homomorphism.

Theorem 3.1 ([37]) The γ-constacyclic codes of length p^s over $\mathcal{R}$, i.e., ideals of the ring $\mathcal{R}_\gamma$, are

Type 1 ($\mathcal{C}_1$):

$$\langle 0\rangle, \quad \langle 1\rangle.$$

Type 2 ($\mathcal{C}_2$):

$$\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle, \text{ where } 0 \le \tau \le p^s-1.$$

Type 3 ($\mathcal{C}_3$):

$$\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x)\rangle,$$

where $0 \le L \le \delta \le p^s-1$, $0 \le t < L$, either $h(x)$ is 0 or $h(x)$ is a unit in $\mathcal{R}_\gamma$ of the form $\sum_{i=0}^{L-t-1} h_i(x-\gamma_0)^i$ with $h_i \in \mathbb{F}_{p^m}$ and $h_0 \neq 0$. Here L is the smallest integer satisfying $u^2(x-\gamma_0)^L \in \mathcal{C}_3$.

Type 4 ($\mathcal{C}_4$):

$$\mathcal{C}_4 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x), u^2(x-\gamma_0)^\omega\rangle,$$

where $0 \le \omega < L \le \delta \le p^s-1$, $0 \le t < \omega$, either $h(x)$ is 0 or $h(x)$ is a unit in $\mathcal{R}_\gamma$ of the form $\sum_{i=0}^{\omega-t-1} h_i(x-\gamma_0)^i$ with $h_i \in \mathbb{F}_{p^m}$, $h_0 \neq 0$ and L is the smallest integer satisfying $u^2(x-\gamma_0)^L \in \mathcal{C}_3$.

Type 5 ($\mathcal{C}_5$):

$$\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle,$$

where $0 < V \le U \le a \le p^s - 1$, $0 \le t_1 < U$, $0 \le t_2 < V$, $h_1(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{U-t_1-1} a_j(x-\gamma_0)^j$ with $a_j \in \mathbb{F}_{p^m}$, $a_0 \neq 0$ and $h_2(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{V-t_2-1} b_j(x-\gamma_0)^j$ with $b_j \in \mathbb{F}_{p^m}$, $b_0 \neq 0$. Here U is the smallest integer satisfying $u(x-\gamma_0)^U + u^2g(x) \in \mathcal{C}_5$, for some $g(x) \in \mathcal{R}_\gamma$ and V is the smallest integer such that $u^2(x-\gamma_0)^V \in \mathcal{C}_5$.

Type 6 ($\mathcal{C}_6$):

$$\mathcal{C}_6 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle,$$

where $0 \le c < V \le U \le a \le p^s - 1$, $0 \le t_1 < U$, $0 \le t_2 < c$, $h_1(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{U-t_1-1} a_j(x-\gamma_0)^j$ with $a_j \in \mathbb{F}_{p^m}$, $a_0 \neq 0$, $h_2(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{c-t_2-1} b_j(x-\gamma_0)^j$ with $b_j \in \mathbb{F}_{p^m}$, $b_0 \neq 0$ and U is the smallest integer satisfying $u(x-\gamma_0)^U + u^2g(x) \in \mathcal{C}_5$, for some $g(x) \in \mathcal{R}_\gamma$, V is the smallest integer such that $u^2(x-\gamma_0)^V \in \mathcal{C}_5$.

Type 7 ($\mathcal{C}_7$):

$$\mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle,$$

where $0 \le W \le b < U \le a \le p^s - 1$, $0 \le t_1 < b$, $0 \le t_2 < W$, $0 \le t_3 < W$, $h_1(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{b-t_1-1} a_j(x-\gamma_0)^j$ with $a_j \in \mathbb{F}_{p^m}$, $a_0 \neq 0$, $h_2(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{W-t_2-1} b_j(x-\gamma_0)^j$ with $b_j \in \mathbb{F}_{p^m}$, $b_0 \neq 0$ and $h_3(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{W-t_3-1} c_j(x-\gamma_0)^j$ with $c_j \in \mathbb{F}_{p^m}$, $c_0 \neq 0$. Here W is the smallest integer satisfying $u^2(x-\gamma_0)^W \in \mathcal{C}_7$ and U is the smallest integer satisfying $u(x-\gamma_0)^U + u^2g(x) \in \mathcal{C}_5$, for some $g(x) \in \mathcal{R}_\gamma$.

Type 8 ($\mathcal{C}_8$):

$$\mathcal{C}_8 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle,$$

where $0 \le c < W \le L_1 \le b < U \le a \le p^s - 1$, $0 \le t_1 < b$, $0 \le t_2 < c$, $0 \le t_3 < c$, $h_1(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{b-t_1-1} a_j(x-\gamma_0)^j$ with $a_j \in \mathbb{F}_{p^m}$, $a_0 \neq 0$, $h_2(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{c-t_2-1} b_j(x-\gamma_0)^i$ with $b_j \in \mathbb{F}_{p^m}$, $b_0 \neq 0$ and $h_3(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{c-t_3-1} c_j(x-\gamma_0)^j$ with $c_j \in \mathbb{F}_{p^m}$, $c_0 \neq 0$. Here L_1 is the smallest integer such that $u^2(x-\gamma_0)^{L_1} \in \langle u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$, U is the smallest integer satisfying $u(x-\gamma_0)^U + u^2g(x) \in \mathcal{C}_5$, for some $g(x) \in \mathcal{R}_\gamma$ and W is the smallest integer such that $u^2(x-\gamma_0)^W \in \mathcal{C}_7$.

Proof First of all, it is obvious to see that ideals of Type 1 ($\mathcal{C}_1$) are trivial ideals. Let I be an arbitrary nontrivial ideal of $\mathcal{R}_\gamma$. We proceed by establishing all possible forms that ideal I can have.

- Case 1. $I \subseteq \langle u\rangle$. Let $J_1 = \{f(x) \in \mathcal{R}_\gamma : f(x)u \in I\} = (I : u)$. Then, by Lemma 2.1,

$$I = uJ_1.$$

  * Case 1a. If $J_1 \subseteq \langle u\rangle$. Then, by Lemma 2.1, $J_1 = uJ_2$, where $J_2 = (J_1 : u) = ((I : u) : u) = (I : u^2)$, then $I = u^2J_2$. Note that $\mu(J_2)$ is a nonzero ideal of the ring $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$. Then according to Theorem 2.1, we have $\mu(J_2) = \langle (x-\gamma_0)^\tau\rangle$ for some τ, $0 \le \tau \le p^s - 1$. Further, by Lemma 2.1, there exists $f(x) \in \mathcal{R}_\gamma$, such that $J_2 = \langle (x-\gamma_0)^\tau + uf(x)\rangle$. This gives

$$I = \langle u^2(x-\gamma_0)^\tau\rangle \text{ with } 0 \le \tau \le p^s - 1,$$

which is of Type 2 ($\mathcal{C}_2$).

  * Case 1b. If $J_1 \not\subseteq \langle u\rangle$. Obviously, $\mu(J_1)$ is a nonzero ideal of the ring $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$. Then $\mu(J_1) = \langle (x-\gamma_0)^\delta\rangle$ for some δ, $0 \le \delta \le p^s - 1$. By Lemma 2.1, there exists $f_1(x) \in \mathcal{R}_\gamma$, such that $J_1 = \langle (x-\gamma_0)^\delta + uf_1(x)\rangle + uJ_2$, where $J_2 = (J_1 : u) = (I : u^2)$. Then $I = \langle u(x-\gamma_0)^\delta + u^2f_1(x)\rangle + u^2J_2$. We see that $J_2 \not\subseteq \langle u\rangle$ (because $J_1 \subseteq J_2$), implying that $\mu(J_2) = \langle (x-\gamma_0)^\omega\rangle$, for some ω, $0 \le \omega \le \delta \le p^s - 1$ (because $\mu(J_1) \subseteq \mu(J_2)$).

Also, by Lemma 2.1, there exists $f_2(x) \in \mathcal{R}_\gamma$, such that $J_2 = \langle (x-\gamma_0)^\omega + uf_2(x)\rangle$, which implies that $u^2J_2 = \langle u^2(x-\gamma_0)^\omega\rangle$. Then

$$I = \langle u(x-\gamma_0)^\delta + u^2f_1(x), u^2(x-\gamma_0)^\omega\rangle.$$

$f_1(x)$ can be expressed as

$$f_1(x) = \sum_{j=0}^{p^s-1} a_j(x-\gamma_0)^j + u\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} c_j(x-\gamma_0)^j,$$

where a_j, b_j and c_j are elements of $\mathbb{F}_{p^m}$, then

$$u(x-\gamma_0)^\delta + u^2f_1(x) = u(x-\gamma_0)^\delta + u^2\sum_{j=0}^{\omega-1} a_j(x-\gamma_0)^j + u^2(x-\gamma_0)^\omega\sum_{j=0}^{p^s-\omega-1} a_{j+\omega}(x-\gamma_0)^j.$$

Since $u(x-\gamma_0)^\delta+u^2f_1(x) \in I$ and $u^2(x-\gamma_0)^\omega \in I$, it follows that $u(x-\gamma_0)^\delta+u^2\sum_{j=0}^{\omega-1} a_j(x-\gamma_0)^j \in I$.

Thus, $I = \langle u(x-\gamma_0)^\delta + u^2\sum_{j=0}^{\omega-1} a_j(x-\gamma_0)^j, u^2(x-\gamma_0)^\omega\rangle$. From this, I can be expressed as

$$I = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x), u^2(x-\gamma_0)^\omega\rangle,$$

where $0 \le \omega \le \delta \le p^s-1$, $0 \le t < \omega$ and either $h(x)$ is 0 or $h(x)$ is a unit in $\mathcal{R}_\gamma$ of the form $\sum_{i=0}^{\omega-t-1} h_i(x-\gamma_0)^i$ with $h_i \in \mathbb{F}_{p^m}$, $h_0 \neq 0$.

Let L be the smallest integer such that $u^2(x-\gamma_0)^L \in \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$. Since $u^2(x-\gamma_0)^\delta \in \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$, we get $L \le \delta$. Note that $(x-\gamma_0)^L \in J_2$, which further implies that $u^2(x-\gamma_0)^L \in \langle u^2(x-\gamma_0)^\omega\rangle$, then $\omega \le L$.

- Case 1b1. If $\omega = L$, then

$$I = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle,$$

which is an ideal of Type3 ($\mathcal{C}_3$).

- Case 1b2. If $\omega < L$, then

$$I = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x), u^2(x-\gamma_0)^\omega\rangle,$$

which means that I is of Type4 ($\mathcal{C}_4$).

• Case 2. If $I \not\subseteq \langle u\rangle$. Then $\mu(I)$ is a nonzero ideal of the ring $\mathbb{F}_{p^m}[x]/\langle x^{p^s}-\gamma\rangle$. Hence there is an integer $a \in \{0,1,\ldots,p^s-1\}$ such that $\mu(I) = \langle (x-\gamma_0)^a\rangle$. Next by Lemma 2.1, there exists $f(x) \in \mathcal{R}_\gamma$, such that $I = \langle (x-\gamma_0)^a + uf(x)\rangle + uJ_1$, where $J_1 = (I : u)$. We have $uJ_1 \subseteq \langle u\rangle$ and we see that $(uJ_1 : u) = (\langle u\rangle \cap I : u) = (I : u) = J_1 \not\subseteq \langle u\rangle$ (because $I \subseteq J_1$). This, by Case 1b, implies that

$$uJ_1 = \langle u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle,$$

where $0 \le c \le L_1 \le b \le p^s-1$, $0 \le t_3 < c$, either $h_3(x)$ is 0 or $h_3(x)$ is a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{c-t-1} c_j(x-\gamma_0)^j$ with $c_j \in \mathbb{F}_{p^m}$, $c_0 \neq 0$ and $u^2J_2 := u^2((uJ_1 : u) : u) = u^2(J_1 : u) = u^2(I : u^2) = \langle u^2(x-\gamma_0)^c\rangle$. Here L_1 is the smallest integer satisfying $u^2(x-\gamma_0)^{L_1} \in \langle u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$. Therefore, we have

$$I = \langle (x-\gamma_0)^a + uf(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle.$$

Let us write

$$f(x) = \sum_{j=0}^{p^s-1} a_j(x-\gamma_0)^j + u\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} c_j(x-\gamma_0)^j,$$

where a_j, b_j and c_j are elements of $\mathbb{F}_{p^m}$, then

$$\begin{aligned}(x-\gamma_0)^a + uf(x) &= (x-\gamma_0)^a + u\sum_{j=0}^{p^s-1} a_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j \\ &= (x-\gamma_0)^a + u\sum_{j=0}^{b-1} a_j(x-\gamma_0)^j + u\sum_{j=b}^{p^s-1} a_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j \\ &= (x-\gamma_0)^a + u\sum_{j=0}^{b-1} a_j(x-\gamma_0)^j + [u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)]\sum_{j=b}^{p^s-1} a_j(x-\gamma_0)^{j-b} \\ &\quad + u^2\left(\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j - (x-\gamma_0)^{t_3}h_3(x)\sum_{j=b}^{p^s-1} a_j(x-\gamma_0)^{j-b}\right).\end{aligned}$$

Since $(x-\gamma_0)^a + uf(x) \in I$ and $u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x) \in I$, it follows that

$$(x-\gamma_0)^a + u\sum_{j=0}^{b-1} a_j(x-\gamma_0)^j + u^2\left(\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j - (x-\gamma_0)^{t_3}h_3(x)\sum_{j=b}^{p^s-1} a_j(x-\gamma_0)^{j-b}\right) \in I$$

Next we write

$$u^2\left(\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j-(x-\gamma_0)^{t_3}h_3(x)\sum_{j=b}^{p^s-1} a_j(x-\gamma_0)^{j-b}\right)=u^2\sum_{j=0}^{p^s-1} d_j(x-\gamma_0)^j,$$

where $d_j\in\mathbb{F}_{p^m}$. Further, for all $j\geq c$, we see that $u^2(x-\gamma_0)^j=u^2(x-\gamma_0)^c(x-\gamma_0)^{j-c}\in I$, which implies that

$$I=\langle(x-\gamma_0)^a+u\sum_{j=0}^{b-1} a_j(x-\gamma_0)^j+u^2\sum_{j=0}^{c-1} d_j(x-\gamma_0)^j, u(x-\gamma_0)^b+u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$$

From this, it follows that

$$I=\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b+u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$$

where $0\leq t_1<b$, $0\leq t_2<c$, $h_1(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{b-t_1-1} a_j(x-\gamma_0)^j$ with $a_j\in\mathbb{F}_{p^m}$, $a_0\neq 0$ and $h_2(x)$ is either 0 or a unit in $\mathcal{R}_\gamma$ of the form $\sum_{j=0}^{c-t_2-1} d_j(x-\gamma_0)^j$ with $d_j\in\mathbb{F}_{p^m}$, $d_0\neq 0$.

Let U be the smallest integer such that $u(x-\gamma_0)^U+u^2g(x)\in\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$, for some $g(x)\in\mathcal{R}_\gamma$. Since $u(x-\gamma_0)^a+u^2(x-\gamma_0)^{t_1}h_1(x)\in\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$, we get $U\leq a$. As $u^2(x-\gamma_0)^U\in\langle u^2(x-\gamma_0)^b\rangle$ with the reason that $(x-\gamma_0)^U+ug(x)\in(I:u)=J_1=(uJ_1:u)$, we have $b\leq U$.

* Case 2a. If $b=U$, then $I=\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$.

Let V be the smallest integer such that $u^2(x-\gamma_0)^V\in\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$. Since $u^2(x-\gamma_0)^U\in\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$, we get $V\leq U$. As $u^2(x-\gamma_0)^V\in\langle u^2(x-\gamma_0)^c\rangle$ with the reason that $(x-\gamma_0)^V\in J_2:=(I:u^2)$, we have $c\leq V$.

  ○ Case 2a1. If $c=V$, then

$$I=\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)\rangle,$$

which is an ideal of Type 5 ($\mathcal{C}_5$).

  ○ Case 2a2. If $c<V$, then

$$I=\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle,$$

which means that I is of Type 6 ($\mathcal{C}_6$).

* Case 2b. If $b < U$, then

$$I = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle.$$

Let W be the smallest integer such that $u^2(x-\gamma_0)^W \in \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$. Since $u^2(x-\gamma_0)^V \in \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$ and $u^2(x-\gamma_0)^{L_1} \in \langle u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$, we get $W \le V$ and $W \le L_1$. As $u^2(x-\gamma_0)^W \in \langle u^2(x-\gamma_0)^c\rangle$ with the reason that $(x-\gamma_0)^W \in J_2 := (I : u^2)$, we have $c \le W$.

  ○ Case 2b1. If $c = W$, then

$$I = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle,$$

which means that I is of Type 7 ($\mathcal{C}_7$).

  ○ Case 2b2. If $c < W$, then

$$I = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle,$$

which is an ideal of Type 8 ($\mathcal{C}_8$). This completes the proof of the theorem. □

Remark 3.1 In the case that $\gamma = 1$, those γ-constacyclic codes are called cyclic codes. Actually, cyclic codes of length p^s over $\mathcal{R}$ had already been studied in [41, Theorem 4.3], but their classification of the structures of such codes is incomplete, i.e., their are some intersections between their types. We illustrate some of the intersections in the following.

1. If $\mathcal{C}$ is of the Type 8, i.e,

$$\mathcal{C} = \left\langle (x-1)^i + u\sum_{j=0}^{i-1} a_j(x-1)^j + u^2\sum_{j=0}^{\eta-1} b_j(x-1)^j, u^2(x-1)^\eta \right\rangle$$
$$= \langle (x-1)^i + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x), u^2(x-1)^\eta\rangle,$$

where $a_j, b_j \in \mathbb{F}_{p^m}$, $0 \le i \le p^s-1$, $\eta < i$, $0 \le t_1 < i$, $0 \le t_2 < \eta$ and either $h_1(x)$, $h_2(x)$ are 0 or $h_1(x)$, $h_2(x)$ are units, with $\deg(h_1(x)) \le i-t_1-1$ and $\deg(h_2(x)) \le \eta-t_2-1$. Then

(a) When $h_1(x) = 0, h_2(x) \ne 0, \frac{p^s+t_2}{2} < i \le p^s-1$ and $\eta = p^s-i+t_2 < i$, we have

$$\begin{aligned} & u^2(x-1)^\eta \\ &= u^2(x-1)^{p^s-i+t_2} \\ &= (h_2(x))^{-1}[(x-1)^i + u^2(x-1)^{t_2}h_2(x)](x-1)^{p^s-i} \\ &\in \langle (x-1)^i + u^2(x-1)^{t_2}h_2(x)\rangle, \end{aligned}$$

which means that $\mathcal{C} = \langle (x-1)^i + u^2(x-1)^{t_2}h_2(x)\rangle$ is of the Type 5.

(b) When $h_1(x)\neq 0$, $\frac{p^s+t_1}{2} < i \leq p^s-1$ and $\eta = p^s - i + t_1 < i$, we have

$$\begin{aligned} & u^2(x-1)^{\eta} \\ &= u^2(x-1)^{p^s-i+t_1} \\ &= u(h_1(x))^{-1}[(x-1)^i + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x)](x-1)^{p^s-i} \\ &\in \langle (x-1)^i + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x)\rangle, \end{aligned}$$

which implies that $\mathcal{C} = \langle (x-1)^i + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x)\rangle$ is of the Type 5.

2. Let $\mathcal{C}$ be of the Type 6, i.e,

$$\begin{aligned} \mathcal{C} &= \left\langle (x-1)^i + u\sum_{j=0}^{q-1} a_j(x-1)^j + u^2\sum_{j=0}^{q-1} b_j(x-1)^j, u(x-1)^q + u^2\sum_{j=0}^{q-1} c_j(x-1)^j \right\rangle \\ &= \langle (x-1)^i + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x), u(x-1)^q + u^2(x-1)^{t_3}h_3(x)\rangle, \end{aligned}$$

where $a_j, b_j, c_j \in \mathbb{F}_{p^m}$, $0 \leq i \leq p^s-1$, $q \leq i$, $0 \leq t_1 < q$, $0 \leq t_2 < q$, $0 \leq t_3 < q$ and either $h_1(x)$, $h_2(x)$, $h_3(x)$ are 0 or $h_1(x)$, $h_2(x)$, $h_3(x)$ are units, with $\deg(h_1(x)) \leq q - t_1 - 1$, $\deg(h_2(x)) \leq q - t_2 - 1$ and $\deg(h_3(x)) \leq q - t_3 - 1$.
When $h_3(x) = h_2(x) = 0$, $h_1(x)\neq 0$, $\frac{p^s+t_1}{2} < i \leq p^s-1$ and $q = p^s - i + t_1 < i$, we have

$$\begin{aligned} u(x-1)^q &= u(x-1)^{p^s-i+t_1} \\ &= (h_1(x))^{-1}[(x-1)^i + u(x-1)^{t_1}h_1(x)](x-1)^{p^s-i} \\ &\in \langle (x-1)^i + u(x-1)^{t_1}h_1(x)\rangle, \end{aligned}$$

which means that $\mathcal{C} = \langle (x-1)^i + u(x-1)^{t_1}h_1(x)\rangle$ is of the Type 5.

3. If $\mathcal{C}$ is of the Type 7, i.e,

$$\mathcal{C} = \langle (x-1)^i + u\sum_{j=0}^{q-1} a_j(x-1)^j + u^2\sum_{j=0}^{\sigma-1} b_j(x-1)^j, u(x-1)^q + u^2\sum_{j=0}^{\sigma-1} c_j(x-1)^j, u^2(x-1)^{\sigma}\rangle$$

$$= \langle (x-1)^i + u(x-1)^{t_1}h_1(x) + u^2(x-1)^{t_2}h_2(x), u(x-1)^q + u^2(x-1)^{t_3}h_3(x), u^2(x-1)^{\sigma}\rangle,$$

where $a_j, b_j, c_j \in \mathbb{F}_{p^m}$, $0 \leq i \leq p^s-1$, $\sigma < q \leq i$, $0 \leq t_1 < q$, $0 \leq t_2 < \sigma$, $0 \leq t_3 < \sigma$, either $h_1(x)$, $h_2(x)$, $h_3(x)$ are 0 or $h_1(x)$, $h_2(x)$, $h_3(x)$ are units, with $\deg(h_1(x)) \leq q - t_1 - 1$, $\deg(h_2(x)) \leq \sigma - t_2 - 1$, $\deg(h_3(x)) \leq \sigma - t_3 - 1$ and $\sigma < T = \begin{cases} q, & \text{if } h_3(x) = 0, \\ \min\{q, p^s - q + t_3\}, & \text{if } h_3(x) \neq 0. \end{cases}$

Then

(a) When $h_1(x) = h_3(x) = 0, h_2(x) \neq 0$, $p^s - q + t_2 < i \leq p^s - 1$ and $\sigma = p^s - i + t_2 < q$, (or $h_1(x) = 0, h_2(x) \neq 0$, $h_3(x) \neq 0$, $\max\{p^s - q + t_2, q + t_2 - t_3\} < i \leq p^s - 1$ and $\sigma = p^s - i + t_2 < \min\{q, p^s - q + t_3\}$), we have

$$\begin{aligned} u^2(x-1)^{\sigma} &= u^2(x-1)^{p^s-i+t_2} \\ &= (h_2(x))^{-1}[(x-1)^i + u^2(x-1)^{t_2}h_2(x)](x-1)^{p^s-i} \\ &\in \langle (x-1)^i + u^2(x-1)^{t_2}h_2(x)\rangle, \end{aligned}$$

which means that $\mathcal{C} = \langle (x-1)^i + u^2(x-1)^{t_2}h_2(x), u(x-1)^q\rangle$ (respectively $\mathcal{C} = \langle (x-1)^i + u^2(x-1)^{t_2}h_2(x), u(x-1)^q + u^2(x-1)^{t_3}h_3(x)\rangle$) is of the Type 6.

(b) When $h_3(x) = h_2(x) = 0$, $h_1(x) \neq 0$, $\frac{p^s + t_1}{2} < i \leq p^s - 1$ and $q = p^s - i + t_1 < i$, we have

$$\begin{aligned} u(x-1)^q &= u(x-1)^{p^s-i+t_1} \\ &= (h_1(x))^{-1}[(x-1)^i + u(x-1)^{t_1}h_1(x)](x-1)^{p^s-i} \\ &\in \langle (x-1)^i + u(x-1)^{t_1}h_1(x)\rangle, \end{aligned}$$

which means that $\mathcal{C} = \langle (x-1)^i + u(x-1)^{t_1}h_1(x), u^2(x-1)^{\sigma}\rangle$ is of the Type 8.

By the above theorem, we see that L, L_1 are the smallest integers such that

$$u^2(x-\gamma_0)^L \in \mathcal{C}_3 = \langle u(x-\gamma_0)^{\delta} + u^2(x-\gamma_0)^t h(x)\rangle,$$

$$u^2(x-\gamma_0)^{L_1} \in \langle u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle.$$

In the following proposition, we determine L and L_1.

Proposition 3.2 Let L and L_1 be as above, then we have

$$L = \begin{cases} \delta, & \text{if } h(x) = 0, \\ \min\{\delta, p^s - \delta + t\}, & \text{if } h(x) \neq 0. \end{cases}$$

$$L_1 = \begin{cases} b, & \text{if } h_3(x) = 0, \\ \min\{b, p^s - b + t_3\}, & \text{if } h_3(x) \neq 0. \end{cases}$$

Proof As $u^2(x-\gamma_0)^\delta = u[u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x)] \in \mathcal{C}_3$, we have $L \le \delta$. Further, $u^2(x-\gamma_0)^L \in \mathcal{C}_3$ can be written as

$$u^2(x-\gamma_0)^L = \left(\sum_{j=0}^{p^s-1} a_j(x-\gamma_0)^j + u\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} c_j(x-\gamma_0)^j\right)[u(x-\gamma_0)^i + u^2(x-\gamma_0)^t h(x)],$$

where a_j, b_j and c_j are elements of $\mathbb{F}_{p^m}$.

As $(x-\gamma_0)^{p^s} = 0$ in $\mathcal{R}_\gamma$ and $u^2(x-\gamma_0)^L \in \langle u^2\rangle$, $u^2(x-\gamma_0)^L$ can be rewritten as

$$\begin{aligned} u^2(x-\gamma_0)^L &= u(x-\gamma_0)^\delta \sum_{j=0}^{p^s-\delta-1} a_j(x-\gamma_0)^j + u^2(x-\gamma_0)^\delta \sum_{j=0}^{p^s-\delta-1} b_j(x-\gamma_0)^j \\ &\quad + u^2(x-\gamma_0)^t h(x)\sum_{j=0}^{p^s-\delta-1} a_j(x-\gamma_0)^j + u^2(x-\gamma_0)^t h(x)\sum_{j=p^s-\delta}^{p^s-1} a_j(x-\gamma_0)^j \\ &= u^2(x-\gamma_0)^\delta \sum_{j=0}^{p^s-\delta-1} b_j(x-\gamma_0)^j + u^2(x-\gamma_0)^{p^s-\delta+t}h(x)\sum_{j=0}^{\delta-1} a_{p^s-\delta+j}(x-\gamma_0)^j. \end{aligned}$$

From this, we get $L \ge \delta$ when $h(x) = 0$ and $L \ge \min\{\delta, p^s - \delta + t\}$ when $h(x) \ne 0$. Moreover, when $h(x) \ne 0$ then $h(x)$ is a unit, so

$$u^2(x-\gamma_0)^{p^s-\delta+t} = (h(x))^{-1}[u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x)](x-\gamma_0)^{p^s-\delta} \in \mathcal{C}_3,$$

then we get $L \le p^s - \delta + t$. Therefore, $L = \min\{\delta, p^s - \delta + t\}$. The proof of L_1 is similar. □

According to the classification in Theorem 3.1, we see that U is the smallest non-negative integer satisfying

$$u(x-\gamma_0)^U + u^2 g(x) \in \mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle,$$

for some $g(x) \in \mathcal{R}_\gamma$. As $u(x-\gamma_0)^a + u^2(x-\gamma_0)^{t_1}h_1(x) \in \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$, we have $U \le a$.

In the following proposition, we determine the integer U.

Proposition 3.3 Let U be as above, then we have

$$U = \begin{cases} a, & \text{if } h_1(x) = 0, \\ \min\{a, p^s - a + t_1\}, & \text{if } h_1(x) \ne 0. \end{cases}$$

Proof Since $u(x-\gamma_0)^U+u^2g(x)\in\mathcal{C}_5=\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$, for some $g(x)\in\mathcal{R}_\gamma$, there is a polynomial $f(x)\in\mathcal{R}_\gamma$ satisfying $u(x-\gamma_0)^U+u^2g(x)=f(x)[(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)]$.

$f(x)$ can be written as $f(x)=\sum_{j=0}^{p^s-1}a_j(x-\gamma_0)^j+u\sum_{j=0}^{p^s-1}b_j(x-\gamma_0)^j+u^2\sum_{j=0}^{p^s-1}c_j(x-\gamma_0)^j$, where a_j, b_j and c_j are elements of $\mathbb{F}_{p^m}$. Then $u^2(x-\gamma_0)^U$ can be expressed as

$$u^2(x-\gamma_0)^U=u(x-\gamma_0)^a\sum_{j=0}^{p^s-1}a_j(x-\gamma_0)^j+u^2(x-\gamma_0)^a\sum_{j=0}^{p^s-1}b_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{t_1}h_1(x)\sum_{j=0}^{p^s-1}a_j(x-\gamma_0)^j.$$

As $(x-\gamma_0)^{p^s}=0$ in $\mathcal{R}_\gamma$ and $u^2(x-\gamma_0)^U\in\langle u^2\rangle$, $u^2(x-\gamma_0)^U$ can be rewritten as

$$\begin{aligned}u^2(x-\gamma_0)^U&=u(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1}a_j(x-\gamma_0)^j+u^2(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1}b_j(x-\gamma_0)^j\\&\quad+u^2(x-\gamma_0)^{t_1}h_1(x)\sum_{j=0}^{p^s-a-1}a_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{t_1}h_1(x)\sum_{j=p^s-a}^{p^s-1}a_j(x-\gamma_0)^j\\&=u^2(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1}b_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{p^s-a+t_1}h_1(x)\sum_{j=0}^{a-1}a_{p^s-a+j}(x-\gamma_0)^j.\end{aligned}$$

From this, we get $U\geq a$ when $h_1(x)=0$ and $U\geq\min\{a,p^s-a+t_1\}$ when $h_1(x)\neq 0$. Moreover, when $h_1(x)\neq 0$ then $h_1(x)$ is a unit, so $u(x-\gamma_0)^{p^s-a+t_1}+u^2(x-\gamma_0)^{p^s-a+t_2}h_2(x)(h_1(x))^{-1}=(h_1(x))^{-1}[(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)](x-\gamma_0)^{p^s-a}\in\mathcal{C}_5$. Hence, we get $U\leq p^s-a+t_1$. From this, the desired result follows. □

In light of Theorem 3.1, we have V is the smallest integer such that

$$u^2(x-\gamma_0)^V\in\mathcal{C}_5=\langle(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)\rangle.$$

We observe that $V\leq a$ with the reason that $u^2(x-\gamma_0)^a=u^2[(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)]\in\mathcal{C}_5$.

In the following proposition, we determine the integer V.

Proposition 3.4 Let V be as above, then we have

$$V=\begin{cases}a, & \text{if } h_1(x)=h_2(x)=0,\\ \min\{a,p^s-a+t_2\}, & \text{if } h_1(x)=0 \text{ and } h_2(x)\neq 0,\\ \min\{a,p^s-a+t_1\}, & \text{if } h_1(x)\neq 0.\end{cases}$$

Proof Since $u^2(x-1)^V \in \mathcal{C}_5$, then $u^2(x-1)^V$ can be written as

$$\left(\sum_{j=0}^{p^s-1} a_j(x-\gamma_0)^j + u\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} c_j(x-\gamma_0)^j\right)[(x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x)],$$

where a_j, b_j and c_j are elements of $\mathbb{F}_{p^m}$.

As $(x-\gamma_0)^{p^s} = 0$ in $\mathcal{R}_\gamma$, $u^2(x-\gamma_0)^V$ can be rewritten as

$$\begin{aligned}
u^2(x-\gamma_0)^V = {} & (x-\gamma_0)^a\sum_{j=0}^{p^s-a-1} a_j(x-\gamma_0)^j + u(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1} b_j(x-\gamma_0)^j \\
& + u^2(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1} c_j(x-\gamma_0)^j + u(x-\gamma_0)^{t_1}h_1(x)\sum_{j=0}^{p^s-a-1} a_j(x-\gamma_0)^j \\
& + u(x-\gamma_0)^{t_1}h_1(x)\sum_{j=p^s-a}^{p^s-1} a_j(x-\gamma_0)^j + u^2(x-\gamma_0)^{t_1}h_1(x)\sum_{j=0}^{p^s-a-1} b_j(x-\gamma_0)^j \\
& + u^2(x-\gamma_0)^{t_1}h_1(x)\sum_{j=p^s-a}^{p^s-1} b_j(x-\gamma_0)^j + u^2(x-\gamma_0)^{t_2}h_2(x)\sum_{j=0}^{p^s-a-1} a_j(x-\gamma_0)^j \\
& + u^2(x-\gamma_0)^{t_2}h_2(x)\sum_{j=p^s-a}^{p^s-1} a_j(x-\gamma_0)^j.
\end{aligned}$$

∗ Case 1. If $h_1(x) = 0$. Then

$$u^2(x-\gamma_0)^V = u^2(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1} c_j(x-\gamma_0)^j + u^2(x-\gamma_0)^{p^s-a+t_2}h_2(x)\sum_{j=0}^{a-1} a_{p^s-a+j}(x-\gamma_0)^j.$$

- Case 1a. If $h_2(x) = 0$. Then, we have $V \geq a$, which means that $V = a$.
- Case 1b. If $h_2(x) \neq 0$. Then, we have $V \geq \min\{a, p^s-a+t_2\}$. Hence,

$$u^2(x-\gamma_0)^{p^s-a+t_2} = (h_2(x))^{-1}[(x-\gamma_0)^a + u^2(x-\gamma_0)^{t_2}h_2(x)](x-\gamma_0)^{p^s-a} \in \mathcal{C}_5.$$

Thus, $V \leq p^s-a+t_2$, which means that $V = \min\{a, p^s-a+t_2\}$.

* Case 2. If $h_1(x) \neq 0$. Then

$$u^2(x-\gamma_0)^V = u^2(x-\gamma_0)^a \sum_{j=0}^{p^s-a-1} c_j(x-\gamma_0)^j + u^2(x-\gamma_0)^{p^s-a+t_1}h_1(x)\sum_{j=0}^{a-1} b_{p^s-a+j}(x-\gamma_0)^j.$$

So, $V \geq \min\{a, p^s-a+t_1\}$. Hence,

$$u^2(x-\gamma_0)^{p^s-a+t_1} = u(h_1(x))^{-1}[(x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)](x-\gamma_0)^{p^s-a} \in \mathcal{C}_5.$$

Thus, $V \leq p^s-a+t_1$, which means that $V = \min\{a, p^s-a+t_1\}$. □

Note that W is the smallest integer such that $u^2(x-1)^W \in \mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$, as determined in Theorem 3.1.

We now proceed to determine W.

Proposition 3.5 Let W be as above, then we have

$$W = \begin{cases} b, & \text{if } h_1(x) = h_2(x) = h_3(x) = 0 \\ & \text{or } h_1(x) \neq 0 \text{ and } h_3(x) = 0, \\ \min\{b, p^s-a+t_2\}, & \text{if } h_1(x) = h_3(x) = 0, h_2(x) \neq 0, \\ \min\{b, p^s-b+t_3\}, & \text{if } h_1(x) = h_2(x) = 0, h_3(x) \neq 0 \\ & \text{or } h_1(x) \neq 0 \text{ and } h_3(x) \neq 0, \\ \min\{b, p^s-a+t_2, p^s-b+t_3\}, & \text{if } h_1(x) = 0, h_2(x) \neq 0, h_3(x) \neq 0. \end{cases}$$

Proof First of all, as $u^2(x-\gamma_0)^b = u[u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)] \in \mathcal{C}_7$, we have $W \leq b$. Now, since $u^2(x-\gamma_0)^W$ is an element of $\mathcal{C}_7$, then there exist $f_1(x)$ and $f_2(x)$ in $\mathcal{R}_\gamma$ such that $u^2(x-\gamma_0)^W = f_1(x)[(x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)] + f_2(x)[u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)]$. Write $f_1(x)$ and $f_2(x)$ as:

$$f_1(x) = \sum_{j=0}^{p^s-1} a_j(x-\gamma_0)^j + u\sum_{j=0}^{p^s-1} b_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} c_j(x-\gamma_0)^j$$

and

$$f_2(x) = \sum_{j=0}^{p^s-1} d_j(x-\gamma_0)^j + u\sum_{j=0}^{p^s-1} e_j(x-\gamma_0)^j + u^2\sum_{j=0}^{p^s-1} f_j(x-\gamma_0)^j,$$

where a_j, b_j, c_j, d_j, e_j and f_j are elements of $\mathbb{F}_{p^m}$.

As $(x-\gamma_0)^{p^s}=0$ in $\mathcal{R}_\gamma$, then $u^2(x-\gamma_0)^W$ can be expressed as follows:

$$\begin{aligned}u^2(x-\gamma_0)^W &= (x-\gamma_0)^a\sum_{j=0}^{p^s-a-1}a_j(x-\gamma_0)^j+u(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1}b_j(x-\gamma_0)^j\\&+u^2(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1}c_j(x-\gamma_0)^j+u(x-\gamma_0)^{t_1}h_1(x)\sum_{j=0}^{p^s-a-1}a_j(x-\gamma_0)^j\\&+u(x-\gamma_0)^{t_1}h_1(x)\sum_{j=p^s-a}^{p^s-1}a_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{t_1}h_1(x)\sum_{j=0}^{p^s-a-1}b_j(x-\gamma_0)^j\\&+u^2(x-\gamma_0)^{t_1}h_1(x)\sum_{j=p^s-a}^{p^s-1}b_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{t_2}h_2(x)\sum_{j=0}^{p^s-a-1}a_j(x-\gamma_0)^j\\&+u^2(x-\gamma_0)^{t_2}h_2(x)\sum_{j=p^s-a}^{p^s-1}a_j(x-\gamma_0)^j+u(x-\gamma_0)^b\sum_{j=0}^{p^s-b-1}d_j(x-\gamma_0)^j\\&+u^2(x-\gamma_0)^b\sum_{j=0}^{p^s-b-1}e_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{t_3}h_3(x)\sum_{j=0}^{p^s-b-1}d_j(x-\gamma_0)^j\\&+u^2(x-\gamma_0)^{t_3}h_3(x)\sum_{j=p^s-b}^{p^s-1}d_j(x-\gamma_0)^j.\end{aligned}$$

- Case 1. If $h_1(x)=0$. Then,

$$\begin{aligned}u^2(x-\gamma_0)^W &= u^2(x-\gamma_0)^a\sum_{j=0}^{p^s-a-1}c_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{p^s-a+t_2}h_2(x)\sum_{j=0}^{a-1}a_{p^s-a+j}(x-\gamma_0)^j\\&+u^2(x-\gamma_0)^b\sum_{j=0}^{p^s-b-1}e_j(x-\gamma_0)^j+u^2(x-\gamma_0)^{p^s-b+t_3}h_3(x)\sum_{j=0}^{b-1}d_{p^s-b+j}(x-\gamma_0)^j.\end{aligned}$$

  * Case 1a. When $h_2(x)=0$. We divide into two subcases.

    ○ Case 1a1. If $h_3(x)=0$. Then, $W\geq\min\{a,b\}=b$, which means that $W=b$.

    ○ Case 1a2. If $h_3(x)\neq 0$. Then, $W\geq\min\{a,p^s-b+t_3,b\}$, but $a\geq b$ and hence $W\geq\min\{p^s-b+t_3,b\}$. As,

$$u^2(x-\gamma_0)^{p^s-b+t_3}=(h_3(x))^{-1}[u(x-\gamma_0)^b+u^2(x-\gamma_0)^{t_3}h_3(x)](x-\gamma_0)^{p^s-b}\in\mathcal{C}_7,$$

we get $W\leq p^s-b+t_3$, which means that $W=\min\{b,p^s-b+t_3\}$.

∗ Case 1b. When $h_2(x) \neq 0$. We have two subcases.

◦ Case 1b1. If $h_3(x) = 0$. Then, $W \geq \min\{a, p^s - a + t_2, b\}$, but $a \geq b$ and hence $W \geq \min\{b, p^s - a + t_2\}$. Moreover,

$$u^2(x-\gamma_0)^{p^s-a+t_2} = (h_2(x))^{-1}[(x-\gamma_0)^a + u^2(x-\gamma_0)^{t_2}h_2(x)](x-\gamma_0)^{p^s-a} \in \mathcal{C}_7.$$

So, $W \leq p^s - a + t_2$, which means that $W = \min\{b, p^s - a + t_2\}$.

◦ Case 1b2. If $h_3(x) \neq 0$. Then, $W \geq \min\{a, p^s - a + t_2, b, p^s - b + t_3\}$, but $a \geq b$ and hence $W \geq \min\{b, p^s - a + t_2, p^s - b + t_3\}$. Then $W = \min\{b, p^s - a + t_2, p^s - b + t_3\}$.

• Case 2. If $h_1(x) \neq 0$. Then,

$$u^2(x-\gamma_0)^W = u^2(x-\gamma_0)^a \sum_{j=0}^{p^s-a-1} c_j(x-\gamma_0)^j + u^2(x-1)^{p^s-a+t_1}h_1(x)\sum_{j=0}^{a-1} b_{p^s-a+j}(x-\gamma_0)^j$$

$$+ u^2(x-\gamma_0)^b \sum_{j=0}^{p^s-b-1} e_j(x-\gamma_0)^j + u^2(x-\gamma_0)^{p^s-b+t_3}h_3(x)\sum_{j=0}^{b-1} d_{p^s-b+j}(x-\gamma_0)^j.$$

∗ Case 2a. If $h_3(x) = 0$. Then, $W \geq \min\{a, p^s-a+t_1, b\}$, but $\min\{a, p^s-a+t_1\} \geq b$ and hence $W \geq b$, which means that $W = b$.

∗ Case 2b. If $h_3(x) \neq 0$. Then, $W \geq \min\{a, p^s-a+t_1, b, p^s-b+t_3\}$, but $\min\{a, p^s-a+t_1\} \geq b$ and hence $W \geq \min\{b, p^s-b+t_3\}$, which means that $W = \min\{b, p^s-b+t_3\}$. □

The following definition is indeed Definition 6.1 in [30] and Definition 2.1 in [36], for our case.

Definition 3.1 Let $\mathcal{C}$ be a γ-constacyclic code of length p^s over $\mathcal{R}$, (i.e., an ideal of the ring $\mathcal{R}_\gamma$). For any $0 \leq i \leq 2$ define

$$\mathrm{Tor}_i(\mathcal{C}) = \mu(\{f(x) \in \mathcal{R}_\gamma : f(x)u^i \in \mathcal{C}\}),$$

which is an ideal of the ring $\mathbb{F}_{p^m}[x]/\langle x^{p^s} - \gamma\rangle$. $\mathrm{Tor}_i(\mathcal{C})$ is called the i-th torsion code of $\mathcal{C}$ and $\mu(\mathcal{C}) = \mathrm{Tor}_0(\mathcal{C}) = \mathrm{Res}(\mathcal{C})$ is called the residue code of $\mathcal{C}$.

Clearly, $v \in \mathrm{Tor}_i(\mathcal{C})$ if and only if $u^i(v+uz) \in \mathcal{C}$ for some z in $\mathcal{R}_\gamma$. Moreover, it is clear that $\mathrm{Tor}_i(\mathcal{C}) \subseteq \mathrm{Tor}_{i+1}(\mathcal{C})$.

The following theorem presents some results and facts about torsion codes of a code $\mathcal{C}$.

Theorem 3.2 For $0 \le i \le 2$, $\mathrm{Tor}_i(\mathcal{C})$ is a γ-constacyclic code of length p^s over $\mathbb{F}_{p^m}$. Furthermore, we have $\mathrm{Tor}_i(\mathcal{C}) = \langle (x-\gamma_0)^{T_i}\rangle$, where T_i is an integer satisfying $0 \le T_i \le p^s$ for each i. Moreover, we have the followings:

(a) $|\mathrm{Tor}_i(\mathcal{C})| = (p^m)^{p^s - T_i}$.

(b) If $u^i[(x-\gamma_0)^{t_i} + ug(x)] \in \mathcal{C}$, where $g(x) \in \mathcal{R}_\gamma$, then we must have $t_i \ge T_i$.

(c) $p^s \ge T_0 \ge T_1 \ge T_2 \ge 0$.

(d) $|\mathcal{C}| = (p^m)^{3p^s - (T_0+T_1+T_2)}$.

Proof Its proof is similar to that of Theorem 2.2 of Kiah et al. [36]. □

Definition 3.2 Let $\mathcal{C}$ be a γ-constacyclic code of length p^s over $\mathcal{R}$. For each $0 \le i \le 2$, the integer T_i is called the i-th torsional degree of $\mathcal{C}$ and is denoted by $T_i(\mathcal{C})$.

By the above Theorem, Definition 3.1 and our classification in Theorem 3.1, $T_i(\mathcal{C})$ can be readily obtained.

Lemma 3.3 Let $\mathcal{C}$ be a γ-constacyclic code of length p^s over $\mathcal{R}$, as classified in Theorem 3.1. Then, for $0 \le i \le 2$, the i-th torsional degree $T_i(\mathcal{C})$ of $\mathcal{C}$ is determined as follows:

* When $\mathcal{C} = \langle 0\rangle$, then $T_0(\mathcal{C}) = T_1(\mathcal{C}) = T_2(\mathcal{C}) = p^s$.
* When $\mathcal{C} = \langle 1\rangle$, then $T_0(\mathcal{C}) = T_1(\mathcal{C}) = T_2(\mathcal{C}) = 0$.
* When $\mathcal{C} = \langle u^2(x-\gamma_0)^\tau\rangle$ with $0 \le \tau \le p^s - 1$, then

$$T_0(\mathcal{C}) = T_1(\mathcal{C}) = p^s \text{ and } T_2(\mathcal{C}) = \tau.$$

* When $\mathcal{C} = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$ is of the Type 3, then

$$T_0(\mathcal{C}) = p^s,\ T_1(\mathcal{C}) = \delta \text{ and } T_2(\mathcal{C}) = L.$$

* When $\mathcal{C} = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x), u^2(x-\gamma_0)^\omega\rangle$ is of the Type 4, then

$$T_0(\mathcal{C}) = p^s,\ T_1(\mathcal{C}) = \delta \text{ and } T_2(\mathcal{C}) = \omega.$$

* When $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x)\rangle$ is of the Type5, then

$$T_0(\mathcal{C}) = a,\ T_1(\mathcal{C}) = U \text{ and } T_2(\mathcal{C}) = V.$$

* When $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x), u^2(x-\gamma_0)^c\rangle$ is of the Type 6, then

$$T_0(\mathcal{C}) = a,\ T_1(\mathcal{C}) = U \text{ and } T_2(\mathcal{C}) = c.$$

* When $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{\dagger_3}h_3(x)\rangle$ is of the Type 7, then

$$T_0(\mathcal{C}) = a,\ T_1(\mathcal{C}) = b \text{ and } T_2(\mathcal{C}) = W.$$

* When $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{\dagger_3}h_3(x), u^2(x-\gamma_0)^c\rangle$ is of the Type 8, then

$$T_0(\mathcal{C}) = a,\ T_1(\mathcal{C}) = b \text{ and } T_2(\mathcal{C}) = c.$$

By the above Lemma and in light of Theorem 3.2(d), now we can determine the cardinalities of all γ-constacyclic code of length p^s over $\mathcal{R}$.

Theorem 3.3 Let $\mathcal{C}$ be a γ-constacyclic code of length p^s over $\mathcal{R}$. Then following the same notations as in Theorem 3.1, we have the following results:

— If $\mathcal{C} = \langle 0\rangle$, then

$$|\mathcal{C}| = 1.$$

— If $\mathcal{C} = \langle 1\rangle$, then

$$|\mathcal{C}| = p^{3mp^s}.$$

— If $\mathcal{C} = \langle u^2(x-\gamma_0)^\tau\rangle$ with $0 \le \tau \le p^s - 1$, then

$$|\mathcal{C}| = p^{m(p^s-\tau)}.$$

— If $\mathcal{C} = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^{\dagger}h(x)\rangle$ is of the Type3, then

$$|\mathcal{C}| = p^{m(2p^s-\delta-L)}$$
$$= \begin{cases} p^{2m(p^s-\delta)}, & \text{if either } h(x) = 0 \text{ or } h(x) \neq 0 \text{ and } 0 \le \delta \le \dfrac{p^s+t}{2}, \\ p^{m(p^s-t)}, & \text{if } h(x) \neq 0 \text{ and } \dfrac{p^s+t}{2} < \delta \le p^s - 1. \end{cases}$$

— If $\mathcal{C} = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^{\dagger}h(x), u^2(x-\gamma_0)^\omega\rangle$ is of the Type 4, then

$$|\mathcal{C}| = p^{m(2p^s-\delta-\omega)}.$$

— If $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$ is of the Type 5, then

$$|\mathcal{C}| = p^{m(3p^s-a-U-V)}$$
$$= \begin{cases} p^{3m(p^s-a)}, & \text{if } h_1(x)=h_2(x)=0 \\ & \text{or } h_1(x)=0,\ h_2(x)\neq 0 \text{ and } 0<a\leq \dfrac{p^s+t_2}{2} \\ & \text{or } h_1(x)\neq 0 \text{ and } 0<a\leq \dfrac{p^s+t_1}{2}, \\ p^{m(2p^s-a-t_1)}, & \text{if } h_1(x)\neq 0 \text{ and } \dfrac{p^s+t_1}{2}<a\leq p^s-1, \\ p^{m(2p^s-a-t_2)}, & \text{if } h_1(x)=0,\ h_2(x)\neq 0 \text{ and } \dfrac{p^s+t_2}{2}<a\leq p^s-1. \end{cases}$$

— If $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$ is of the Type 6, then

$$|\mathcal{C}| = p^{m(3p^s-a-U-c)}$$
$$= \begin{cases} p^{m(3p^s-2a-c)}, & \text{if } h_1(x)=0 \text{ or } h_1(x)\neq 0 \text{ and } 0<a\leq \dfrac{p^s+t_1}{2}, \\ p^{m(2p^s-t_1-c)}, & \text{if } h_1(x)\neq 0 \text{ and } \dfrac{p^s+t_1}{2}<a\leq p^s-1. \end{cases}$$

— If $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$ is of the Type 7, then

$$|\mathcal{C}| = p^{m(3p^s-a-b-W)}$$
$$= \begin{cases} p^{m(3p^s-a-2b)}, & \text{if } h_1(x)=h_2(x)=h_3(x)=0, \\ & \text{or } h_1(x)\neq 0 \text{ and } h_3(x)=0, \\ & \text{or } h_1(x)=h_3(x)=0,\ h_2(x)\neq 0 \text{ and } 0\leq b\leq p^s-a+t_2, \\ & \text{or } h_1(x)=h_2(x)=0,\ h_3(x)\neq 0 \text{ and } 0\leq b\leq \dfrac{p^s+t_3}{2}, \\ & \text{or } h_1(x)\neq 0,\ h_3(x)\neq 0 \text{ and } 0\leq b\leq \dfrac{p^s+t_3}{2}, \\ & \text{or } h_1(x)=0, h_2(x)\neq 0, h_3(x)\neq 0, 0\leq b\leq \min\{p^s-a+t_2, \dfrac{p^s+t_3}{2}\}, \\ p^{m(2p^s-b-t_2)}, & \text{if } h_1(x)=h_3(x)=0, h_2(x)\neq 0, p^s-a+t_2<b<p^s-1, \\ & \text{or } h_1(x)=0, h_2(x)\neq 0,\ h_3(x)\neq 0 \text{ and } p^s-a+t_2<b\leq a+t_3-t_2, \\ p^{m(2p^s-a-t_3)}, & \text{if } h_1(x)=h_2(x)=0,\ h_3(x)\neq 0 \text{ and } \dfrac{p^s+t_3}{2}<b<p^s-1, \\ & \text{or } h_1(x)\neq 0,\ h_3(x)\neq 0, \text{ and } \dfrac{p^s+t_3}{2}<b<p^s-1, \\ & \text{or } h_1(x)=0, h_2(x)\neq 0, h_3(x)\neq 0, \max\{a+t_3-t_2, \dfrac{p^s+t_3}{2}\}<b<p^s-1. \end{cases}$$

— If $\mathcal{C} = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$ is of the Type 8, then

$$|\mathcal{C}| = p^{m(3p^s-a-b-c)}.$$

3.3 Some examples

In this section, we present some examples of constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m} (u^3 = 0)$.

Example 3.1 γ-constacyclic codes of length 3 over the chain ring $\mathcal{R} = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ are precisely the ideals of $\mathcal{R}[x]/\langle x^3 - \gamma\rangle$, where $\gamma \in \{1, 2\}$.
In the following, we list all distinct γ-constacyclic codes of length 3 over the chain ring $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$. There are 82 distinct γ-constacyclic codes listed below. In all codes we have $h_0, a_0, b_0, c_0 \in \{1, 2\}$ and $b_1 \in \{0, 1, 3\}$.

* Type1($\mathcal{C}_1$): $\langle 0\rangle$, $\langle 1\rangle$.
* Type2($\mathcal{C}_2$):
  - $\tau = 0$: $\langle u^2\rangle$,
  - $\tau = 1$: $\langle u^2(x - \gamma)\rangle$,
  - $\tau = 2$: $\langle u^2(x - \gamma)^2\rangle$.
* Type3($\mathcal{C}_3$):
  - $h(x) = 0$ and $\delta = 0$: $\langle u\rangle$,
  - $h(x) = 0$ and $\delta = 1$: $\langle u(x - \gamma)\rangle$,
  - $h(x) = 0$ and $\delta = 2$: $\langle\langle u(x - \gamma)^2\rangle$,
  - $h(x) \neq 0$, $\delta = 1$ and $t = 0$: $\langle u(x - \gamma) + h_0u^2\rangle$,
  - $h(x) \neq 0$, $\delta = 2$ and $t = 0$: $\langle u(x - \gamma)^2 + h_0u^2\rangle$
  - $h(x) \neq 0$, $\delta = 2$ and $t = 1$: $\langle u(x - \gamma)^2 + h_0u^2(x - \gamma)\rangle$.
* Type4($\mathcal{C}_4$):
  - $h(x) = 0$, $\delta = 1$ and $\omega = 0$: $\langle u(x - \gamma), u^2\rangle$,
  - $h(x) = 0$, $\delta = 2$ and $\omega = 0$: $\langle u(x - \gamma)^2, u^2\rangle$,
  - $h(x) = 0$, $\delta = 2$ and $\omega = 1$: $\langle u(x - \gamma)^2, u^2(x - \gamma)\rangle$.
* Type5($\mathcal{C}_5$):
  - $h_1(x) = h_2(x) = 0$ and $a = 1$: $\langle (x - \gamma)\rangle$,
  - $h_1(x) = h_2(x) = 0$ and $a = 2$: $\langle (x - \gamma)^2\rangle$,
  - $h_1(x) = 0$, $h_2(x) \neq 0$, $a = 1$ and $t_2 = 0$: $\langle (x - \gamma) + b_0u^2\rangle$,
  - $h_1(x) = 0$, $h_2(x) \neq 0$, $a = 2$ and $t_2 = 0$: $\langle (x - \gamma)^2 + b_0u^2\rangle$,
  - $h_1(x) = 0$, $h_2(x) \neq 0$, $a = 2$ and $t_2 = 1$: $\langle (x - \gamma)^2 + b_0u^2(x - \gamma)\rangle$,
  - $h_1(x) \neq 0$, $h_2(x) = 0$, $a = 1$ and $t_1 = 0$: $\langle (x - \gamma) + a_0u\rangle$,
  - $h_1(x) \neq 0$, $h_2(x) = 0$, $a = 2$ and $t_1 = 0$: $\langle (x - \gamma)^2 + a_0u\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) = 0$, $a = 2$ and $t_1 = 1$: $\langle (x-\gamma)^2 + a_0u(x-\gamma)\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) \neq 0$, $a = 1$ and $t_1 = t_2 = 0$: $\langle (x-\gamma) + a_0u + b_0u^2\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) \neq 0$, $a = 2$ and $t_1 = t_2 = 0$: $\langle (x-\gamma)^2 + a_0u + b_0u^2\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) \neq 0$, $a = 2$, $t_1 = 1$ and $t_2 = 0$: $\langle (x-\gamma)^2 + a_0u(x-\gamma) + b_0u^2 + b_1u^2(x-\gamma)\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) \neq 0$, $a = 2$ and $t_1 = t_2 = 1$: $\langle (x-\gamma)^2 + a_0u(x-\gamma) + b_0u^2(x-\gamma)\rangle$.

* Type6 ($\mathcal{C}_6$):

→ $h_1(x) = h_2(x) = 0$, $a = 1$ and $c = 0$: $\langle (x-\gamma), u^2\rangle$,

→ $h_1(x) = h_2(x) = 0$, $a = 2$ and $c = 0$: $\langle (x-\gamma)^2, u^2\rangle$,

→ $h_1(x) = h_2(x) = 0$, $a = 2$ and $c = 1$: $\langle (x-\gamma)^2, u^2(x-\gamma)\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) = 0$, $a = 1$, $t_1 = 0$ and $c = 0$: $\langle (x-\gamma) + a_0u, u^2\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) = 0$, $a = 2$, $t_1 = 0$ and $c = 0$: $\langle (x-\gamma)^2 + a_0u, u^2\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) = 0$, $a = 2$, $t_1 = 1$ and $c = 0$: $\langle (x-\gamma)^2 + a_0u(x-\gamma), u^2\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) = 0$, $a = 2$, $t_1 = 1$ and $c = 1$: $\langle (x-\gamma)^2 + a_0u(x-\gamma), u^2(x-\gamma)\rangle$,

→ $h_1(x) \neq 0$, $h_2(x) \neq 0$, $a = 2$, $t_1 = 1$, $c = 1$ and $t_2 = 0$: $\langle (x-\gamma)^2 + a_0u(x-\gamma) + b_0u^2, u^2(x-\gamma)\rangle$.

* Type7 ($\mathcal{C}_7$):

→ $h_1(x) = h_2(x) = h_3(x) = 0$, $a = 1$ and $b = 0$: $\langle (x-\gamma), u\rangle$,

→ $h_1(x) = h_2(x) = h_3(x) = 0$, $a = 2$ and $b = 0$: $\langle (x-\gamma)^2, u\rangle$,

→ $h_1(x) = h_2(x) = h_3(x) = 0$, $a = 2$ and $b = 1$: $\langle (x-\gamma)^2, u(x-\gamma)\rangle$,

→ $h_1(x) = h_2(x) = 0$, $h_3(x) \neq 0$, $a = 2$, $b = 1$ and $t_3 = 0$: $\langle (x-\gamma)^2, u(x-\gamma) + c_0u^2\rangle$,

→ $h_1(x) = 0$, $h_2(x) \neq 0$, $h_3(x) = 0$, $a = 2$, $b = 1$ and $t_2 = 0$: $\langle (x-\gamma)^2 + b_0u^2, u(x-\gamma)\rangle$,

→ $h_1(x) = 0$, $h_2(x) \neq 0$, $h_3(x) \neq 0$, $a = 2$, $b = 1$, $t_2 = 0$ and $t_3 = 0$: $\langle (x-\gamma)^2 + b_0u^2, u(x-\gamma) + c_0u^2\rangle$.

* Type8 ($\mathcal{C}_8$):

→ $h_1(x) = h_2(x) = h_3(x) = 0$, $a = 2$, $b = 1$ and $c = 0$: $\langle (x-\gamma)^2, u(x-\gamma), u^2\rangle$.

The following Table 3.1 shows the representation of all γ-constacyclic codes $\mathcal{C}$ of length 3 over the chain ring $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, together with the number of codewords $|\mathcal{C}|$ in each of of those constacyclic codes.

Example 3.2 Consider the ring $\mathcal{R} = \mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$. Here $p = 7$, $m = 1$. The units in the ring $\mathcal{R}$ of the form γ are $1, 2, 3, 4, 5, 6$. γ-constacyclic codes of length 49 over $\mathcal{R}$ has eight types of generator. Table 3.2 shows the representation of some γ-constacyclic codes $\mathcal{C}$ of length 49 over the chain ring $\mathcal{R}$, together with the number of codewords $|\mathcal{C}|$ in each of those constacyclic codes.

Table 3.1 – γ-constacyclic codes of length **3** over the chain ring $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$

Type	Ideal$(\mathcal{C})$	$\lvert\mathcal{C}\rvert$
Type 1	$\langle 0\rangle$	1
	$\langle 1\rangle$	19683
Type 2	$\langle u^2\rangle$	27
	$\langle u^2(x-\gamma)\rangle$	9
	$\langle u^2(x-\gamma)^2\rangle$	3
Type 3	$\langle u\rangle$	729
	$\langle u(x-\gamma)\rangle; \langle u(x-\gamma)+h_0u^2\rangle$	81
	$\langle u(x-\gamma)^2\rangle; \langle u(x-\gamma)^2+h_0u^2(x-\gamma)\rangle$	9
	$\langle u(x-\gamma)^2+h_0u^2\rangle$	27
Type 4	$\langle u(x-\gamma), u^2\rangle$	243
	$\langle u(x-\gamma)^2, u^2\rangle$	81
	$\langle u(x-\gamma)^2, u^2(x-\gamma)\rangle$	27
Type 5	$\langle (x-\gamma)\rangle; \langle (x-\gamma)+a_0u\rangle; \langle (x-\gamma)+b_0u^2\rangle; \langle (x-\gamma)+a_0u+b_0u^2\rangle$	729
	$\langle (x-\gamma)^2\rangle; \langle (x-\gamma)^2+a_0u(x-\gamma)\rangle; \langle (x-\gamma)^2+b_0u^2(x-\gamma)\rangle; \langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2\rangle$	27
	$\langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2(x-\gamma)\rangle$	27
	$\langle (x-\gamma)^2+a_0u\rangle; \langle (x-\gamma)^2+b_0u^2\rangle; \langle (x-\gamma)^2+a_0u+b_0u^2\rangle; \langle (x-\gamma)^2+a_0u+b_0u^2(x-\gamma)\rangle$	81
Type 6	$\langle (x-\gamma), u^2\rangle; \langle (x-\gamma)+a_0u, u^2\rangle$	2187
	$\langle (x-\gamma)^2, u^2\rangle; \langle (x-\gamma)^2+a_0u(x-\gamma), u^2\rangle$	243
	$\langle (x-\gamma)^2, u^2(x-\gamma)\rangle; \langle (x-\gamma)^2+a_0u(x-\gamma), u^2(x-\gamma)\rangle; \langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2, u^2(x-\gamma)\rangle$	81
	$\langle (x-\gamma)^2+a_0u, u^2\rangle$	729
Type 7	$\langle (x-\gamma), u\rangle$	6561
	$\langle (x-\gamma)^2, u\rangle$	2187
	$\langle (x-\gamma)^2, u(x-\gamma)\rangle; \langle (x-\gamma)^2, u(x-\gamma)+c_0u^2\rangle; \langle (x-\gamma)^2+b_0u^2, u(x-\gamma)\rangle$	243
	$\langle (x-\gamma)^2+b_0u^2, u(x-\gamma)+c_0u^2\rangle$	243
Type 8	$\langle (x-\gamma)^2, u(x-\gamma), u^2\rangle$	729

Table 3.2 – Some γ-constacyclic codes of length **49** over the chain ring $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Type	Ideal $(\mathcal{C})$	$\lvert\mathcal{C}\rvert$
Type 1	$\langle 0\rangle$	1
	$\langle 1\rangle$	7^{147}
Type 2	$\langle u^2(x-\gamma)^{30}\rangle$	7^{19}
	$\langle u^2(x-\gamma)^{37}\rangle$	7^{12}
	$\langle u^2(x-\gamma)^{48}\rangle$	7
Type 3	$\langle u\rangle$	7^{98}
	$\langle u(x-\gamma)^{30} + h_0u^2(x-\gamma)^{27} + h_1u^2(x-\gamma)^{28} + h_2u^2(x-\gamma)^{29}\rangle$	7^{38}
	$\langle u(x-\gamma)^{47} + h_0u^2(x-\gamma)^{39} + h_1u^2(x-\gamma)^{40}\rangle$	7^{10}
	$\langle u(x-\gamma)^{47} + h_0u^2(x-\gamma)^{45} + h_1u^2(x-\gamma)^{46}\rangle$	7^4
Type 4	$\langle u(x-\gamma)^9, u^2(x-\gamma)\rangle$	7^{88}
	$\langle u(x-\gamma)^{46} + h_0u^2(x-\gamma)^{42} + h_1u^2(x-\gamma)^{43}, u^2(x-\gamma)^{44}\rangle$	7^8
	$\langle u(x-\gamma)^{48}, u^2(x-\gamma)^{47}\rangle$	7^3
Type 5	$\langle (x-\gamma) + a_0u + b_0u^2\rangle$	7^{144}
	$\langle (x-\gamma)^2 + a_0u + a_1u(x-\gamma) + b_0u^2 + b_1u^2(x-\gamma)\rangle$	7^{141}
	$\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{23} + a_1u(x-\gamma)^{24} + b_0u^2(x-\gamma)^{24}\rangle$	7^{50}
	$\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{46} + b_0u^2(x-\gamma)^{45} + b_1u^2(x-\gamma)^{46}\rangle$	7^6
Type 6	$\langle (x-\gamma)^{48} + a_0u(x-\gamma)^{29}, u^2(x-\gamma)^{28}\rangle$	7^{41}
	$\langle (x-\gamma)^{44} + b_0u^2(x-\gamma)^{41}, u^2(x-\gamma)^{42}\rangle$	7^{17}
	$\langle (x-\gamma)^{48} + a_0u(x-\gamma)^{47} + b_0u^2(x-\gamma)^{42} + b_1u^2(x-\gamma)^{43}, u^2(x-\gamma)^{44}\rangle$	7^7
	$\langle (x-\gamma)^{48}, u^2(x-\gamma)^{47}\rangle$	7^4
Type 7	$\langle (x-\gamma)^{30}, u(x-\gamma)^6\rangle$	7^{105}
	$\langle (x-\gamma)^{31} + a_0u(x-\gamma)^{18} + a_1u(x-\gamma)^{19}, u(x-\gamma)^{20}\rangle$	7^{76}
	$\langle (x-\gamma)^{48}, u(x-\gamma)^{47} + c_0u^2(x-\gamma)^{41} + c_1u^2(x-\gamma)^{42}\rangle$	7^5
	$\langle (x-\gamma)^{46}, u(x-\gamma)^{44}\rangle$	7^{13}
	$\langle (x-\gamma)^{47} + b_0u^2(x-\gamma)^{43} + b_1u^2(x-\gamma)^{44}, u(x-\gamma)^{46}\rangle$	7^9
Type 8	$\langle (x-\gamma)^{30} + a_0u(x-\gamma)^{14}, u(x-\gamma)^{15}, u^2\rangle$	7^{102}
	$\langle (x-\gamma)^{27} + b_0u^2, u(x-\gamma)^{13} + c_0u^2, u^2(x-\gamma)\rangle$	7^{106}
	$\langle (x-\gamma)^{39} + a_0u(x-\gamma)^{18} + a_1u(x-\gamma)^{19}, u(x-\gamma)^{20} + c_0u^2(x-\gamma)^7, u^2(x-\gamma)^8\rangle$	7^{80}
	$\langle (x-\gamma)^{34}, u(x-\gamma)^{29} + c_0u^2(x-\gamma)^{24} + c_1u^2(x-\gamma)^{25}, u^2(x-\gamma)^{26}\rangle$	7^{58}
	$\langle (x-\gamma)^{48}, u(x-\gamma)^{47}, u^2(x-\gamma)^{46}\rangle$	7^6

Chapter 4

Hamming distance distributions of repeated-root γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$

4.1 Introduction

Throughout this chapter, let p be a prime, s, m be positive integers, γ be a nonzero element of the finite field $\mathbb{F}_{p^m}$, and let $\mathcal{R} = \mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$, $u^3 = 0$ be a finite commutative ring with p^{3m} elements.

In this chapter, using generator polynomial structures of γ-constacyclic codes of length p^s over $\mathcal{R}$, the Hamming distance distributions of all such codes are completely determined. Apart from this, we derive necessary and sufficient conditions under which a γ-constacyclic code of length p^s over $\mathcal{R}$ is maximum distance separable (MDS) with respect to the Hamming distance.

This chapter is structured as follows: In Section 4.2, we obtain Hamming distances of all γ-constacyclic codes of length p^s over $\mathcal{R}$. As applications, in Section 4.3, we identify all maximum distance saparable codes (i.e., optimal codes with respect to the Singleton bound) among them. Section 4.4 contains some examples in which we discuss the parameter of some MDS constacyclic Hamming codes for different values of p and s.

4.2 Hamming distance

In this section, we will determine Hamming distances of all γ-constacyclic codes of length p^s over $\mathcal{R}$. Note that $\mathbb{F}_{p^m}$ is a subring of $\mathcal{R}$, for a code $\mathcal{C}$ over $\mathcal{R}$, we denote $d_H(\mathcal{C}_{\mathbb{F}})$ as the Hamming distance of $\mathcal{C}|_{\mathbb{F}_{p^m}}$.

As we mentioned in Section 3.2 the γ-constacyclic codes of length p^s over $\mathcal{R}$ are precisely the ideals of the ring $\mathcal{R}_\gamma$. In order to compute the Hamming distances of all γ-constacyclic codes of length p^s over $\mathcal{R}$, we count the Hamming distance of the ideals of the ring $\mathcal{R}_\gamma$ as classified into 8 types in Theorem 3.1. The following results can be found in [28].

Obviously, the trivial ideals $\langle 0\rangle$, $\langle 1\rangle$ reside in Type 1, and hence, their Hamming distances are given by 0 and 1, respectively.

The Hamming distance of Type 2 γ-constacyclic codes can be determined as follows:

Theorem 4.1 Let $\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 2 (as classified in Theorem 3.1), where $0 \le \tau \le p^s-1$. Then the Hamming distance of $\mathcal{C}_2$ is given by

$$\begin{aligned} d_H(\mathcal{C}_2) &= d_H(\langle (x-\gamma_0)^\tau\rangle_{\mathbb{F}}) \\ &= \mathcal{H}_\tau \\ &= \begin{cases} \bullet\ 1, & \text{if } \tau = 0, \\ \bullet\ (n+1)p^k, & \text{if } p^s - pr + (n-1)r + 1 \le \tau \le p^s - pr + nr, \\ & \text{where } r = p^{s-k-1},\ 1 \le n \le p-1 \text{ and } 0 \le k \le s-1. \end{cases} \end{aligned}$$

Proof For a code $\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle$ of Type 2, $0 \le \tau \le p^s-1$, the codewords of $\mathcal{C}_2$ are precisely the codewords of the γ-constacyclic codes $\langle (x-\gamma_0)^\tau\rangle$ in $\mathbb{F}_{p^m}[x]/\langle x^{p^s}-\gamma\rangle$ multiplied by u^2. Therefore $d_H(\mathcal{C}_2) = d_H(\langle (x-\gamma_0)^\tau\rangle_{\mathbb{F}})$, which are given in Theorem 2.3. □

In order to compute the Hamming distances of those codes for the rest cases (Type 3, 4, 5, 6, 7 and 8), we first observe that

$$wt_H(a(x)) \ge wt_H(ua(x)), \quad \text{where } a(x) \in \mathcal{R}_\gamma. \tag{4.1}$$

Now, we discuss the Hamming distance of Type 3 γ-constacyclic codes of length p^s.

Theorem 4.2 Let $\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 3 (as classified in Theorem 3.1). Then the Hamming distance of $\mathcal{C}_3$ is given by

$$\begin{aligned} d_H(\mathcal{C}_3) &= d_H(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}) \\ &= \mathcal{H}_L \\ &= \begin{cases} \bullet\, 1, & \text{if } L = 0, \\ \bullet\, (n+1)p^k, & \text{if } p^s - pr + (n-1)r + 1 \le L \le p^s - pr + nr, \\ & \text{where } r = p^{s-k-1},\ 1 \le n \le p-1 \text{ and } 0 \le k \le s-1. \end{cases} \end{aligned}$$

Proof Let $\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$ be of Type3. And let $c(x)$ be an arbitrary nonzero element of $\mathcal{C}_3$. That means there exist $f_0(x), f_u(x), f_{u^2}(x) \in \mathbb{F}_{p^m}[x]$ such that

$$c(x) = [f_0(x) + uf_u(x) + u^2 f_{u^2}(x)][u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)].$$

Thus, $uc(x) = u^2 f_0(x)(x-\gamma_0)^\delta$. By (4.1), we obtain that

$$\begin{aligned} wt_H(c(x)) &\ge wt_H(uc(x)) \\ &= wt_H(u^2 f_0(x)(x-\gamma_0)^\delta) \\ &\ge d_H(\langle u^2(x-\gamma_0)^\delta\rangle) \\ &= d_H(\langle (x-\gamma_0)^\delta\rangle_{\mathbb{F}}). \end{aligned}$$

Since, $\langle (x-\gamma_0)^\delta\rangle \subseteq \langle (x-\gamma_0)^L\rangle$, we have $d_H(\langle (x-\gamma_0)^\delta\rangle_{\mathbb{F}}) \ge d_H(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}})$. From this, we get $wt_H(c(x)) \ge d_H(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}})$ for each $c(x)$ nonzero element of $\mathcal{C}_3$. This implies that

$$d_H(\mathcal{C}_3) \ge d_H(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}). \tag{4.2}$$

On the other hand we have that

$$\langle u^2(x-\gamma_0)^L\rangle \subseteq \mathcal{C}_3,$$

which implies that

$$d_H(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}) = d_H(\langle u^2(x-\gamma_0)^L\rangle) \ge d_H(\mathcal{C}_3). \tag{4.3}$$

Now by (4.2) and (4.3), we get

$$d_H(\mathcal{C}_3) = d_H(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}).$$

Now by applying Theorem 2.3, we get the desired result. □

Next, we compute the Hamming distance of Type 4 γ-constacyclic codes as follows:

Theorem 4.3 Let $\mathcal{C}_4 = \langle u(x-\gamma_0)^{\delta} + u^2(x-\gamma_0)^{\dagger}h(x), u^2(x-\gamma_0)^{\omega}\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 4 (as classified in Theorem 3.1). Then the Hamming distance of $\mathcal{C}_4$ is given by

$$\begin{aligned} d_H(\mathcal{C}_4) &= d_H(\langle (x-\gamma_0)^{\omega}\rangle_{\mathbb{F}}) \\ &= \mathcal{H}_{\omega} \\ &= \begin{cases} \bullet\, 1, & \text{if } \omega = 0, \\ \bullet\, (n+1)p^k, & \text{if } p^s - pr + (n-1)r + 1 \le \omega \le p^s - pr + nr, \\ & \text{where } r = p^{s-k-1},\ 1 \le n \le p-1 \text{ and } 0 \le k \le s-1. \end{cases} \end{aligned}$$

Proof As $u^2(x-\gamma_0)^{\omega} \in \mathcal{C}_4$, we have

$$d_H(\mathcal{C}_4) \le d_H(\langle u^2(x-\gamma_0)^{\omega}\rangle) = d_H(\langle (x-\gamma_0)^{\omega}\rangle_{\mathbb{F}}).$$

Now, consider an arbitrary polynomial $c(x) \in \mathcal{C}_4 \setminus \langle u^2(x-\gamma_0)^{\omega}\rangle$. Thus, by (4.1), we see that

$$\begin{aligned} wt_H(c(x)) &\ge wt_H(uc(x)) \\ &\ge d_H(\langle u^2(x-\gamma_0)^{\delta}\rangle) \\ &= d_H(\langle (x-\gamma_0)^{\delta}\rangle_{\mathbb{F}}) \\ &\ge d_H(\langle (x-\gamma_0)^{\omega}\rangle_{\mathbb{F}}). \end{aligned}$$

From this, we obtain $d_H(\langle (x-\gamma_0)^{\omega}\rangle_{\mathbb{F}}) \le d_H(\mathcal{C}_4)$, which implies that

$$d_H(\mathcal{C}_4) = d_H(\langle (x-\gamma_0)^{\omega}\rangle_{\mathbb{F}}).$$

Now by applying Theorem 2.3, we get the desired result. □

The Hamming distance of Type 5 γ-constacyclic codes can be determined as follows:

Theorem 4.4 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 5 (as classified in Theorem 3.1). Then the Hamming distance of $\mathcal{C}_5$ is given by

$$\begin{aligned} d_H(\mathcal{C}_5) &= d_H(\langle (x-\gamma_0)^{V}\rangle_{\mathbb{F}}) \\ &= \mathcal{H}_V \\ &= (n+1)p^k, \end{aligned}$$

where $p^s - pr + (n-1)r + 1 \le V \le p^s - pr + nr$, $r = p^{s-k-1}$, $1 \le n \le p-1$ and $0 \le k \le s-1$.

Proof First of all, since $\langle u^2(x-\gamma_0)^V\rangle \subseteq \mathcal{C}_5$, it follows that

$$d_H(\mathcal{C}_5) \le d_H(\langle u^2(x-\gamma_0)^V\rangle) = d_H(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}).$$

Now, let c(x) be an arbitrary nonzero element of $\mathcal{C}_5$. Thus, by (4.1), we obtain that

$$\begin{aligned} wt_H(c(x)) &\ge wt_H(u^2c(x)) \\ &\ge d_H(\langle u^2(x-\gamma_0)^a\rangle) \\ &= d_H(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}). \end{aligned}$$

Since, $\langle (x-\gamma_0)^a\rangle \subseteq \langle (x-\gamma_0)^V\rangle$, we have

$$d_H(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \ge d_H(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}).$$

Hence, $d_H(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}) \le d_H(\mathcal{C}_5)$. This implies that

$$d_H(\mathcal{C}_5) = d_H(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}).$$

Finally, by the above assertion and by applying Theorem 2.3, we get the desired result.

□

Now, we discuss the Hamming distance of Type6 γ-constacyclic codes of length p^s.

Theorem 4.5 Let $\mathcal{C}_6 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 6 (as classified in Theorem 3.1). Then the Hamming distance of $\mathcal{C}_6$ is given by

$$\begin{aligned} d_H(\mathcal{C}_6) &= d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \\ &= \mathcal{H}_c \\ &= \begin{cases} \bullet\ 1, & \text{if } c = 0, \\ \bullet\ (n+1)p^k, & \text{if } p^s - pr + (n-1)r + 1 \le c \le p^s - pr + nr, \\ & \text{where } r = p^{s-k-1},\ 1 \le n \le p-1 \text{ and } 0 \le k \le s-1. \end{cases} \end{aligned}$$

Proof As $u^2(x-\gamma_0)^c \in \mathcal{C}_6$, we have

$$d_H(\mathcal{C}_6) \le d_H(\langle u^2(x-\gamma_0)^c\rangle) = d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}).$$

Now, let us take an arbitrary polynomial $c(x) \in \mathcal{C}_6 \setminus \langle u^2(x-\gamma_0)^c\rangle$. Thus, by (4.1), we see that

$$\begin{aligned} wt_H(c(x)) &\geq wt_H(u^2c(x)) \\ &\geq d_H(\langle u^2(x-\gamma_0)^a\rangle) \\ &= d_H(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \\ &\geq d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}). \end{aligned}$$

From this, we get $d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \leq d_H(\mathcal{C}_6)$, which implies that

$$d_H(\mathcal{C}_6) = d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}).$$

The rest of the proof follows from Theorem 2.3 and the discussion above. □

The Hamming distance of Type 7 γ-constacyclic codes can be determined as follows:

Theorem 4.6 Let $\mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 7 (as classified in Theorem 3.1). Then the Hamming distance of $\mathcal{C}_7$ is given by

$$\begin{aligned} d_H(\mathcal{C}_7) &= d_H(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}) \\ &= \mathcal{H}_W \\ &= \begin{cases} \bullet\ 1, & \text{if } W = 0, \\ \bullet\ (n+1)p^k, & \text{if } p^s - pr + (n-1)r + 1 \leq W \leq p^s - pr + nr, \\ & \text{where } r = p^{s-k-1},\ 1 \leq n \leq p-1 \text{ and } 0 \leq k \leq s-1. \end{cases} \end{aligned}$$

Proof Since $u^2(x-\gamma_0)^W \in \mathcal{C}_7$, we have

$$d_H(\mathcal{C}_7) \leq d_H(\langle u^2(x-\gamma_0)^W\rangle) = d_H(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}).$$

Now, let $c(x)$ be an arbitrary nonzero element of $\mathcal{C}_7$. We consider two cases.

* Case 1: $c(x) \in \langle u\rangle$. In this case, by (4.1). We have

$$\begin{aligned} wt_H(c(x)) &\geq wt_H(uc(x)) \\ &\geq d_H(\langle u^2(x-\gamma_0)^b\rangle) \\ &= d_H(\langle (x-\gamma_0)^b\rangle_{\mathbb{F}}). \end{aligned}$$

$*$ Case 2: $c(x) \notin \langle u\rangle$. In this case, by (4.1). We have

$$\begin{aligned} wt_H(c(x)) &\geq wt_H(u^2c(x)) \\ &\geq d_H(\langle u^2(x-\gamma_0)^a\rangle) \\ &= d_H(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}). \end{aligned}$$

Since, $\langle (x-\gamma_0)^a\rangle \subseteq \langle (x-\gamma_0)^b\rangle \subseteq \langle (x-\gamma_0)^W\rangle$, we have

$$d_H(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \geq d_H(\langle (x-\gamma_0)^b\rangle_{\mathbb{F}}) \geq d_H(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}).$$

Hence, $d_H(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}) \leq d_H(\mathcal{C}_7)$, forcing

$$d_H(\mathcal{C}_7) = d_H(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}).$$

Now by applying Theorem 2.3, we get the desired result. □

Next, we compute the Hamming distance of Type 8 γ-constacyclic codes as follows:

Theorem 4.7 Let $\mathcal{C}_8 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{\dagger_3}h_3(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 8 (as classified in Theorem 3.1). Then the Hamming distance of $\mathcal{C}_8$ is given by

$$\begin{aligned} d_H(\mathcal{C}_8) &= d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \\ &= \mathcal{H}_c \\ &= \begin{cases} \bullet\ 1, & \text{if } c = 0, \\ \bullet\ (n+1)p^k, & \text{if } p^s - pr + (n-1)r + 1 \leq c \leq p^s - pr + nr, \\ & \text{where } r = p^{s-k-1},\ 1 \leq n \leq p-1 \text{ and } 0 \leq k \leq s-1. \end{cases} \end{aligned}$$

Proof As $u^2(x-\gamma_0)^c \in \mathcal{C}_8$, we have

$$d_H(\mathcal{C}_8) \leq d_H(\langle u^2(x-\gamma_0)^c\rangle) = d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}).$$

Now, consider an arbitrary polynomial $c(x) \in \mathcal{C}_8 \setminus \langle u^2(x-\gamma_0)^c\rangle$. We consider two cases.

$*$ Case 1: $c(x) \in \langle u\rangle$. In this case, by (4.1). We have

$$\begin{aligned} wt_H(c(x)) &\geq wt_H(uc(x)) \\ &\geq d_H(\langle u^2(x-\gamma_0)^b\rangle) \\ &= d_H(\langle (x-\gamma_0)^b\rangle_{\mathbb{F}}) \\ &\geq d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}). \end{aligned}$$

∗ Case 2: $c(x) \notin \langle u\rangle$. In this case, by (4.1). We have

$$\begin{aligned} wt_H(c(x)) &\geq wt_H(u^2c(x)) \\ &\geq d_H(\langle u^2(x-\gamma_0)^a\rangle) \\ &= d_H(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \\ &\geq d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}). \end{aligned}$$

Hence, by combining both the cases, we get $d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \leq d_H(\mathcal{C}_8)$, which implies that

$$d_H(\mathcal{C}_8) = d_H(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}).$$

Finally, by the above assertion and by applying Theorem 2.3, we get the desired result.

□

4.3 MDS codes with respect to Hamming distance

In this Section, we identify the MDS codes for each type of γ-constacyclic codes one by one. First, we consider the γ-constacyclic codes of length p^s of Type 1.

Theorem 4.8 Let $\mathcal{C}_1$ be a γ-constacyclic code of length p^s over $\mathcal{R}$ of Type 1 (as classified in Theorem 3.1), then the only MDS code is $\langle 1\rangle$.

Proof Case 1: If $\mathcal{C}_1 = \langle 0\rangle$, then the Hamming distance is $d_H(\mathcal{C}_1) = 0$. Thus by (2.1), we see that the code $\mathcal{C}_1$ is an MDS code if and only if $|\mathcal{C}_1| = p^{3m(p^s-d_H(\mathcal{C}_1)+1)}$, i.e., $1 = p^{3m(p^s+1)}$, i.e., $p^s+1 = 0$, which is not true for any p and s.

Case 2: If $\mathcal{C}_1 = \langle 1\rangle$, then $d_H(\mathcal{C}_1) = 1$. Thus by (2.1), $\mathcal{C}_1$ is an MDS code if and only if $|\mathcal{C}_1| = p^{3m(p^s-d_H(\mathcal{C}_1)+1)}$, i.e., $p^{3mp^s} = p^{3m(p^s-1+1)}$, which is true for all p and s. Thus, the code $\mathcal{C}_1$ is MDS in this case. □

Now we examine the MDS condition for Type 2 γ-constacyclic codes.

Theorem 4.9 Let $\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 2 (as classified in Theorem 3.1), where $0 \leq \tau \leq p^s-1$. Then no MDS codes exist.

Proof To prove the result, we note, by Theorem 3.3, that $|\mathcal{C}_2| = p^{m(p^s-\tau)}$. From this and by (2.1), we see that the code $\mathcal{C}_2$ is an MDS code if and only if $p^{m(p^s-\tau)} = p^{3m(p^s-d_H(\mathcal{C}_2)+1)}$, i.e., $\tau = 3d_H(\mathcal{C}_2) - 2p^s - 3$. We consider two cases as follows:

Case 1: If $\tau = 0$, then $d_H(\mathcal{C}_2) = 1$. For $\mathcal{C}_2$ to be MDS we must have, $p^s = 0$, which is not true for any p and s. Thus, $\mathcal{C}_2$ is not MDS for $\tau = 0$.

Case 2: If $p^s - pr + (n-1)r + 1 \le \tau \le p^s - pr + nr$, where $r = p^{s-k-1}$, $1 \le n \le p-1$ and $0 \le k \le s-1$. Then we have Hamming distance $d_H(\mathcal{C}_2) = (n+1)p^k$.

Now,

$$\begin{aligned}
\tau &\ge p^s - p^{s-k} + (n-1)p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + (n-1)p^{s-k-1} + 1 \\
&\ge p(3p^k - 1) - 2p^s + (n-1) + 1 \\
&\ge (n+1)(3p^k - 1) - 2p^s + n \\
&= 3(n+1)p^k - 2p^s - 1 \\
&> 3(n+1)p^k - 2p^s - 3 \\
&= 3d_H(\mathcal{C}_2) - 2p^s - 3.
\end{aligned}$$

Since, $\tau > 3d_H(\mathcal{C}_2) - 2p^s - 3$, no MDS code exists in this case. □

Here, we consider the γ-constacyclic codes of Type 3 to verify the MDS condition for these codes. We note, by Theorem 3.3, that $|\mathcal{C}_3| = p^{m(2p^s-\delta-L)}$. From this and by (2.1), we see that the code $\mathcal{C}_3$ is an MDS code if and only if $p^{m(2p^s-\delta-L)} = p^{3m(p^s-d_H(\mathcal{C}_3)+1)}$, which holds if and only if $L = 3d_H(\mathcal{C}_3) - p^s - \delta - 3$. Hence, follows the theorem.

Theorem 4.10 Let $\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 3 (as classified in Theorem 3.1). Then, there is no MDS code.

Proof We consider two cases as follows:

Case 1: If $L = 0$, then $d_H(\mathcal{C}_3) = 1$. For $\mathcal{C}_3$ to be MDS we must have, $\delta = -p^s$, which is not true for any p and s. Thus, $\mathcal{C}_3$ is not MDS for $L = 0$.

Case 2: If $p^s - pr + (n-1)r + 1 \le L \le p^s - pr + nr$, where $r = p^{s-k-1}$, $1 \le n \le p-1$ and $0 \le k \le s-1$. Then we have Hamming distance $d_H(\mathcal{C}_3) = (n+1)p^k$.

Now,

$$\begin{aligned}
L &\geq p^s - p^{s-k} + (n-1)p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + (n-1)p^{s-k-1} + 1 \\
&\geq p(3p^k - 1) - 2p^s + (n-1) + 1 \\
&\quad \times (\text{equality when } k = s-1, \text{or } s = 1) \\
&\geq (n+1)(3p^k - 1) - 2p^s + n \\
&\quad \times (\text{equality when } n = p-1) \\
&= 3(n+1)p^k - 2p^s - 1 \\
&= 3d_H(\mathcal{C}_3) - 2p^s - 1.
\end{aligned}$$

Now, $L \geq 3d_H(\mathcal{C}_3) - p^s - \delta - 3$ if and only if $\delta \geq p^s - 2$, i.e., equality when $\delta = p^s - 2$. Thus, equality occurs when $n = p-1, k = s-1, \delta = p^s-2$, i.e., $L = p^s-1$, which is a contradiction, since $L \leq \delta$. Thus, there is no MDS code in this case. □

Now we examine the MDS condition for Type4 γ-constacyclic codes.

Theorem 4.11 Let $\mathcal{C}_4 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x), u^2(x-\gamma_0)^\omega\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type4 (as classified in Theorem 3.1). Then, there is no MDS code.

Proof Here, by Theorem 3.3, we have $|\mathcal{C}_4| = p^{m(2p^s-\delta-\omega)}$. So, by (2.1), $\mathcal{C}_4$ is an MDS code if and only if $p^{m(2p^s-\delta-\omega)} = p^{3m(p^s-d_H(\mathcal{C}_4)+1)}$, i.e., $\omega = 3d_H(\mathcal{C}_4) - p^s - 3 - \delta$. We consider two cases as follows:

Case 1: If $\omega = 0$, then $d_H(\mathcal{C}_4) = 1$. For $\mathcal{C}_4$ to be MDS we must have, $\delta = -p^s$, which is a contradiction, since $1 \leq \delta \leq p^s - 1$. Thus, $\mathcal{C}_4$ is not MDS for $\omega = 0$.

Case 2: If $p^s - pr + (n-1)r + 1 \leq \omega \leq p^s - pr + nr$, where $r = p^{s-k-1}$, $1 \leq n \leq p-1$ and $0 \leq k \leq s-1$. Then we have Hamming distance $d_H(\mathcal{C}_4) = (n+1)p^k$. For $\mathcal{C}_4$ to be MDS we must have $\omega = 3d_H(\mathcal{C}_4) - p^s - 3 - \delta$. Let $\delta = p^s - m$, where $1 \leq m \leq p^s - 1$. Thus, the condition for $\mathcal{C}_4$ to be an MDS constacyclic code becomes $\omega = 3d_H(\mathcal{C}_4) - 2p^s - 3 + m$.

Now,

$$\begin{aligned}
\omega &\geq p^s - p^{s-k} + (n-1)p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + (n-1)p^{s-k-1} + 1 \\
&\geq p(3p^k - 1) - 2p^s + (n-1) + 1 \\
&\quad \times (\text{equality when } k = s-1, \text{or } s = 1) \\
&\geq (n+1)(3p^k - 1) - 2p^s + n \\
&\quad \times (\text{equality when } n = p-1) \\
&= 3(n+1)p^k - 2p^s - 1 \\
&= 3d_H(\mathcal{C}_4) - 2p^s - 1.
\end{aligned}$$

Now, $\omega \geq 3d_H(\mathcal{C}_4) - 2p^s - 3 + m$ if and only if $2 \geq m$, i.e., equality when $m = 2$. Thus, equality occurs when $n = p-1, k = s-1, m = 2$, i.e., $\delta = p^s - 2$ and $\omega = p^s - 1$, which is a contradiction, since $\omega < \delta$. Thus, there is no MDS code in this case. □

Now we examine the MDS condition for Type5 γ-constacyclic codes. By Theorem 3.3, we have $|\mathcal{C}_5| = p^{m(3p^s-a-U-V)}$. From this and by (2.1), we see that the code $\mathcal{C}_5$ is an MDS code if and only if $p^{m(3p^s-a-U-V)} = p^{3m(p^s-d_H(\mathcal{C}_5)+1)}$, which holds if and only if $V = 3d_H(\mathcal{C}_5) - a - U - 3$. Thus, we get the following cases:

Case 1: When $h_1(x) = h_2(x) = 0$ then, $V = U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = d_H(\mathcal{C}_5) - 1$. Hence, the MDS codes for Type5 ideals are similar to the MDS γ-constacyclic codes over $\mathbb{F}_{p^m}$ (see Theorem 2.4). Hence, we have the following theorem:

Theorem 4.12 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a \rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type5 (as classified in Theorem 3.1). Then $\mathcal{C}_5$ is an MDS constacyclic code if and only if one of the following conditions holds:

- If $s = 1$ then $a = n$ for $1 \leq n \leq p-1$, in such case, $d_H(\mathcal{C}_5) = n+1$.
- If $s \geq 2$, then
  - $a = 1$, in such case, $d_H(\mathcal{C}_5) = 2$,
  - $a = p^s - 1$, in such case, $d_H(\mathcal{C}_5) = p^s$.

Case 2: When $h_1(x) = 0, h_2(x) \neq 0$ and $1 \leq a \leq \frac{p^s + t_2}{2}$ then, $V = U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = d_H(\mathcal{C}_5) - 1$, which is similar to the result in case 1. But we have $1 \leq a \leq \frac{p^s + t_2}{2}$ and $0 \leq t_2 < a$, which implies that $\max\{2a - p^s, 0\} \leq t_2 < a$. Hence, we conclude the following theorem.

Theorem 4.13 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u^2(x-\gamma_0)^{t_2} h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type5 (as classified in Theorem 3.1), where $h_2(x) \neq 0$ and $1 \leq a \leq \frac{p^s + t_2}{2}$. Then $\mathcal{C}_5$ is an MDS constacyclic code if and only if one of the following conditions holds:

- If $s = 1$, $a = n$, $1 \leq n \leq p-1$ and $\max\{2n - p, 0\} \leq t_2 < n$, then $d_H(\mathcal{C}_5) = n + 1$.
- If $s \geq 2$,
  - $a = 1$ and $t_2 = 0$, then $d_H(\mathcal{C}_5) = 2$,
  - $a = p^s - 1$ and $t_2 = p^s - 2$, then $d_H(\mathcal{C}_5) = p^s$.

Case 3: When $h_1(x) \neq 0$ and $1 \leq a \leq \frac{p^s + t_1}{2}$ then, $V = U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = d_H(\mathcal{C}_5) - 1$, which is similar to the result in case 1. But we have $1 \leq a \leq \frac{p^s + t_1}{2}$ and $0 \leq t_1 < a$, which implies that $\max\{2a - p^s, 0\} \leq t_1 < a$. Hence, we conclude the following theorem.

Theorem 4.14 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1} h_1(x) + u^2(x-\gamma_0)^{t_2} h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 5 (as classified in Theorem 3.1), where $h_1(x) \neq 0$ and $1 \leq a \leq \frac{p^s + t_1}{2}$. Then $\mathcal{C}_5$ is an MDS constacyclic code if and only if one of the following conditions holds:

- If $s = 1$, $a = n$, $1 \leq n \leq p-1$ and $\max\{2n - p, 0\} \leq t_1 < n$, then $d_H(\mathcal{C}_5) = n + 1$.
- If $s \geq 2$,
  - $a = 1$ and $t_1 = 0$, then $d_H(\mathcal{C}_5) = 2$,
  - $a = p^s - 1$ and $t_1 = p^s - 2$, then $d_H(\mathcal{C}_5) = p^s$.

Case 4: When $h_1(x) \neq 0$ and $\frac{p^s + t_1}{2} < a \leq p^s - 1$ then, $V = U = p^s - a + t_1$. For $\mathcal{C}_5$ to be MDS we must have $a = 2p^s - 3d_H(\mathcal{C}_5) + 2t_1 + 3$. Hence, follows the theorem.

Theorem 4.15 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1} h_1(x) + u^2(x-\gamma_0)^{t_2} h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type5 (as classified in Theorem 3.1), where $h_1(x) \neq 0$ and $\frac{p^s + t_1}{2} < a \leq p^s - 1$. Then, there is no MDS code.

Proof When $h_1(x) \neq 0$ and $\frac{p^s + t_1}{2} < a \leq p^s - 1$, then $V = p^s - a + t_1$. If $p^s - pr + (n-1)r + 1 \leq p^s - a + t_1 \leq p^s - pr + nr$, i.e., $t_1 + pr - nr \leq a \leq t_1 + pr - (n-1)r - 1$, where $r = p^{s-k-1}$, $1 \leq n \leq p-1$ and $0 \leq k \leq s-1$. Then we have Hamming distance $d_H(\mathcal{C}_5) = (n+1)p^k$. We get MDS code for $a = 2p^s - 3d_H(\mathcal{C}_5) + 2t_1 + 3$.

Now,

$$\begin{aligned}
a &\geq t_1 + p^{s-k} - np^{s-k-1} \\
&= t_1 + p^{s-k-1}(p-n) \\
&\geq t_1 + (p-n) \\
&\quad \times (\text{equality when } k = s-1, \text{or } s = 1) \\
&\geq t_1 + 1 \\
&\quad \times (\text{equality when } n = p-1) \\
&= -3(n+1)p^k + t_1 + 1 + 3(n+1)p^k \\
&\geq -3(n+1)p^k + t_1 + 1 + 3(n+1) \\
&\quad \times (\text{equality when } k = 0) \\
&\geq -3(n+1)p^k + t_1 + 7 \\
&\quad \times (\text{equality when } n = 1) \\
&= -3d_H(\mathcal{C}_5) + t_1 + 7.
\end{aligned}$$

Now, $a \geq 2p^s - 3d_H(\mathcal{C}_5) + 2t_1 + 3$ if and only if $-2p^s + 4 \geq t_1$, i.e., equality when $t_1 = -2p^s + 4$. Thus, equality occurs when $n = 1, k = 0, s = 1, p = 2$ and $t_1 = 0$, i.e., $a = 1$, which is a contradiction, since $1 = \frac{2^1 + 0}{2} < a$. Thus, there is no MDS code in this case. □

Case 5: When $h_1(x) = 0, h_2(x) \neq 0$ and $\frac{p^s + t_2}{2} < a \leq p^s - 1$ then, $V = p^s - a + t_2$ and $U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = 3d_H(\mathcal{C}_5) - p^s - t_2 - 3$. Hence, follows the theorem.

Theorem 4.16 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u^2(x-\gamma_0)^{t_2} h_2(x) \rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 5 (as classified in Theorem 3.1), where $h_2(x) \neq 0$ and $\frac{p^s + t_2}{2} < a \leq p^s - 1$. Then, there is no MDS code.

Proof When $h_1(x) = 0, h_2(x) \neq 0$ and $\frac{p^s + t_2}{2} < a \leq p^s - 1$, then $V = p^s - a + t_2$. If $p^s - pr + (n-1)r + 1 \leq p^s - a + t_2 \leq p^s - pr + nr$, i.e., $t_2 + pr - nr \leq a \leq t_2 + pr - (n-1)r - 1$, where $r = p^{s-k-1}$, $1 \leq n \leq p-1$ and $0 \leq k \leq s-1$. Then we have Hamming distance $d_H(\mathcal{C}_5) = (n+1)p^k$. We get MDS code for $a = 3d_H(\mathcal{C}_5) - p^s - t_2 - 3$.

Now,

$$\begin{aligned} a &\geq t_2 + p^{s-k} - np^{s-k-1} \\ &= t_2 + p^{s-k-1}(p-n) \\ &\geq t_2 + 1 \\ &= 3(n+1)p^k + t_2 + 1 - 3(n+1)p^k \\ &\geq 3(n+1)p^k + t_2 + 1 - 3p^s \\ &= 3d_H(\mathcal{C}_5) + t_2 + 1 - 3p^s. \end{aligned}$$

Now, $a \geq 3d_H(\mathcal{C}_5) - p^s - t_2 - 3$ if and only if $t_2 \geq p^s - 2$, i.e., equality when $t_2 = p^s - 2$, i.e., $\frac{p^s + p^s - 2}{2} < a \leq p^s - 1$, i.e., $p^s - 1 < a \leq p^s - 1$, which is a contradiction. Thus, there is no MDS code in this case. □

Here, we consider the γ-constacyclic codes of Type6 to verify the MDS condition for these codes.

Theorem 4.17 Let $\mathcal{C}_6 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type6 (as classified in Theorem 3.1). Then, there is no MDS code.

Proof To prove the result, we note, by Theorem 3.3, that $|\mathcal{C}_6| = p^{m(3p^s-a-U-c)}$. From this and by (2.1), we see that the code $\mathcal{C}_6$ is an MDS code if and only if $p^{m(3p^s-a-U-c)} = p^{3m(p^s-d_H(\mathcal{C}_6)+1)}$, i.e., $c = 3d_H(\mathcal{C}_6) - U - a - 3$. We consider two cases as follows:

Case 1: If $c = 0$, then $d_H(\mathcal{C}_6) = 1$. For $\mathcal{C}_6$ to be MDS we must have, $a = -U$, which is contradiction, since $0 < U \leq a$.

Case 2: If $p^s - pr + (n-1)r + 1 \leq c \leq p^s - pr + nr$, where $r = p^{s-k-1}$, $1 \leq n \leq p-1$ and $0 \leq k \leq s-1$. Then we have Hamming distance $d_H(\mathcal{C}_6) = (n+1)p^k$. We have the following subcases:

Subcase 2.1: When $h_1(x) = 0$ or $h_1(x) \neq 0$ and $0 < a \leq \frac{p^s + t_1}{2}$, then $U = a$. So, $\mathcal{C}_6$ is MDS code if and only if $c = 3d_H(\mathcal{C}_6) - 2a - 3$. Now,

$$\begin{aligned}
c &\geq p^s - p^{s-k} + (n-1)p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + (n-1)p^{s-k-1} + 1 \\
&\geq p(3p^k - 1) - 2p^s + (n-1) + 1 \\
&\quad \times (\text{equality when } k = s-1, \text{or } s = 1) \\
&\geq (n+1)(3p^k - 1) - 2p^s + n \\
&\quad \times (\text{equality when } n = p-1) \\
&= 3(n+1)p^k - 2p^s - 1 \\
&= 3d_H(\mathcal{C}_6) - 2p^s - 1.
\end{aligned}$$

Now, $c \geq 3d_H(\mathcal{C}_6) - 2a - 3$ if and only if $a \geq p^s - 1$, i.e., equality when $a = p^s - 1$. Thus, equality occurs when $n = p-1, k = s-1, a = p^s - 1$, i.e., $c = p^s - 1$, which is a contradiction, since $c < a$. Thus, there is no MDS code in this case.

Subcase 2.2: When $h_1(x) \neq 0$ and $\frac{p^s + t_1}{2} < a \leq p^s - 1$, then $U = p^s - a + t_1$. So, $\mathcal{C}_6$ is an MDS code if and only if $c = 3d_H(\mathcal{C}_6) - p^s - t_1 - 3$.

Now,

$$\begin{aligned}
c &\geq p^s - p^{s-k} + (n-1)p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + (n-1)p^{s-k-1} + 1 \\
&\geq p(3p^k - 1) - 2p^s + (n-1) + 1 \\
&\quad \times (\text{equality when } k = s-1, \text{or } s = 1) \\
&\geq (n+1)(3p^k - 1) - 2p^s + n \\
&\quad \times (\text{equality when } n = p-1) \\
&= 3(n+1)p^k - 2p^s - 1 \\
&= 3d_H(\mathcal{C}_6) - 2p^s - 1.
\end{aligned}$$

Now, $c \geq 3d_H(\mathcal{C}_6) - p^s - t_1 - 3$ if and only if $t_1 \geq p^s - 2$, i.e., equality when $t_1 = p^s - 2$, i.e., $\frac{p^s + p^s - 2}{2} < a \leq p^s - 1$, i.e., $p^s - 1 < a \leq p^s - 1$, which is a contradiction. Thus, there is no MDS code in this case. □

Now we examine the MDS condition for Type 7 γ-constacyclic codes. By Theorem 3.3, we have $|\mathcal{C}_7| = p^{m(3p^s-a-b-W)}$. From this and by (2.1), we see that the code $\mathcal{C}_7$ is an MDS code if and only if $p^{m(3p^s-a-b-W)} = p^{3m(p^s-d_H(\mathcal{C}_7)+1)}$, which holds if and only if $W = 3d_H(\mathcal{C}_7) - b - a - 3$.

Theorem 4.18 Let $\mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 7 (as classified in Theorem 3.1). Then, there is no MDS code.

Proof Case 1: If $W = 0$, then $d_H(\mathcal{C}_7) = 1$. For $\mathcal{C}_7$ to be MDS we must have, $a = -b$, which is contradiction, since $0 \le b < a$. Thus, $\mathcal{C}_7$ is not MDS for $W = 0$.

Case 2: If $p^s - pr + (n-1)r + 1 \le W \le p^s - pr + nr$, where $r = p^{s-k-1}$, $1 \le n \le p-1$ and $0 \le k \le s-1$. Then we have Hamming distance $d_H(\mathcal{C}_7) = (n+1)p^k$.

Now,

$$\begin{aligned}
W &\ge p^s - p^{s-k} + (n-1)p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + (n-1)p^{s-k-1} + 1 \\
&\ge p(3p^k - 1) - 2p^s + (n-1) + 1 \\
&\quad \times (\text{equality when } k = s-1, \text{or } s = 1) \\
&\ge (n+1)(3p^k - 1) - 2p^s + n \\
&\quad \times (\text{equality when } n = p-1) \\
&= 3(n+1)p^k - 2p^s - 1 \\
&= 3d_H(\mathcal{C}_7) - 2p^s - 1.
\end{aligned}$$

Now, $W \ge 3d_H(\mathcal{C}_7) - b - a - 3$ if and only if $a + b \ge 2p^s - 2$, i.e., equality when $a + b = 2p^s - 2$. Thus, equality occurs when $n = p-1, k = s-1, a+b = 2p^s - 2$, i.e., $W = p^s - 1$, which is a contradiction, since $W < p^s - 1$. Thus, there is no MDS code in this case. □

Finally, we explore the MDS γ-constacyclic codes of Type 8.

Theorem 4.19 Let $\mathcal{C}_8 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 8 (as classified in Theorem 3.1). Then, there is no MDS code.

Proof To prove the result, we note, by Theorem 3.3, that $|\mathcal{C}_8| = p^{m(3p^s-a-b-c)}$. From this and by (2.1), we see that the code $\mathcal{C}_8$ is an MDS code if and only if $p^{m(3p^s-a-b-c)} = p^{3m(p^s-d_H(\mathcal{C}_8)+1)}$, i.e., $c = 3d_H(\mathcal{C}_8) - b - a - 3$. We consider two cases as follows:

Case 1: If $c = 0$, then $d_H(\mathcal{C}_8) = 1$. For $\mathcal{C}_8$ to be MDS we must have $a = -b$, which is contradiction, since $0 \le b < a$. Thus, $\mathcal{C}_8$ is not MDS for $c = 0$.

Case 2: If $p^s - pr + (n-1)r + 1 \le c \le p^s - pr + nr$, where $r = p^{s-k-1}$, $1 \le n \le p-1$ and $0 \le k \le s-1$. Then we have Hamming distance $d_H(\mathcal{C}_8) = (n+1)p^k$. Now,

$$\begin{aligned}
c &\ge p^s - p^{s-k} + (n-1)p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + (n-1)p^{s-k-1} + 1 \\
&\ge p(3p^k - 1) - 2p^s + (n-1) + 1 \\
&\quad \times (\text{equality when } k = s-1, \text{or } s = 1) \\
&\ge (n+1)(3p^k - 1) - 2p^s + n \\
&\quad \times (\text{equality when } n = p-1) \\
&= 3(n+1)p^k - 2p^s - 1 \\
&= 3d_H(\mathcal{C}_8) - 2p^s - 1.
\end{aligned}$$

Now, $c \ge 3d_H(\mathcal{C}_8) - b - a - 3$ if and only if $a + b \ge 2p^s - 2$, i.e., equality when $a + b = 2p^s - 2$. Thus, equality occurs when $n = p-1, k = s-1, a+b = 2p^s - 2$, i.e., $c = p^s - 1$, which is a contradiction, since $c < p^s - 1$. Thus, there is no MDS code in this case. □

4.4 Some examples

In this section, we present some examples of Hamming distance distributions of constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m} (u^3 = 0)$.

Example 4.1 Using the results in Sections 4.2 and 4.3, we list all Hamming distances d_H of all γ-constacyclic codes $\mathcal{C}$ of length 3 over the chain ring $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, where $\gamma \in \{1, 2\}$. We also give all MDS and non-MDS codes (Table 4.1). Among these 82 codes, 31 of them are MDS codes. In all codes we have $h_0, a_0, b_0, c_0 \in \{1, 2\}$ and $b_1 \in \{0, 1, 3\}$.

Example 4.2 Let $\mathcal{R} = \mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$, where $u^3 = 0$. Recall that for a $\gamma \in \mathbb{F}_7^*$, a γ-constacyclic code of length of length 49 over the chain ring $\mathcal{R}$ is an ideal of the quotient ring $\mathcal{R}[x]/\langle x^{49} - \gamma\rangle$. Different generators of the constacyclic codes and their corresponding conditions to be MDS codes are given as follows:

- Type 1 ($\mathcal{C}_1$) : $\langle 0\rangle$, $\langle 1\rangle$. For these codes the condition for MDS code are given by $3 = d_H(C_1)$ and $1 = d_H(C_1)$.
  As mentioned in Section 4.3, the only MDS constacyclic codes in this case is $\langle 1\rangle$.
- Type 2: $\mathcal{C}_2 = \langle u^2(x-\gamma)^\tau\rangle$, where $0 \le \tau \le 48$. The condition for MDS code is given by $\tau = 3d_H(C_2) - 101$. MDS constacyclic codes are non-existent in this case.
- Type 3: $\mathcal{C}_3 = \langle u(x-\gamma)^\delta + u^2(x-\gamma)^t h(x)\rangle$, where $0 \le \delta \le 48$, $0 \le t < \delta$, either $h(x)$ is 0 or a unit in $\mathcal{R}_\gamma$. The condition for MDS code is given by $L = 3d_H(C_3) - \delta - 52$. No MDS constacyclic code can be obtained in this case.
- Type 4: $\mathcal{C}_4 = \langle u(x-\gamma)^\delta + u^2(x-\gamma)^t h(x), u^2(x-\gamma)^\omega\rangle$, where $0 \le \omega < \delta \le 48$, $0 \le t < \omega$, either $h(x)$ is 0 or a unit in $\mathcal{R}_\gamma$. The condition for MDS code is given by $\omega = 3d_H(C_4) - \delta - 52$. No MDS constacyclic code can be obtained in this case.
- Type 5: $\mathcal{C}_5 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1} h_1(x) + u^2(x-\gamma)^{t_2} h_2(x)\rangle$, where $1 \le a \le 48$, $0 \le t_1 < a$, $0 \le t_2 < a$, either $h_1(x), h_2(x)$ are 0 or are units in $\mathcal{R}_\gamma$. The condition for MDS code is given by $V = 3d_H(C_5) - a - U - 3$ and all the distinct MDS codes are given by:
  - $\langle (x-\gamma)\rangle$
  - $\langle (x-\gamma)^{48}\rangle$,
  - $\langle (x-\gamma) + b_0u^2\rangle$,
  - $\langle (x-\gamma)^{48} + b_0u^2(x-\gamma)^{47}\rangle$,
  - $\langle (x-\gamma) + a_0u\rangle$,
  - $\langle (x-\gamma) + a_0u + b_0u^2\rangle$,

- $\langle (x-\gamma)^{48} + a_0u(x-\gamma)^{47}\rangle$,
- $\langle (x-\gamma)^{48} + a_0u(x-\gamma)^{47} + u^2(x-\gamma)^{t_2}\sum_{j=0}^{47-t_2} b_j(x-\gamma)^j\rangle$,

where $0 \le t_2 \le 47$, $a_0, b_0 \in \{1,\dots,6\}$ and $b_j \in \{0,1,\dots,6\}$.

We present γ-constacyclic codes of Type5 $\{h_1(x) = h_2(x) = 0\}$ in Table 4.2, together with the Hamming distances d_H of such codes. We also give all MDS and non-MDS codes.

— Type6: $\mathcal{C}_6 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1}h_1(x) + u^2(x-\gamma)^{t_2}h_2(x), u^2(x-\gamma)^c\rangle$, where $0 \le c < a \le 48$, $0 \le t_1 < a$, $0 \le t_2 < c$, either $h_1(x), h_2(x)$ are 0 or are units in $\mathcal{R}_\gamma$. The condition for MDS code is given by $c = 3d_H(\mathcal{C}_6) - a - U - 3$. No MDS constacyclic code can be obtained in this case.

— Type7: $\mathcal{C}_7 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1}h_1(x) + u^2(x-\gamma)^{t_2}h_2(x), u(x-\gamma)^b + u^2(x-\gamma)^{t_3}h_3(x)\rangle$, where $0 \le b < a \le 48$, $0 \le t_1 < b$, $0 \le t_2 < b$, $0 \le t_3 < b$, either $h_1(x), h_2(x), h_3(x)$ are 0 or are units in $\mathcal{R}_\gamma$. The condition for MDS code is given by $W = 3d_H(\mathcal{C}_7) - b - a - 3$. No MDS constacyclic code can be obtained in this case.

— Type8: $\mathcal{C}_8 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1}h_1(x) + u^2(x-\gamma)^{t_2}h_2(x), u(x-\gamma)^b + u^2(x-\gamma)^{t_3}h_3(x), u^2(x-\gamma)^c\rangle$, where $0 \le c < b < a \le 48$, $0 \le t_1 < b$, $0 \le t_2 < c$, $0 \le t_3 < c$, either $h_1(x), h_2(x), h_3(x)$ are 0 or are units in $\mathcal{R}_\gamma$. The condition for MDS code is given by $c = 3d_H(\mathcal{C}_8) - b - a - 3$. No MDS constacyclic code can be obtained in this case.

Table 4.1 – Hamming distance of γ-constacyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$

Ideal $(\mathcal{C})$	d_H	MDS
$\rightarrow$ Type 1 :		
$*\langle 0\rangle$	0	No
$*\langle 1\rangle$	1	Yes
$\rightarrow$ Type 2 :		
$*\langle u^2\rangle$	1	No
$*\langle u^2(x-\gamma)\rangle$	2	No
$*\langle u^2(x-\gamma)^2\rangle$	3	No
$\rightarrow$ Type 3 :		
$*\langle u\rangle$	1	No
$*\langle u(x-\gamma)\rangle$; $*\langle u(x-\gamma)+h_0u^2\rangle$; $*\langle u(x-\gamma)^2+h_0u^2\rangle$	2	No
$*\langle u(x-\gamma)^2\rangle$;$*\langle u(x-\gamma)^2+h_0u^2(x-\gamma)\rangle$	3	No
$\rightarrow$ Type 4 :		
$*\langle u(x-\gamma),u^2\rangle$; $*\langle u(x-\gamma)^2,u^2\rangle$	1	No
$*\langle u(x-\gamma)^2,u^2(x-\gamma)\rangle$	2	No
$\rightarrow$ Type 5 :		
$*\langle (x-\gamma)\rangle$; $*\langle (x-\gamma)+b_0u^2\rangle$; $*\langle (x-\gamma)+a_0u\rangle$; $*\langle (x-\gamma)+a_0u+b_0u^2\rangle$	2	Yes
$*\langle (x-\gamma)^2\rangle$; $*\langle (x-\gamma)^2+b_0u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2(x-\gamma)\rangle$	3	Yes
$*\langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2+b_1u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma)\rangle$	3	Yes
$*\langle (x-\gamma)^2+b_0u^2\rangle$; $*\langle (x-\gamma)^2+a_0u\rangle$; $*\langle (x-\gamma)^2+a_0u+b_0u^2\rangle$	2	No
$\rightarrow$ Type 6 :		
$*\langle (x-\gamma),u^2\rangle$; $*\langle (x-\gamma)^2,u^2\rangle$; $*\langle (x-\gamma)+a_0u,u^2\rangle$; $*\langle (x-\gamma)^2+a_0u,u^2\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma),u^2\rangle$	1	No
$*\langle (x-\gamma)^2,u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma),u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2,u^2(x-\gamma)\rangle$	2	No
$\rightarrow$ Type 7 :		
$*\langle (x-\gamma),u\rangle$; $*\langle (x-\gamma)^2,u\rangle$	1	No
$*\langle (x-\gamma)^2,u(x-\gamma)\rangle$; $*\langle (x-\gamma)^2,u(x-\gamma)+c_0u^2\rangle$	2	No
$*\langle (x-\gamma)^2+b_0u^2,u(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+b_0u^2,u(x-\gamma)+c_0u^2\rangle$	2	No
$\rightarrow$ Type 8 :		
$*\langle (x-\gamma)^2,u(x-\gamma),u^2\rangle$	1	No

Table 4.2 – Hamming distance of γ-constacyclic codes of **Type5** over $\mathbb{F}_7 + \mathbf{u}\mathbb{F}_7 + \mathbf{u^2}\mathbb{F}_7$.

Ideal($\mathcal{C}$)	d_H	MDS
$*\langle(x-\gamma)\rangle$	2	Yes
$*\langle(x-\gamma)^2\rangle$; $*\langle(x-\gamma)^3\rangle$; $*\langle(x-\gamma)^4\rangle$; $*\langle(x-\gamma)^5\rangle$; $*\langle(x-\gamma)^6\rangle$; $*\langle(x-\gamma)^7\rangle$	2	No
$*\langle(x-\gamma)^8\rangle$; $*\langle(x-\gamma)^9\rangle$; $*\langle(x-\gamma)^{10}\rangle$; $*\langle(x-\gamma)^{11}\rangle$; $*\langle(x-\gamma)^{12}\rangle$; $*\langle(x-\gamma)^{13}\rangle$;$*\langle(x-\gamma)^{14}\rangle$	3	No
$*\langle(x-\gamma)^{15}\rangle$; $*\langle(x-\gamma)^{16}\rangle$; $*\langle(x-\gamma)^{17}\rangle$; $*\langle(x-\gamma)^{18}\rangle$; $*\langle(x-\gamma)^{19}\rangle$; $*\langle(x-\gamma)^{20}\rangle$; $*\langle(x-\gamma)^{21}\rangle$	4	No
$*\langle(x-\gamma)^{22}\rangle$; $*\langle(x-\gamma)^{23}\rangle$; $*\langle(x-\gamma)^{24}\rangle$; $*\langle(x-\gamma)^{25}\rangle$; $*\langle(x-\gamma)^{26}\rangle$; $*\langle(x-\gamma)^{27}\rangle$; $*\langle(x-\gamma)^{28}\rangle$	5	No
$*\langle(x-\gamma)^{29}\rangle$; $*\langle(x-\gamma)^{30}\rangle$; $*\langle(x-\gamma)^{31}\rangle$; $*\langle(x-\gamma)^{32}\rangle$; $*\langle(x-\gamma)^{33}\rangle$; $*\langle(x-\gamma)^{34}\rangle$; $*\langle(x-\gamma)^{35}\rangle$	6	No
$*\langle(x-\gamma)^{36}\rangle$; $*\langle(x-\gamma)^{37}\rangle$; $*\langle(x-\gamma)^{38}\rangle$; $*\langle(x-\gamma)^{39}\rangle$; $*\langle(x-\gamma)^{40}\rangle$; $*\langle(x-\gamma)^{41}\rangle$; $*\langle(x-\gamma)^{42}\rangle$	7	No
$*\langle(x-\gamma)^{43}\rangle$	14	No
$*\langle(x-\gamma)^{44}\rangle$	21	No
$*\langle(x-\gamma)^{45}\rangle$	28	No
$*\langle(x-\gamma)^{46}\rangle$	35	No
$*\langle(x-\gamma)^{47}\rangle$	42	No
$*\langle(x-\gamma)^{48}\rangle$	49	Yes

Chapter 5

Symbol-pair distance distributions of repeated-root γ-constacyclic codes of prime power lengths over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$

5.1 Introduction

In this chapter, using generator polynomial structures of γ-constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$, the symbol-pair distance distributions of all such codes are completely determined. Apart from this, we derive necessary and sufficient conditions under which a γ-constacyclic code of length p^s over $\mathcal{R}$ is maximum distance separable (MDS) with respect to the symbol-pair distance.

For this, throughout this chapter, let p be a prime, s, m be positive integers, γ be a nonzero element of the finite field $\mathbb{F}_{p^m}$, and let $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3\rangle$ be the finite commutative chain ring with unity.

This chapter is structured as follows: In Section 5.2, we obtain symbol-pair distances of all γ-constacyclic codes of length p^s over $\mathcal{R}$. Using these results, in Section 5.3, we shall identify all MDS symbol-pair codes within this class of codes. Section 5.4 contains some examples in which we discuss the parameter of some MDS constacyclic symbol-pair codes for different values of p and s.

5.2 Symbol-pair distance

In this section, we aim to determine the symbol-pair distances of all γ-constacyclic codes of length p^s over $\mathcal{R}$. Obviously, we know that $\mathbb{F}_{p^m}$ is a subring of $\mathcal{R}$. From now, we will denote $d_{sp}(\mathcal{C}_{\mathbb{F}})$ as the symbol-pair distance of the code $\mathcal{C}$ over $\mathbb{F}_{p^m}$.

Our technique in Section 4.2 can also be extended to compute the symbol-pair distance of the ideals of the ring $\mathcal{R}_\gamma$. Now, we determine the symbol-pair distance for each type of γ-constacyclic codes of length p^s one by one. The following results can be found in [14].

Type 1 consists of the trivial ideals. It is easy to see that $d_{sp}(\mathcal{C}_1) = 0$ when $\mathcal{C}_1 = \{0\}$, while $d_{sp}(\mathcal{C}_1) = 2$ when $\mathcal{C}_1 = \{1\}$.

For a code $\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle$ of Type 2, $0 \le \tau \le p^s-1$, the codewords of $\mathcal{C}_2$ are precisely the codewords of the γ-constacyclic codes $\langle (x-\gamma_0)^\tau\rangle$ in $\mathbb{F}_{p^m}[x]/\langle x^{p^s}-\gamma\rangle$ multiplied by u^2. Therefore $d_{sp}(\mathcal{C}_2) = d_{sp}(\langle (x-\gamma_0)^\tau\rangle_{\mathbb{F}})$, which are given in Theorem 2.5.

Theorem 5.1 Let $\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 2 (as classified in Theorem 3.1), where $0 \le \tau \le p^s-1$. Then the symbol-pair distance $d_{sp}(\mathcal{C}_2)$ of the code $\mathcal{C}_2$ is given by

$$
\begin{aligned}
d_{sp}(\mathcal{C}_2) &= d_{sp}(\langle (x-\gamma_0)^\tau\rangle_{\mathbb{F}}) \\
&= \mathcal{S}_\tau \\
&= \begin{cases}
\bullet\ 2, & \text{if } \tau = 0, \\
\bullet\ 3p^k, & \text{if } \tau = p^s - p^{s-k}+1, \text{ where } 0 \le k \le s-2, \\
\bullet\ 4p^k, & \text{if } p^s - p^{s-k}+2 \le \tau \le p^s - p^{s-k}+p^{s-k-1}, \\
& \quad \text{where } 0 \le k \le s-2, \\
\bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr + \sigma r + 1 \le \tau \le p^s - pr + (\sigma+1)r, \\
& \quad \text{where } r = p^{s-k-1},\ 0 \le k \le s-2 \text{ and } 1 \le \sigma \le p-2, \\
\bullet\ (\sigma+2)p^{s-1}, & \text{if } \tau = p^s - p + \sigma, \text{ where } 0 \le \sigma \le p-2, \\
\bullet\ p^s, & \text{if } \tau = p^s - 1.
\end{cases}
\end{aligned}
$$

Now, we are going to determine the symbol-pair distance distribution of those codes for the rest cases (Type 3, 4, 5, 6, 7 and 8). We first observe that

$$\mathrm{wt}_{sp}(a(x)) \ge \mathrm{wt}_{sp}(ua(x)), \quad \text{for each } a(x) \in \mathcal{R}_\gamma. \tag{5.1}$$

The symbol-pair distance of Type3 γ-constacyclic codes can be determined as follows:

Theorem 5.2 Let $\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type3 (as classified in Theorem 3.1). Then the symbol-pair distance $d_{sp}(\mathcal{C}_3)$ of $\mathcal{C}_3$ is given by

$$
\begin{aligned}
d_{sp}(\mathcal{C}_3) &= d_{sp}(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}) \\
&= \mathcal{S}_L \\
&= \begin{cases}
\bullet\ 2, & \text{if } L = 0, \\
\bullet\ 3p^k, & \text{if } L = p^s - p^{s-k} + 1, \text{ where } 0 \le k \le s-2, \\
\bullet\ 4p^k, & \text{if } p^s - p^{s-k} + 2 \le L \le p^s - p^{s-k} + p^{s-k-1}, \\
 & \text{where } 0 \le k \le s-2, \\
\bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr + \sigma r + 1 \le L \le p^s - pr + (\sigma+1)r, \\
 & \text{where } r = p^{s-k-1},\ 0 \le k \le s-2 \text{ and } 1 \le \sigma \le p-2, \\
\bullet\ (\sigma+2)p^{s-1}, & \text{if } L = p^s - p + \sigma, \text{ where } 0 \le \sigma \le p-2, \\
\bullet\ p^s, & \text{if } L = p^s - 1.
\end{cases}
\end{aligned}
$$

Proof Let $\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x)\rangle$ be of Type3. And let $c(x)$ be an arbitrary nonzero element of $\mathcal{C}_3$. Thus, by (5.1), we obtain that

$$
\begin{aligned}
wt_{sp}(c(x)) &\ge wt_{sp}(uc(x)) \\
&\ge d_{sp}(\langle u^2(x-\gamma_0)^\delta\rangle) \\
&= d_{sp}(\langle (x-\gamma_0)^\delta\rangle_{\mathbb{F}}).
\end{aligned}
$$

Since, $\langle (x-\gamma_0)^\delta\rangle \subseteq \langle (x-\gamma_0)^L\rangle$, we have

$$d_{sp}(\langle (x-\gamma_0)^\delta\rangle_{\mathbb{F}}) \ge d_{sp}(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}).$$

From this, we get $wt_{sp}(c(x)) \ge d_{sp}(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}})$ for each $c(x)$ nonzero element of $\mathcal{C}_3$. This implies that

$$d_{sp}(\mathcal{C}_3) \ge d_{sp}(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}). \tag{5.2}$$

On the other hand we have that

$$\langle u^2(x-\gamma_0)^L\rangle \subseteq \mathcal{C}_3,$$

which implies that

$$d_{sp}(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}) = d_{sp}(\langle u^2(x-\gamma_0)^L\rangle) \ge d_{sp}(\mathcal{C}_3). \tag{5.3}$$

Now by (5.2) and (5.3), we get

$$d_{sp}(\mathcal{C}_3) = d_{sp}(\langle (x-\gamma_0)^L\rangle_{\mathbb{F}}).$$

Finally, by the above assertion and by applying Theorem 2.5, we get the desired result.

□

Now, we discuss the symbol-pair distance of Type4 γ-constacyclic codes of length p^s.

Theorem 5.3 Let $\mathcal{C}_4 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x), u^2(x-\gamma_0)^\omega\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type4 (as classified in Theorem 3.1). Then the symbol-pair distance $d_{sp}(\mathcal{C}_4)$ of $\mathcal{C}_4$ is given by

$$\begin{aligned} d_{sp}(\mathcal{C}_4) &= d_{sp}(\langle (x-\gamma_0)^\omega\rangle_{\mathbb{F}}) \\ &= \mathcal{S}_\omega \\ &= \begin{cases} \bullet\ 2, & \text{if } \omega = 0, \\ \bullet\ 3p^k, & \text{if } \omega = p^s - p^{s-k} + 1, \text{ where } 0 \le k \le s-2, \\ \bullet\ 4p^k, & \text{if } p^s - p^{s-k} + 2 \le \omega \le p^s - p^{s-k} + p^{s-k-1}, \\ & \text{where } 0 \le k \le s-2, \\ \bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr + \sigma r + 1 \le \omega \le p^s - pr + (\sigma+1)r, \\ & \text{where } r = p^{s-k-1},\ 0 \le k \le s-2 \text{ and } 1 \le \sigma \le p-2, \\ \bullet\ (\sigma+2)p^{s-1}, & \text{if } \omega = p^s - p + \sigma, \text{ where } 0 \le \sigma \le p-2. \end{cases} \end{aligned}$$

Proof Let $\mathcal{C}_4 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^\dagger h(x), u^2(x-\gamma_0)^\omega\rangle$ be of Type4. And consider an arbitrary polynomial $c(x) \in \mathcal{C}_4 \setminus \langle u^2(x-\gamma_0)^\omega\rangle$. Here by (4.1), we note that

$$\begin{aligned} wt_{sp}(c(x)) &\ge wt_{sp}(uc(x)) \\ &\ge d_{sp}(\langle u^2(x-\gamma_0)^\delta\rangle) \\ &= d_{sp}(\langle (x-\gamma_0)^\delta\rangle_{\mathbb{F}}) \\ &\ge d_{sp}(\langle (x-\gamma_0)^\omega\rangle_{\mathbb{F}}). \end{aligned}$$

From this, we get $d_{sp}(\langle (x-\gamma_0)^\omega\rangle_{\mathbb{F}}) \le d_{sp}(\mathcal{C}_4)$.

Since

$$\langle u^2(x-\gamma_0)^\omega\rangle \subseteq \mathcal{C}_4,$$

we have $d_{sp}(\mathcal{C}_4) \le d_{sp}(\langle u^2(x-\gamma_0)^\omega\rangle) = d_{sp}(\langle (x-\gamma_0)^\omega\rangle_{\mathbb{F}})$. This implies that $d_{sp}(\mathcal{C}_4) = d_{sp}(\langle (x-\gamma_0)^\omega\rangle_{\mathbb{F}})$. The rest of the proof follows from Theorem 2.3 and the discussion above. □

Next, we compute the symbol-pair distance of Type5 γ-constacyclic codes as follows:

Theorem 5.4 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1} h_1(x) + u^2(x-\gamma_0)^{\dagger_2} h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type5 (as classified in Theorem 3.1). Then the symbol-pair distance $d_{sp}(\mathcal{C}_5)$ of $\mathcal{C}_5$ is given by

$$
\begin{aligned}
d_{sp}(\mathcal{C}_5) &= d_{sp}(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}) \\
&= \mathcal{S}_V \\
&= \begin{cases}
\bullet\ 3p^k, & \text{if } V = p^s - p^{s-k} + 1, \text{ where } 0 \le k \le s-2, \\
\bullet\ 4p^k, & \text{if } p^s - p^{s-k} + 2 \le V \le p^s - p^{s-k} + p^{s-k-1}, \\
 & \text{where } 0 \le k \le s-2, \\
\bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr + \sigma r + 1 \le V \le p^s - pr + (\sigma+1)r, \\
 & \text{where } r = p^{s-k-1},\ 0 \le k \le s-2 \text{ and } 1 \le \sigma \le p-2, \\
\bullet\ (\sigma+2)p^{s-1}, & \text{if } V = p^s - p + \sigma, \text{ where } 0 \le \sigma \le p-2, \\
\bullet\ p^s, & \text{if } V = p^s - 1.
\end{cases}
\end{aligned}
$$

Proof Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1} h_1(x) + u^2(x-\gamma_0)^{\dagger_2} h_2(x)\rangle$ be of Type5. Now for each nonzero $c(x) \in \mathcal{C}_5$, by (4.1), we see that

$$
\begin{aligned}
wt_{sp}(c(x)) &\ge wt_{sp}(u^2 c(x)) \\
&\ge d_{sp}(\langle u^2(x-\gamma_0)^a\rangle) \\
&= d_{sp}(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}).
\end{aligned}
$$

Since, $\langle (x-\gamma_0)^a\rangle \subseteq \langle (x-\gamma_0)^V\rangle$, we have

$$d_{sp}(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \ge d_{sp}(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}).$$

This implies that

$$d_{sp}(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}) \le d_{sp}(\mathcal{C}_5).$$

On the other hand we have that

$$u^2(x-\gamma_0)^V \in \mathcal{C}_5,$$

then $d_{sp}(\mathcal{C}_5) \le d_{sp}(\langle u^2(x-\gamma_0)^V\rangle) = d_{sp}(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}})$ and we get $d_{sp}(\mathcal{C}_5) = d_{sp}(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}})$. Now by applying Theorem 2.5, we get the desired result. □

The symbol-pair distance of Type6 γ-constacyclic codes can be determined as follows:

Theorem 5.5 Let $\mathcal{C}_6 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type6 (as classified in Theorem 3.1). Then the symbol-pair distance $d_{sp}(\mathcal{C}_6)$ of $\mathcal{C}_6$ is given by

$$
\begin{aligned}
d_{sp}(\mathcal{C}_6) &= d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \\
&= \mathcal{S}_c \\
&= \begin{cases}
\bullet\ 2, & \text{if } c = 0, \\
\bullet\ 3p^k, & \text{if } c = p^s - p^{s-k} + 1, \text{ where } 0 \le k \le s-2, \\
\bullet\ 4p^k, & \text{if } p^s - p^{s-k} + 2 \le c \le p^s - p^{s-k} + p^{s-k-1}, \\
& \text{where } 0 \le k \le s-2, \\
\bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr + \sigma r + 1 \le c \le p^s - pr + (\sigma+1)r, \\
& \text{where } r = p^{s-k-1},\ 0 \le k \le s-2 \text{ and } 1 \le \sigma \le p-2, \\
\bullet\ (\sigma+2)p^{s-1}, & \text{if } c = p^s - p + \sigma, \text{ where } 0 \le \sigma \le p-2.
\end{cases}
\end{aligned}
$$

Proof Let $\mathcal{C}_6 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$ be of Type6. For each $c(x) \in \mathcal{C}_6 \setminus \langle u^2(x-\gamma_0)^c\rangle$, by (5.1), we obtain that

$$
\begin{aligned}
wt_{sp}(c(x)) &\ge wt_{sp}(u^2c(x)) \\
&\ge d_{sp}(\langle u^2(x-\gamma_0)^a\rangle) \\
&= d_{sp}(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \\
&\ge d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}).
\end{aligned}
$$

This implies that

$$d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \le d_{sp}(\mathcal{C}_6).$$

On the other hand, as

$$u^2(x-\gamma_0)^c \in \mathcal{C}_6,$$

we have $d_{sp}(\mathcal{C}_6) \le d_{sp}(\langle u^2(x-\gamma_0)^c\rangle) = d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}})$, which implies that

$$d_{sp}(\mathcal{C}_6) = d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}).$$

From this and by Theorem 2.5, the desired result follows. □

Now, we discuss the symbol-pair distance of Type7 γ-constacyclic codes of length p^s.

Theorem 5.6 Let $\mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{\dagger_3}h_3(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type7 (as classified in Theorem 3.1). Then the symbol-pair distance $d_{sp}(\mathcal{C}_7)$ of $\mathcal{C}_7$ is given by

$$
\begin{aligned}
d_{sp}(\mathcal{C}_7) &= d_{sp}(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}) \\
&= \mathcal{S}_W \\
&= \begin{cases}
\bullet\ 2, & \text{if } W = 0, \\
\bullet\ 3p^k, & \text{if } W = p^s - p^{s-k} + 1, \text{ where } 0 \le k \le s-2, \\
\bullet\ 4p^k, & \text{if } p^s - p^{s-k} + 2 \le W \le p^s - p^{s-k} + p^{s-k-1}, \\
& \text{where } 0 \le k \le s-2, \\
\bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr + \sigma r + 1 \le W \le p^s - pr + (\sigma+1)r, \\
& \text{where } r = p^{s-k-1},\ 0 \le k \le s-2 \text{ and } 1 \le \sigma \le p-2, \\
\bullet\ (\sigma+2)p^{s-1}, & \text{if } W = p^s - p + \sigma, \text{ where } 0 \le \sigma \le p-2.
\end{cases}
\end{aligned}
$$

Proof Let $\mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{\dagger_1}h_1(x) + u^2(x-\gamma_0)^{\dagger_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{\dagger_3}h_3(x)\rangle$ be of Type7. First of all, since $u^2(x-\gamma_0)^W \in \mathcal{C}_7$, it follows that

$$d_{sp}(\mathcal{C}_7) \le d_{sp}(\langle u^2(x-\gamma_0)^W\rangle) = d_{sp}(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}).$$

Now, let $c(x)$ be an arbitrary nonzero element of $\mathcal{C}_7$. We consider two cases.

* Case 1: $c(x) \in \langle u\rangle$. In this case, by (4.1). We have

$$
\begin{aligned}
wt_{sp}(c(x)) &\ge wt_{sp}(uc(x)) \\
&\ge d_{sp}(\langle u^2(x-\gamma_0)^b\rangle) \\
&= d_{sp}(\langle (x-\gamma_0)^b\rangle_{\mathbb{F}}).
\end{aligned}
$$

* Case 2: $c(x) \notin \langle u\rangle$. In this case, by (5.1). We have

$$
\begin{aligned}
wt_{sp}(c(x)) &\ge wt_{sp}(u^2c(x)) \\
&\ge d_{sp}(\langle u^2(x-\gamma_0)^a\rangle) \\
&= d_{sp}(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}).
\end{aligned}
$$

Since, $\langle (x-\gamma_0)^a\rangle \subseteq \langle (x-\gamma_0)^b\rangle \subseteq \langle (x-\gamma_0)^W\rangle$, we have

$$d_{sp}(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \ge d_{sp}(\langle (x-\gamma_0)^b\rangle_{\mathbb{F}}) \ge d_{sp}(\langle (x-\gamma_0)^V\rangle_{\mathbb{F}}).$$

Hence, $d_{sp}(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}) \leq d_{sp}(\mathcal{C}_7)$, forcing

$$d_{sp}(\mathcal{C}_7) = d_{sp}(\langle (x-\gamma_0)^W\rangle_{\mathbb{F}}).$$

The rest of the proof follows from Theorem 2.5 and the discussion above. □

Next, we compute the symbol-pair distance of Type 8 γ-constacyclic codes as follows:

Theorem 5.7 Let $\mathcal{C}_8 = \langle (x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b+u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 8 (as classified in Theorem 3.1). Then the symbol-pair distance $d_{sp}(\mathcal{C}_8)$ of $\mathcal{C}_8$ is given by

$$\begin{aligned} d_{sp}(\mathcal{C}_8) &= d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \\ &= \mathcal{S}_c \\ &= \begin{cases} \bullet\ 2, & \text{if } c = 0, \\ \bullet\ 3p^k, & \text{if } c = p^s - p^{s-k}+1, \text{ where } 0 \leq k \leq s-2, \\ \bullet\ 4p^k, & \text{if } p^s - p^{s-k}+2 \leq c \leq p^s - p^{s-k}+p^{s-k-1}, \\ & \text{where } 0 \leq k \leq s-2, \\ \bullet\ 2(\sigma+2)p^k, & \text{if } p^s - pr+\sigma r+1 \leq c \leq p^s - pr+(\sigma+1)r, \\ & \text{where } r = p^{s-k-1},\ 0 \leq k \leq s-2 \text{ and } 1 \leq \sigma \leq p-2, \\ \bullet\ (\sigma+2)p^{s-1}, & \text{if } c = p^s - p+\sigma, \text{ where } 0 \leq \sigma \leq p-2. \end{cases} \end{aligned}$$

Proof Let $\mathcal{C}_8 = \langle (x-\gamma_0)^a+u(x-\gamma_0)^{t_1}h_1(x)+u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b+u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$ be of Type 8. And consider an arbitrary polynomial $c(x) \in \mathcal{C}_8 \setminus \langle u^2(x-\gamma_0)^c\rangle$. Now, we consider two cases as follows:

* Case 1: $c(x) \in \langle u\rangle$. In this case, by (5.1). We have

$$\begin{aligned} wt_{sp}(c(x)) &\geq wt_{sp}(uc(x)) \\ &\geq d_{sp}(\langle u^2(x-\gamma_0)^b\rangle) \\ &= d_{sp}(\langle (x-\gamma_0)^b\rangle_{\mathbb{F}}) \\ &\geq d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}). \end{aligned}$$

* Case 2: $c(x) \notin \langle u\rangle$. In this case, by (5.1). We have

$$\begin{aligned} wt_{sp}(c(x)) &\geq wt_{sp}(u^2c(x)) \\ &\geq d_{sp}(\langle u^2(x-\gamma_0)^a\rangle) \\ &= d_{sp}(\langle (x-\gamma_0)^a\rangle_{\mathbb{F}}) \\ &\geq d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}). \end{aligned}$$

This implies that $d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}}) \leq d_{sp}(\mathcal{C}_8)$.

On the other hand we have that

$$\langle u^2(x-\gamma_0)^c\rangle \subseteq \mathcal{C}_8,$$

then $d_{sp}(\mathcal{C}_8) \leq d_{sp}(\langle u^2(x-\gamma_0)^c\rangle) = d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}})$ and we get $d_{sp}(\mathcal{C}_8) = d_{sp}(\langle (x-\gamma_0)^c\rangle_{\mathbb{F}})$. Now by applying Theorem 2.5, we get the desired result. □

Now, let us consider an example of symbol-pair constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$.

Example 5.1 Consider the ring $\mathcal{R} = \mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$, where $p = 7$, $m = 1$ and $\gamma \in \mathbb{F}_7^*$. We will determine the symbol-pair distance of all γ-constacyclic codes of length $n = p^s = 49$. γ-constacyclic codes of length 49 over $\mathcal{R}$ has eight types of generator. The symbol-pair distances corresponding to different generators are given as follows:

- Type 1 ($\mathcal{C}_1$) : $\langle 0\rangle$, $\langle 1\rangle$, $d_{sp}(\langle 0\rangle) = 0$, $d_{sp}(\langle 1\rangle) = 2$.
- Type 2: $\mathcal{C}_2 = \langle u^2(x-\gamma)^\tau\rangle$, where $0 \leq \tau \leq 48$, then the symbol-pair distance, $d_{sp}(\mathcal{C}_2)$, is determined in Table 5.1.
- Type 3: $\mathcal{C}_3 = \langle u(x-\gamma)^\delta + u^2(x-\gamma)^t h(x)\rangle$, where $0 \leq \delta \leq 48$, $0 \leq t < \delta$, either $h(x)$ is 0 or a unit in $\mathcal{R}_\gamma$, and then symbol-pair distance, $d_{sp}(\mathcal{C}_3)$, is given in Table 5.2.
- Type 4: $\mathcal{C}_4 = \langle u(x-\gamma)^\delta + u^2(x-\gamma)^t h(x), u^2(x-\gamma)^\omega\rangle$, where $0 \leq \omega < \delta \leq 48$, $0 \leq t < \omega$, either $h(x)$ is 0 or a unit in $\mathcal{R}_\gamma$, then the symbol-pair distance, $d_{sp}(\mathcal{C}_4)$, is determined in Table 5.3.
- Type 5: $\mathcal{C}_5 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1}h_1(x) + u^2(x-\gamma)^{t_2}h_2(x)\rangle$, where $1 \leq a \leq 48$, $0 \leq t_1 < a$, $0 \leq t_2 < a$, either $h_1(x), h_2(x)$ are 0 or are units in $\mathcal{R}_\gamma$. Then the symbol-pair distance, $d_{sp}(\mathcal{C}_5)$, is given in Table 5.4.
- Type 6: $\mathcal{C}_6 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1}h_1(x) + u^2(x-\gamma)^{t_2}h_2(x), u^2(x-\gamma)^c\rangle$, where $0 \leq c < a \leq 48$, $0 \leq t_1 < a$, $0 \leq t_2 < c$, either $h_1(x), h_2(x)$ are 0 or are units in $\mathcal{R}_\gamma$, then the symbol-pair distance, $d_{sp}(\mathcal{C}_6)$, is determined in Table 5.5.
- Type 7: $\mathcal{C}_7 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1}h_1(x) + u^2(x-\gamma)^{t_2}h_2(x), u(x-\gamma)^b + u^2(x-\gamma)^{t_3}h_3(x)\rangle$, where $0 \leq b < a \leq 48$, $0 \leq t_1 < b$, $0 \leq t_2 < b$, $0 \leq t_3 < b$, either $h_1(x), h_2(x), h_3(x)$ are 0 or are units in $\mathcal{R}_\gamma$. Then the symbol-pair distance, $d_{sp}(\mathcal{C}_7)$, is given in Table 5.6.
- Type 8: $\mathcal{C}_8 = \langle (x-\gamma)^a + u(x-\gamma)^{t_1}h_1(x) + u^2(x-\gamma)^{t_2}h_2(x), u(x-\gamma)^b + u^2(x-\gamma)^{t_3}h_3(x), u^2(x-\gamma)^c\rangle$, where $0 \leq c < b < a \leq 48$, $0 \leq t_1 < b$, $0 \leq t_2 < c$, $0 \leq t_3 < c$, either $h_1(x), h_2(x), h_3(x)$ are 0 or are units in $\mathcal{R}_\gamma$, then the symbol-pair distance, $d_{sp}(\mathcal{C}_8)$, is determined in Table 5.7.

Table 5.1 – Symbol-pair distance of γ-constacyclic codes of **Type 2** over $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Range of τ	$d_{sp}(\mathcal{C}_2)$
$\tau = 0$	2
$\tau = 1$	3
$2 \le \tau \le 7$	4
$8 \le \tau \le 14$	6
$15 \le \tau \le 21$	8
$22 \le \tau \le 28$	10
$29 \le \tau \le 35$	12
$36 \le \tau \le 42$	14
$\tau = 43$	21
$\tau = 44$	28
$\tau = 45$	35
$\tau = 46$	42
$\tau = 47$	49
$\tau = 48$	49

Table 5.2 – Symbol-pair distance of γ-constacyclic codes of **Type 3** over $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Range of L	$d_{sp}(\mathcal{C}_3)$
$L = 0$	2
$L = 1$	3
$2 \le L \le 7$	4
$8 \le L \le 14$	6
$15 \le L \le 21$	8
$22 \le L \le 28$	10
$29 \le L \le 35$	12
$36 \le L \le 42$	14
$L = 43$	21
$L = 44$	28
$L = 45$	35
$L = 46$	42
$L = 47$	49
$L = 48$	49

Table 5.3 – Symbol-pair distance of γ-constacyclic codes of **Type 4** over $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Range of ω	$d_{sp}(\mathcal{C}_4)$
$\omega = 0$	2
$\omega = 1$	3
$2 \le \omega \le 7$	4
$8 \le \omega \le 14$	6
$15 \le \omega \le 21$	8
$22 \le \omega \le 28$	10
$29 \le \omega \le 35$	12
$36 \le \omega \le 42$	14
$\omega = 43$	21
$\omega = 44$	28
$\omega = 45$	35
$\omega = 46$	42
$\omega = 47$	49

Table 5.4 – Symbol-pair distance of γ-constacyclic codes of **Type 5** over $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Range of V	$d_{sp}(\mathcal{C}_5)$
$V = 1$	3
$2 \le V \le 7$	4
$8 \le V \le 14$	6
$15 \le V \le 21$	8
$22 \le V \le 28$	10
$29 \le V \le 35$	12
$36 \le V \le 42$	14
$V = 43$	21
$V = 44$	28
$V = 45$	35
$V = 46$	42
$V = 47$	49
$V = 48$	49

Table 5.5 – Symbol-pair distance of γ-constacyclic codes of **Type 6** over $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Range of c	$d_{sp}(\mathcal{C}_6)$
$c = 0$	2
$c = 1$	3
$2 \le c \le 7$	4
$8 \le c \le 14$	6
$15 \le c \le 21$	8
$22 \le c \le 28$	10
$29 \le c \le 35$	12
$36 \le c \le 42$	14
$c = 43$	21
$c = 44$	28
$c = 45$	35
$c = 46$	42
$c = 47$	49

Table 5.6 – Symbol-pair distance of γ-constacyclic codes of **Type 7** over $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Range of W	$d_{sp}(\mathcal{C}_7)$
$W = 0$	2
$W = 1$	3
$2 \le W \le 7$	4
$8 \le W \le 14$	6
$15 \le W \le 21$	8
$22 \le W \le 28$	10
$29 \le W \le 35$	12
$36 \le W \le 42$	14
$W = 43$	21
$W = 44$	28
$W = 45$	35
$W = 46$	42
$W = 47$	49

Table 5.7 – Symbol-pair distance of γ-constacyclic codes of **Type 8** over $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Range of c	$d_{sp}(\mathcal{C}_8)$
$c = 0$	2
$c = 1$	3
$2 \le c \le 7$	4
$8 \le c \le 14$	6
$15 \le c \le 21$	8
$22 \le c \le 28$	10
$29 \le c \le 35$	12
$36 \le c \le 42$	14
$c = 43$	21
$c = 44$	28
$c = 45$	35
$c = 46$	42

5.3 Determination of MDS symbol-pair codes

All the MDS symbol-pair γ-constacyclic codes are identified in this Section by utilizing the symbol-pair distance obtained in Section 5.2 of all symbol-pair constacyclic codes of prime power length over $\mathcal{R}$.

A. **Type 1 ($\mathcal{C}_1$)**:

If $\mathcal{C}_1 = \langle 0\rangle$, then $|\mathcal{C}_1| = 1$ and $d_{sp}(\langle 0\rangle) = 0$. Thus by (2.2), $\mathcal{C}_1$ is a symbol-pair MDS code if and only if $|\mathcal{C}_1| = p^{3m(p^s - d_{sp}(\mathcal{C}_1)+2)}$, i.e., $1 = p^{3m(p^s+2)}$, i.e., $p^s = -2$, which is not true for any p and s.

Again, if $\mathcal{C}_1 = \langle 1\rangle$, then $|\mathcal{C}_1| = p^{3mp^s}$ and $d_{sp}(\langle 1\rangle) = 2$. Thus by (2.2), $\mathcal{C}_1$ is a symbol-pair MDS code if and only if $|\mathcal{C}_1| = p^{3m(p^s - d_{sp}(\mathcal{C}_1)+2)}$, i.e., $p^{3mp^s} = p^{3m(p^s-2+2)}$, which is true for all p and s. Thus, the code $\mathcal{C}_1$ is MDS symbol-pair code in this case.

Thus, MDS symbol-pair codes for trivial ideals is $\langle 1\rangle$.

B. **Type 2 ($\mathcal{C}_2$)**:

Here, we have $\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle$, where $0 \le \tau \le p^s - 1$. We note, by Theorem 3.3, that

$$|\mathcal{C}_2| = p^{m(p^s-\tau)}.$$

From this and by (2.2), we see that the code $\mathcal{C}_2$ is a symbol-pair MDS code if and only if $p^{m(p^s-\tau)} = p^{3m(p^s - d_{sp}(\mathcal{C}_2)+2)}$, which holds if and only if

$$\tau = 3d_{sp}(\mathcal{C}_2) - 2p^s - 6.$$

Hence, follows the theorem.

Theorem 5.8 Let $\mathcal{C}_2 = \langle u^2(x-\gamma_0)^\tau\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 2 (as classified in Theorem 3.1), where $0 \le \tau \le p^s - 1$. Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $\tau = 3d_{sp}(\mathcal{C}_2) - 2p^s - 6$. The symbol-pair distance $d_{sp}(\mathcal{C}_2)$ of Type2 γ-constacyclic code is established in Theorem 5.1. Now, we consider the cases according to the range of τ.

Case1: $\tau = 0$, then $d_{sp}(\mathcal{C}_2) = 2$, and $\tau = 3d_{sp}(\mathcal{C}_2) - 6 > 3d_{sp}(\mathcal{C}_2) - 2p^s - 6$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case2: $\tau = p^s - p^{s-k} + 1$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_2) = 3p^k$, and

$$\begin{aligned}
\tau &= p^s - p^{s-k} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + 1 \\
&\geq p^2(3p^k - 1) - 2p^s + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\geq 4(3p^k - 1) - 2p^s + 1 \ (\text{equality when } p = 2) \\
&= 3d_{sp}(\mathcal{C}_2) - 2p^s + 3p^k - 3 \\
&\geq 3d_{sp}(\mathcal{C}_2) - 2p^s \ (\text{equality when } k = 0) \\
&> 3d_{sp}(\mathcal{C}_2) - 2p^s - 6.
\end{aligned}$$

Since, $\tau > 3d_{sp}(\mathcal{C}_2) - 2p^s - 6$, no MDS symbol-pair constacyclic code exists in this case.

Case3: $p^s - p^{s-k} + 2 \leq \tau \leq p^s - p^{s-k} + p^{s-k-1}$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_2) = 4p^k$, and

$$\begin{aligned}
\tau &= p^s - p^{s-k} + 2 \\
&= p^{s-k}(3p^k - 1) - 2p^s + 2 \\
&\geq p^2(3p^k - 1) - 2p^s + 2 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\geq 4(3p^k - 1) - 2p^s + 2 \ (\text{equality when } p = 2) \\
&= 3d_{sp}(\mathcal{C}_2) - 2p^s - 2 \\
&> 3d_{sp}(\mathcal{C}_2) - 2p^s - 6.
\end{aligned}$$

Since, $\tau > 3d_{sp}(\mathcal{C}_2) - 2p^s - 6$, no MDS symbol-pair constacyclic code exists in this case.

Case 4: $p^s - pr + \sigma r + 1 \le \tau \le p^s - pr + (\sigma+1)r$, where $r = p^{s-k-1}$, $0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_2) = 2(\sigma+2)p^k$, and

$$\begin{aligned}
\tau &\ge p^s - p^{s-k} + \sigma p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + \sigma p^{s-k-1} + 1 \\
&\ge p^2(3p^k - 1) - 2p^s + \sigma p + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\ge (\sigma+2)^2(3p^k - 1) - 2p^s + \sigma(\sigma+2) + 1 \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+1)(\sigma+2)p^k - 2p^s + (\sigma+2)(3p^k - 2) + 1 \\
&\ge 6(\sigma+2)p^k - 2p^s + 3(3p^k - 2) + 1 \\
&\quad \times (\text{equality when } \sigma = 1) \\
&\ge 3d_{sp}(\mathcal{C}_2) - 2p^s + 4 \ (\text{equality when } k = 0) \\
&> 3d_{sp}(\mathcal{C}_2) - 2p^s - 6.
\end{aligned}$$

Since, $\tau > 3d_{sp}(\mathcal{C}_2) - 2p^s - 6$, no MDS symbol-pair constacyclic code exists in this case.

Case 5: $\tau = p^s - p + \sigma$, where $0 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_2) = (\sigma+2)p^{s-1}$, and

$$\begin{aligned}
\tau &= p^s - p + \sigma \\
&= p(3p^{s-1} - 1) - 2p^s + \sigma \\
&\ge (\sigma+2)(3p^{s-1} - 1) - 2p^s + \sigma \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+2)p^{s-1} - 2p^s - 2 \\
&= 3d_{sp}(\mathcal{C}_2) - 2p^s - 2 \\
&> 3d_{sp}(\mathcal{C}_2) - 2p^s - 6.
\end{aligned}$$

Since, $\tau > 3d_{sp}(\mathcal{C}_2) - 2p^s - 6$, no MDS symbol-pair constacyclic code exists in this case.

Case 6: $\tau = p^s - 1$. Then $d_{sp}(\mathcal{C}_2) = p^s$, and $\tau = 3p^s - 2p^s - 1 = 3d_{sp}(\mathcal{C}_2) - 2p^s - 1 > 3d_{sp}(\mathcal{C}_2) - 2p^s - 6$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Hence, MDS symbol-pair code does not exist for γ-constacyclic codes of Type 2. This completes the proof. □

C. **Type 3 ($\mathcal{C}_3$)**:

Here, we have $\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x)\rangle$, where $0 \le \delta \le p^s - 1$, $0 \le t < \delta$, either $h(x)$ is 0 or a unit in $\mathcal{R}_\gamma$. By Theorem 3.3, we see that $|\mathcal{C}_3| = p^{m(2p^s-\delta-L)}$. From this and by (2.2), the code $\mathcal{C}_3$ is a symbol-pair MDS code if and only if $p^{m(2p^s-\delta-L)} = p^{3m(p^s-d_{sp}(\mathcal{C}_3)+2)}$, i.e., $L = 3d_{sp}(\mathcal{C}_3) - p^s - \delta - 6$. Let $\delta = p^s - \rho$, where $1 \le \rho \le p^s$. Thus, the condition for $\mathcal{C}_3$ to be a MDS symbol-pair constacyclic code becomes $L = 3d_{sp}(\mathcal{C}_3) - 2p^s - 6 + \rho$. Hence, follows the theorem.

Theorem 5.9 Let $\mathcal{C}_3 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type3 (as classified in Theorem 3.1). Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $L = 3d_{sp}(\mathcal{C}_3) - 2p^s - 6 + \rho$. The symbol-pair distance $d_{sp}(\mathcal{C}_3)$ of Type3 γ-constacyclic code is established in Theorem 5.2. Now, we consider the cases according to the range of L.

Case1: $L = 0$, then $d_{sp}(\mathcal{C}_3) = 2$. Thus $\mathcal{C}_3$ is a symbol-pair MDS code if and only if $\rho = 2p^s$, i.e., $\delta = -p^s$, which is not possible.

Case2: $L = p^s - p^{s-k} + 1$, where $0 \le k \le s-2$. Then $d_{sp}(\mathcal{C}_3) = 3p^k$, and

$$\begin{aligned}
L &= p^s - p^{s-k} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + 1 \\
&\ge p^2(3p^k - 1) - 2p^s + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\ge 4(3p^k - 1) - 2p^s + 1 \ (\text{equality when } p = 2) \\
&= 3d_{sp}(\mathcal{C}_3) - 2p^s + 3p^k - 3 \\
&\ge 3d_{sp}(\mathcal{C}_3) - 2p^s \ (\text{equality when } k = 0)
\end{aligned}$$

Now, $L \ge 3d_{sp}(\mathcal{C}_3) - 2p^s - 6 + \rho$ if and only if $6 \ge \rho$, i.e., equality when $\rho = 6$. Thus, equality occurs when $p = 2, k = 0, s = 2, \rho = 6$, i.e., $L = 1$ and $\delta = -2$, which is a contradiction, since $0 \le L \le \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case3: $p^s - p^{s-k} + 2 \le L \le p^s - p^{s-k} + p^{s-k-1}$, where $0 \le k \le s-2$. Then $d_{sp}(\mathcal{C}_3) = 4p^k$, and

$$\begin{aligned} L &= p^s - p^{s-k} + 2 \\ &= p^{s-k}(3p^k - 1) - 2p^s + 2 \\ &\ge p^2(3p^k - 1) - 2p^s + 2 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\ge 4(3p^k - 1) - 2p^s + 2 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(\mathcal{C}_3) - 2p^s - 2. \end{aligned}$$

Now, $L \ge 3d_{sp}(\mathcal{C}_3) - 2p^s - 6 + \rho$ if and only if $4 \ge \rho$, i.e., equality when $\rho = 4$. Thus, equality occurs when $p = 2, k = s-2, \rho = 4$, i.e., $L = 2^s - 2$ and $\delta = 2^s - 4$, which is a contradiction, since $L \le \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case4: $p^s - pr + \sigma r + 1 \le L \le p^s - pr + (\sigma+1)r$, where $r = p^{s-k-1}, 0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_3) = 2(\sigma+2)p^k$, and

$$\begin{aligned} L &\ge p^s - p^{s-k} + \sigma p^{s-k-1} + 1 \\ &= p^{s-k}(3p^k - 1) - 2p^s + \sigma p^{s-k-1} + 1 \\ &\ge p^2(3p^k - 1) - 2p^s + \sigma p + 1 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\ge (\sigma+2)^2(3p^k - 1) - 2p^s + \sigma(\sigma+2) + 1 \\ &\quad \times (\text{equality when } \sigma = p-2) \\ &= 3(\sigma+1)(\sigma+2)p^k - 2p^s + (\sigma+2)(3p^k - 2) + 1 \\ &\ge 6(\sigma+2)p^k - 2p^s + 3(3p^k - 2) + 1 \\ &\quad \times (\text{equality when } \sigma = 1) \\ &\ge 3d_{sp}(\mathcal{C}_3) - 2p^s + 4 \ (\text{equality when } k = 0). \end{aligned}$$

Now, $L \ge 3d_{sp}(\mathcal{C}_3) - 2p^s - 6 + \rho$ if and only if $10 \ge \rho$, i.e., equality when $\rho = 10$. Thus, equality occurs when $\sigma = 1, p = 3, k = 0, s = 2, \rho = 10$, i.e., $L = 4$ and $\delta = -1$, which is a contradiction, since $0 \le L \le \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 5: $L = p^s - p + \sigma$, where $0 \leq \sigma \leq p-2$. Then $d_{sp}(\mathcal{C}_3) = (\sigma+2)p^{s-1}$, and

$$\begin{aligned} L &= p^s - p + \sigma \\ &= p(3p^{s-1} - 1) - 2p^s + \sigma \\ &\geq (\sigma+2)(3p^{s-1} - 1) - 2p^s + \sigma \\ &\quad \times (\text{equality when } \sigma = p-2) \\ &= 3(\sigma+2)p^{s-1} - 2p^s - 2 \\ &= 3d_{sp}(\mathcal{C}_3) - 2p^s - 2. \end{aligned}$$

Now, $L \geq 3d_{sp}(\mathcal{C}_3) - 2p^s - 6 + \rho$ if and only if $4 \geq \rho$, i.e., equality when $\rho = 4$. Thus, equality occurs when $\sigma = p-2, \rho = 4$, i.e., $L = p^s - 2$ and $\delta = p^s - 4$, which is a contradiction, since $L \leq \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 6: $L = p^s - 1$. Then $d_{sp}(\mathcal{C}_3) = p^s$, and $L = 3p^s - 2p^s - 1 = 3d_{sp}(\mathcal{C}_3) - 2p^s - 1$.
Now, $L \geq 3d_{sp}(\mathcal{C}_3) - 2p^s - 6 + \rho$ if and only if $5 \geq \rho$, i.e., equality when $\rho = 5$. Thus, $\delta = p^s - 5 < L$, which is a contradiction. Thus, no MDS symbol-pair constacyclic code exists in this case.

Hence, MDS symbol-pair code does not exist for γ-constacyclic codes of Type 3. This completes the proof. □

D. **Type 4 ($\mathcal{C}_4$)**:

Here, we have $\mathcal{C}_4 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x), u^2(x-\gamma_0)^\omega \rangle$, where $0 \leq \omega < \delta \leq p^s - 1$, $0 \leq t < \omega$, either $h(x)$ is 0 or a unit in $\mathcal{R}_\gamma$. And $|\mathcal{C}_4| = p^{m(2p^s-\delta-\omega)}$. Thus by (2.2), $\mathcal{C}_4$ is a symbol-pair MDS code if and only if $|\mathcal{C}_4| = p^{3m(p^s - d_{sp}(\mathcal{C}_4)+2)}$, i.e., $p^{m(2p^s-\delta-\omega)} = p^{3m(p^s - d_{sp}(\mathcal{C}_4)+2)}$, i.e., $\omega = 3d_{sp}(\mathcal{C}_4) - p^s - \delta - 6$. Let $\delta = p^s - \rho$, where $1 \leq \rho \leq p^s$. Thus, the condition for $\mathcal{C}_4$ to be a MDS symbol-pair constacyclic code becomes

$$\omega = 3d_{sp}(\mathcal{C}_4) - 2p^s - 6 + \rho.$$

Hence, follows the theorem.

Theorem 5.10 Let $\mathcal{C}_4 = \langle u(x-\gamma_0)^\delta + u^2(x-\gamma_0)^t h(x), u^2(x-\gamma_0)^\omega \rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 4 (as classified in Theorem 3.1). Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $\omega = 3d_{sp}(\mathcal{C}_4) - 2p^s - 6 + \rho$. The symbol-pair distance $d_{sp}(\mathcal{C}_4)$ of Type4 γ-constacyclic code is established in Theorem 5.3. Now, we consider the cases according to the range of ω.

Case1: $\omega = 0$, then $d_{sp}(\mathcal{C}_4) = 2$. Thus $\mathcal{C}_4$ is a symbol-pair MDS code if and only if $\rho = 2p^s$, i.e., $\delta = -p^s$, which is not possible.

Case2: $\omega = p^s - p^{s-k} + 1$, where $0 \le k \le s-2$. Then $d_{sp}(C_4) = 3p^k$, and

$$\begin{aligned}
\omega &= p^s - p^{s-k} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + 1 \\
&\ge p^2(3p^k - 1) - 2p^s + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\ge 4(3p^k - 1) - 2p^s + 1 \ (\text{equality when } p = 2) \\
&= 3d_{sp}(\mathcal{C}_4) - 2p^s + 3p^k - 3 \\
&\ge 3d_{sp}(\mathcal{C}_4) - 2p^s \ (\text{equality when } k = 0)
\end{aligned}$$

Now, $\omega \ge 3d_{sp}(\mathcal{C}_4) - 2p^s - 6 + \rho$ if and only if $6 \ge \rho$, i.e., equality when $\rho = 6$. Thus, equality occurs when $p = 2, k = 0, s = 2, \rho = 6$, i.e., $\omega = 1$ and $\delta = -2$, which is a contradiction, since $0 \le \omega < \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case3: $p^s - p^{s-k} + 2 \le \omega \le p^s - p^{s-k} + p^{s-k-1}$, where $0 \le k \le s-2$. Then $d_{sp}(\mathcal{C}_4) = 4p^k$, and

$$\begin{aligned}
\omega &= p^s - p^{s-k} + 2 \\
&= p^{s-k}(3p^k - 1) - 2p^s + 2 \\
&\ge p^2(3p^k - 1) - 2p^s + 2 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\ge 4(3p^k - 1) - 2p^s + 2 \ (\text{equality when } p = 2) \\
&= 3d_{sp}(C_4) - 2p^s - 2.
\end{aligned}$$

Now, $\omega \ge 3d_{sp}(\mathcal{C}_4) - 2p^s - 6 + \rho$ if and only if $4 \ge \rho$, i.e., equality when $\rho = 4$. Thus, equality occurs when $p = 2, k = s-2, \rho = 4$, i.e., $\omega = 2^s - 2$ and $\delta = 2^s - 4$, which is a contradiction, since $\omega < \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 4: $p^s - pr + \sigma r + 1 \le \omega \le p^s - pr + (\sigma+1)r$, where $r = p^{s-k-1}$, $0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_4) = 2(\sigma+2)p^k$, and

$$\begin{aligned}
\omega &\ge p^s - p^{s-k} + \sigma p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + \sigma p^{s-k-1} + 1 \\
&\ge p^2(3p^k - 1) - 2p^s + \sigma p + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\ge (\sigma+2)^2(3p^k - 1) - 2p^s + \sigma(\sigma+2) + 1 \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+1)(\sigma+2)p^k - 2p^s + (\sigma+2)(3p^k - 2) + 1 \\
&\ge 6(\sigma+2)p^k - 2p^s + 3(3p^k - 2) + 1 \\
&\quad \times (\text{equality when } \sigma = 1) \\
&\ge 3d_{sp}(C_4) - 2p^s + 4 \ (\text{equality when } k = 0).
\end{aligned}$$

Now, $\omega \ge 3d_{sp}(\mathcal{C}_4) - 2p^s - 6 + \rho$ if and only if $10 \ge \rho$, i.e., equality when $\rho = 10$. Thus, equality occurs when $\sigma = 1, p = 3, k = 0, s = 2, \rho = 10$, i.e., $\omega = 4$ and $\delta = -1$, which is a contradiction, since $0 \le \omega < \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 5: $\omega = p^s - p + \sigma$, where $0 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_4) = (\sigma+2)p^{s-1}$, and

$$\begin{aligned}
\omega &= p^s - p + \sigma \\
&= p(3p^{s-1} - 1) - 2p^s + \sigma \\
&\ge (\sigma+2)(3p^{s-1} - 1) - 2p^s + \sigma \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+2)p^{s-1} - 2p^s - 2 \\
&= 3d_{sp}(C_4) - 2p^s - 2.
\end{aligned}$$

Now, $\omega \ge 3d_{sp}(\mathcal{C}_4) - 2p^s - 6 + \rho$ if and only if $4 \ge \rho$, i.e., equality when $\rho = 4$. Thus, equality occurs when $\sigma = p-2, \rho = 4$, i.e., $\omega = p^s - 2$ and $\delta = p^s - 4$, which is a contradiction, since $\omega < \delta$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Hence, MDS symbol-pair code does not exist for γ-constacyclic codes of Type 4. This completes the proof. □

E. **Type 5 ($\mathcal{C}_5$)**:

Here, we have $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$, where $1 \le a \le p^s - 1$, $0 \le t_1 < a$, $0 \le t_2 < a$, either $h_1(x), h_2(x)$ are 0 or are units in $\mathcal{R}_\gamma$. We note, by Theorem 3.3, that $|\mathcal{C}_5| = p^{m(3p^s-a-U-V)}$. From this and by (2.2), we see that the code $\mathcal{C}_5$ is a symbol-pair MDS code if and only if $p^{m(3p^s-a-U-V)} = p^{3m(p^s-d_{sp}(\mathcal{C}_5)+2)}$, which holds if and only if

$$V = 3d_{sp}(\mathcal{C}_5) - a - U - 6.$$

Thus, we get the following cases:

Case 1: When $h_1(x) = h_2(x) = 0$ then, $V = U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = d_{sp}(\mathcal{C}_5) - 2$. Hence, the MDS symbol-pair codes for Type5 ideals are similar to the MDS γ-constacyclic symbol-pair codes over $\mathbb{F}_{p^m}$ (see Theorem 2.6). Hence, we have the following theorem:

Theorem 5.11 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 5 (as classified in Theorem 3.1). Then $\mathcal{C}_5$ is an MDS symbol-pair constacyclic code if and only if one of the following conditions holds:

- If $s = 1$, then $a = n$ for $1 \le n \le p-2$, in such case, $d_{sp}(\mathcal{C}_5) = n+2$.
- If $s \ge 2$, then
  - $a = 1$, in such case, $d_{sp}(\mathcal{C}_5) = 3$,
  - $a = 2$, in such case, $d_{sp}(\mathcal{C}_5) = 4$,
  - $s = 2$, $p = 3$, $a = 4$, in such case, $d_{sp}(\mathcal{C}_5) = 6$,
  - $a = p^s - 2$, in such case, $d_{sp}(\mathcal{C}_5) = p^s$.

Case 2: When $h_1(x) = 0, h_2(x) \neq 0$ and $1 \le a \le \dfrac{p^s + t_2}{2}$ then, $V = U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = d_{sp}(\mathcal{C}_5) - 2$, which is similar to the result in case 1. But we have $1 \le a \le \dfrac{p^s + t_2}{2}$ and $0 \le t_2 < a$, which implies that $\max\{2a - p^s, 0\} \le t_2 < a$.

Hence, we conclude the following theorem.

Theorem 5.12 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 5 (as classified in Theorem 3.1), where $h_2(x) \neq 0$ and $1 \leq a \leq \frac{p^s+t_2}{2}$. Then $\mathcal{C}_5$ is an MDS symbol-pair constacyclic code if and only if one of the following conditions holds:

- If $s = 1$, $a = n$, $1 \leq n \leq p-2$ and $\max\{2n-p, 0\} \leq t_2 < n$, then $d_{sp}(\mathcal{C}_5) = n+2$.
- If $s \geq 2$,
  - $a = 1$, $t_2 = 0$, then $d_{sp}(\mathcal{C}_5) = 3$,
  - $a = 2$, $0 \leq t_2 \leq 1$, then $d_{sp}(\mathcal{C}_5) = 4$,
  - $s = 2$, $p = 3$, $a = 4$, $0 \leq t_2 \leq 3$, then $d_{sp}(\mathcal{C}_5) = 6$,
  - $a = p^s - 2$, $p^s - 4 \leq t_2 \leq p^s - 3$, then $d_{sp}(\mathcal{C}_5) = p^s$.

Case 3: When $h_1(x) \neq 0$ and $1 \leq a \leq \frac{p^s+t_1}{2}$ then, $V = U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = d_{sp}(\mathcal{C}_5) - 2$, which is similar to the result in case 1. But we have $1 \leq a \leq \frac{p^s+t_1}{2}$ and $0 \leq t_1 < a$, which implies that $\max\{2a-p^s, 0\} \leq t_1 < a$. Hence, we conclude the following theorem.

Theorem 5.13 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 5 (as classified in Theorem 3.1), where $h_1(x) \neq 0$ and $1 \leq a \leq \frac{p^s+t_1}{2}$. Then $\mathcal{C}_5$ is an MDS symbol-pair constacyclic code if and only if one of the following conditions holds:

- If $s = 1$, $a = n$, $1 \leq n \leq p-2$ and $\max\{2n-p, 0\} \leq t_1 < n$, then $d_{sp}(\mathcal{C}_5) = n+2$.
- If $s \geq 2$,
  - $a = 1$, $t_1 = 0$, then $d_{sp}(\mathcal{C}_5) = 3$,
  - $a = 2$, $0 \leq t_1 \leq 1$, then $d_{sp}(\mathcal{C}_5) = 4$,
  - $s = 2$, $p = 3$, $a = 4$, $0 \leq t_1 \leq 3$, then $d_{sp}(\mathcal{C}_5) = 6$,
  - $a = p^s - 2$, $p^s - 4 \leq t_1 \leq p^s - 3$, then $d_{sp}(\mathcal{C}_5) = p^s$.

Case 4: When $h_1(x) \neq 0$ and $\frac{p^s+t_1}{2} < a \leq p^s - 1$ then, $V = U = p^s - a + t_1$. For $\mathcal{C}_5$ to be MDS we must have $a = 2p^s - 3d_{sp}(\mathcal{C}_5) + 2t_1 + 6$. Hence, follows the theorem.

Theorem 5.14 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type5 (as classified in Theorem 3.1), where $h_1(x) \neq 0$ and $\frac{p^s+t_1}{2} < a \leq p^s - 1$. Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $a = 2p^s - 3d_{sp}(\mathcal{C}_5) + 2t_1 + 6$. The symbol-pair distance $d_{sp}(\mathcal{C}_5)$ of Type5 γ-constacyclic code is established in Theorem 5.4. Now, we consider the cases according to the range of a.

Case1: $V = p^s - p^{s-k} + 1$, i.e., $p^s - a + t_1 = p^s - p^{s-k} + 1$, i.e., $a = p^{s-k} + t_1 - 1$, where $0 \le k \le s-2$. Then $d_{sp}(\mathcal{C}_5) = 3p^k$, and

$$\begin{aligned} a &= p^{s-k} + t_1 - 1 \\ &\ge p^2 + t_1 - 1 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &= -9p^k + p^2 + t_1 - 1 + 9p^k \\ &\ge -9p^k + p^2 + t_1 + 8 \ (\text{equality when } k = 0) \\ &\ge -9p^k + t_1 + 12 \ (\text{equality when } p = 2) \\ &= -3d_{sp}(C_5) + t_1 + 12 \end{aligned}$$

Now, $a \ge 2p^s - 3d_{sp}(\mathcal{C}_5) + 2t_1 + 6$ if and only if $-2p^s + 6 \ge t_1$, i.e., equality when $t_1 = -2p^s + 6$. Thus, equality occurs when $p = 2, k = 0, s = 2, t_1 = -2p^s + 6$, i.e., $t_1 = -2$ and $a = 1$, which is a contradiction, since $0 \le t_1$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case2: $p^s - p^{s-k} + 2 \le V \le p^s - p^{s-k} + p^{s-k-1}$, i.e., $p^s - p^{s-k} + 2 \le p^s - a + t_1 \le p^s - p^{s-k} + p^{s-k-1}$, i.e., $t_1 + p^{s-k} - p^{s-k-1} \le a \le t_1 + p^{s-k} - 2$, where $0 \le k \le s-2$. Then $d_{sp}(\mathcal{C}_5) = 4p^k$, and

$$\begin{aligned} a &= t_1 + p^{s-k} - p^{s-k-1} \\ &= t_1 + p^{s-k-1}(p-1) \\ &\ge t_1 + p(p-1) \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\ge t_1 + 2 \ (\text{equality when } p = 2) \\ &= -12p^k + t_1 + 2 + 12p^k \\ &\ge -12p^k + t_1 + 14 \ (\text{equality when } k = 0) \\ &= -3d_{sp}(C_5) + t_1 + 14. \end{aligned}$$

Now, $a \ge 2p^s - 3d_{sp}(\mathcal{C}_5) + 2t_1 + 6$ if and only if $-2p^s + 8 \ge t_1$, i.e., equality when $t_1 = -2p^s + 8$. Thus, equality occurs when $p = 2, k = 0, s = 2, t_1 = -2p^s + 8$, i.e., $t_1 = 0$ and $a = 2$, which is a contradiction, since $2 = \frac{2^2 + 0}{2} < a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case3: $p^s-pr+\sigma r+1 \le V \le p^s-pr+(\sigma+1)r$, i.e., $p^s-pr+\sigma r+1 \le p^s-a+t_1 \le p^s-pr+(\sigma+1)r$, i.e., $t_1+pr-(\sigma+1)r \le a \le t_1+pr-\sigma r-1$, where $r=p^{s-k-1}, 0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_5)=2(\sigma+2)p^k$, and

$$\begin{aligned}
a &\ge t_1+p^{s-k}-(\sigma+1)p^{s-k-1}\\
&= t_1+p^{s-k-1}(p-\sigma-1)\\
&\ge t_1+p(p-\sigma-1)\\
&\quad \times (\text{equality when } k=s-2, \text{or } s=2)\\
&\ge t_1+p \ (\text{equality when } \sigma=p-2)\\
&= -6(\sigma+2)p^k+t_1+p+6(\sigma+2)p^k\\
&\ge -6(\sigma+2)p^k+t_1+p+18p^k\\
&\quad \times (\text{equality when } \sigma=1)\\
&\ge -3d_{sp}(\mathcal{C}_5)+t_1+p+18 \ (\text{equality when } k=0).
\end{aligned}$$

Now, $a \ge 2p^s-3d_{sp}(\mathcal{C}_5)+2t_1+6$ if and only if $-2p^s+p+12 \ge t_1$, i.e., equality when $t_1=-2p^s+p+12$. Thus, equality occurs when $\sigma=1, p=3, k=0, s=2, t_1=-2p^s+p+12$, i.e., $t_1=-3$ and $a=0$, which is a contradiction, since $0 \le t_1 < a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case4: $V=p^s-p+\sigma$, i.e., $p^s-a+t_1=p^s-p+\sigma$, i.e., $a=t_1+p-\sigma$, where $0 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_5)=(\sigma+2)p^{s-1}$, and

$$\begin{aligned}
a &= t_1+p-\sigma\\
&\ge t_1+2\\
&\quad \times (\text{equality when } \sigma=p-2)\\
&= -3(\sigma+2)p^{s-1}+t_1+2+3(\sigma+2)p^{s-1}\\
&\ge -3(\sigma+2)p^{s-1}+t_1+2+6p^{s-1}\\
&\quad \times (\text{equality when } \sigma=0)\\
&= -3d_{sp}(\mathcal{C}_5)+t_1+2+6p^{s-1}.
\end{aligned}$$

Now, $a \ge 2p^s-3d_{sp}(\mathcal{C}_5)+2t_1+6$ if and only if $-2p^s+6p^{s-1}-4 \ge t_1$, i.e., equality when $t_1=-2p^s+6p^{s-1}-4$. Thus, equality occurs when $\sigma=0, p=2, t_1=-2p^s+6p^{s-1}-4$, i.e., $t_1=2^s-4$ and $a=2^s-2$, which is a contradiction, since $2^s-2=\dfrac{2^s+(2^s-4)}{2} < a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case5: $V = p^s - 1$, i.e., $p^s - a + t_1 = p^s - 1$, i.e., $a = t_1 + 1$. Then $d_{sp}(C_5) = p^s$, and $a = -3p^s + 3p^s + t_1 + 1 = -3d_{sp}(\mathcal{C}_5) + 3p^s + t_1 + 1$.

Now, $a \geq 2p^s - 3d_{sp}(\mathcal{C}_5) + 2t_1 + 6$ if and only if $p^s - 5 \geq t_1$, i.e., equality when $t_1 = p^s - 5$, i.e., $a = p^s - 4$, which is a contradiction, since $p^s - 4 < \frac{p^s + (p^s - 5)}{2} < a$. Thus, no MDS symbol-pair constacyclic code exists in this case. This completes the proof. □

Case5: When $h_1(x) = 0, h_2(x) \neq 0$ and $\frac{p^s + t_2}{2} < a \leq p^s - 1$ then, $V = p^s - a + t_2$ and $U = a$. For $\mathcal{C}_5$ to be MDS we must have $a = 3d_{sp}(\mathcal{C}_5) - p^s - t_2 - 6$. Hence, follows the theorem.

Theorem 5.15 Let $\mathcal{C}_5 = \langle (x-\gamma_0)^a + u^2(x-\gamma_0)^{t_2}h_2(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type5 (as classified in Theorem 3.1), where $h_2(x) \neq 0$ and $\frac{p^s + t_2}{2} < a \leq p^s - 1$. Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $a = 3d_{sp}(\mathcal{C}_5) - p^s - t_2 - 6$. The symbol-pair distance $d_{sp}(\mathcal{C}_5)$ of Type5 γ-constacyclic code is established in Theorem 5.4. Now, we consider the cases according to the range of a.

Case1: $V = p^s - p^{s-k} + 1$, i.e., $p^s - a + t_2 = p^s - p^{s-k} + 1$, i.e., $a = p^{s-k} + t_2 - 1$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_5) = 3p^k$, and

$$\begin{aligned} a &= p^{s-k} + t_2 - 1 \\ &\geq p^2 + t_2 - 1 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\geq t_2 + 3 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(\mathcal{C}_5) + t_2 + 3 - 9p^k. \end{aligned}$$

Now, $a \geq 3d_{sp}(\mathcal{C}_5) - p^s - t_2 - 6$ if and only if $2t_2 \geq 9p^k - p^s - 9$, i.e., equality when $2t_2 = 9p^k - p^s - 9$. Thus, equality occurs when $p = 2, k = s-2, 2t_2 = 9p^k - p^s - 9$, i.e., $2t_2 = 5 \times 2^{s-2} - 9$ and $4a = 10 \times 2^{s-2} - 6$, which is a contradiction, since $10 \times 2^{s-2} - 6 \leq 2 \times 2^s + (5 \times 2^{s-2} - 9) < 4a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 2: $p^s - p^{s-k} + 2 \le V \le p^s - p^{s-k} + p^{s-k-1}$, i.e., $p^s - p^{s-k} + 2 \le p^s - a + t_2 \le p^s - p^{s-k} + p^{s-k-1}$, i.e., $t_2 + p^{s-k} - p^{s-k-1} \le a \le t_2 + p^{s-k} - 2$, where $0 \le k \le s-2$. Then $d_{sp}(\mathcal{C}_5) = 4p^k$, and

$$\begin{aligned} a &= t_2 + p^{s-k} - p^{s-k-1} \\ &= t_2 + p^{s-k-1}(p-1) \\ &\ge t_2 + p(p-1) \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\ge t_2 + 2 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(\mathcal{C}_5) + t_2 + 2 - 12p^k. \end{aligned}$$

Now, $a \ge 3d_{sp}(\mathcal{C}_5) - p^s - t_2 - 6$ if and only if $2t_2 \ge 12p^k - p^s - 8$, i.e., equality when $2t_2 = 12p^k - p^s - 8$. Thus, equality occurs when $p = 2, k = s-2, 2t_2 = 12p^k - p^s - 8$, i.e., $t_2 = 2^s - 4$ and $a = 2^s - 2$, which is a contradiction, since $2^s - 2 = \dfrac{2^s + (2^s - 4)}{2} < a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 3: $p^s - pr + \sigma r + 1 \le V \le p^s - pr + (\sigma+1)r$, i.e., $p^s - pr + \sigma r + 1 \le p^s - a + t_2 \le p^s - pr + (\sigma+1)r$, i.e., $t_2 + pr - (\sigma+1)r \le a \le t_2 + pr - \sigma r - 1$, where $r = p^{s-k-1}, 0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_5) = 2(\sigma+2)p^k$, and

$$\begin{aligned} a &\ge t_2 + p^{s-k} - (\sigma+1)p^{s-k-1} \\ &= t_2 + p^{s-k-1}(p - \sigma - 1) \\ &\ge t_2 + p(p - \sigma - 1) \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\ge t_2 + p \ (\text{equality when } \sigma = p-2) \\ &\ge t_2 + 3 \ (\text{equality when } p = 3) \\ &= 3d_{sp}(\mathcal{C}_5) + t_2 + 3 - 6(\sigma+2)p^k. \end{aligned}$$

Now, $a \ge 3d_{sp}(\mathcal{C}_5) - p^s - t_2 - 6$ if and only if $2t_2 \ge 6(\sigma+2)p^k - p^s - 9$, i.e., equality when $2t_2 = 6(\sigma+2)p^k - p^s - 9$. Thus, equality occurs when $k = s-2$, $p = 3$, $\sigma = 1$, $2t_2 = 6(\sigma+2)p^k - p^s - 9$, i.e., $2t_2 = 3^s - 9$ and $4a = 2\times 3^s - 6$, which is a contradiction, since $2\times 3^s - 6 < 2\times 3^s + (3^s - 9) < 4a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case4: $V = p^s - p + \sigma$, i.e., $p^s - a + t_2 = p^s - p + \sigma$, i.e., $a = t_2 + p - \sigma$, where $0 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_5) = (\sigma+2)p^{s-1}$, and

$$\begin{aligned} a &= t_2 + p - \sigma \\ &= 3(\sigma+2)p^{s-1} + t_2 + p - \sigma - 3(\sigma+2)p^{s-1} \\ &\ge 3(\sigma+2)p^{s-1} + t_2 + 2 - 3p^s \\ &\quad \times (\text{equality when } \sigma = p-2) \\ &= 3d_{sp}(\mathcal{C}_5) + t_2 + 2 - 3p^s. \end{aligned}$$

Now, $a \ge 3d_{sp}(\mathcal{C}_5) - p^s - t_2 - 6$ if and only if $t_2 \ge p^s - 4$, i.e., equality when $t_2 = p^s - 4$. Thus, equality occurs when $\sigma = p-2, t_2 = p^s - 4$, i.e., $a = p^s - 2$, which is a contradiction, since $p^s - 2 = \dfrac{p^s + (p^s - 4)}{2} < a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case5: $V = p^s - 1$, i.e., $p^s - a + t_2 = p^s - 1$, i.e., $a = t_2 + 1$. Then $d_{sp}(\mathcal{C}_5) = p^s$, and $a = 3p^s - 3p^s + t_2 + 1 = 3d_{sp}(\mathcal{C}_5) - 3p^s + t_2 + 1$.
Now, $a \ge 3d_{sp}(\mathcal{C}_5) - p^s - t_2 - 6$ if and only if $2t_2 \ge 2p^s - 7$, i.e., equality when $2t_2 = 2p^s - 7$, i.e., $4a = 4p^s - 10$, which is a contradiction, since $4p^s - 10 < 2p^s + (2p^s - 7) < 4a$. Thus, no MDS symbol-pair constacyclic code exists in this case. This completes the proof. □

F. **Type6 ($\mathcal{C}_6$)**:

Here, we have $\mathcal{C}_6 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$, where $0 \le c < a \le p^s - 1$, $0 \le t_1 < a$, $0 \le t_2 < c$, either $h_1(x), h_2(x)$ are 0 or are units in $\mathcal{R}_\gamma$. And $|\mathcal{C}_6| = p^{m(3p^s - a - U - c)}$. From this and by (2.2), we see that the code $\mathcal{C}_6$ is a symbol-pair MDS code if and only if $p^{m(3p^s - a - U - c)} = p^{3m(p^s - d_{sp}(\mathcal{C}_6) + 2)}$, i.e.,

$$c = 3d_{sp}(\mathcal{C}_6) - U - a - 6.$$

Hence, follows the theorem.

Theorem 5.16 Let $\mathcal{C}_6 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type6 (as classified in Theorem 3.1). Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $c = 3d_{sp}(\mathcal{C}_6) - U - a - 6$. The symbol-pair distance $d_{sp}(\mathcal{C}_6)$ of Type6 γ-constacyclic code is established in Theorem 5.5. Now, we consider the cases according to the range of c.

Case 1: $c = 0$, then $d_{sp}(\mathcal{C}_6) = 2$. Thus $\mathcal{C}_6$ is a symbol-pair MDS code if and only if $a = -U$, which is not possible.

Case 2: $c = p^s - p^{s-k} + 1$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_6) = 3p^k$, and

$$\begin{aligned} c &= p^s - p^{s-k} + 1 \\ &= p^{s-k}(3p^k - 1) - 2p^s + 1 \\ &\geq p^2(3p^k - 1) - 2p^s + 1 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\geq 4(3p^k - 1) - 2p^s + 1 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(C_6) - 2p^s + 3p^k - 3 \\ &\geq 3d_{sp}(\mathcal{C}_6) - 2p^s \ (\text{equality when } k = 0) \end{aligned}$$

Now, $c \geq 3d_{sp}(\mathcal{C}_6) - U - a - 6$ if and only if $a + U \geq 2p^s - 6$, i.e., equality when $a + U = 2p^s - 6$. Thus, equality occurs when $p = 2, k = 0, s = 2, a + U = 2p^s - 6$, i.e., $c = 1$ and $a + U = 2$, i.e., $a = 1$ and $U = 1$ (because $0 < U \leq a$), which is a contradiction, since $c < U \leq a$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 3: $p^s - p^{s-k} + 2 \leq c \leq p^s - p^{s-k} + p^{s-k-1}$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_6) = 4p^k$, and

$$\begin{aligned} c &= p^s - p^{s-k} + 2 \\ &= p^{s-k}(3p^k - 1) - 2p^s + 2 \\ &\geq p^2(3p^k - 1) - 2p^s + 2 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\geq 4(3p^k - 1) - 2p^s + 2 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(\mathcal{C}_6) - 2p^s - 2. \end{aligned}$$

Now, $c \geq 3d_{sp}(\mathcal{C}_6) - U - a - 6$ if and only if $a + U \geq 2p^s - 4$, i.e., equality when $a + U = 2p^s - 4$. Thus, equality occurs when $p = 2, k = s-2, a + U = 2p^s - 4$, i.e., $c = 2^s - 2$ and $a + U = 2^{s+1} - 4$, i.e., $a + U = 2c$. But we have $U \leq a$, i.e., $2U \leq a + U$, i.e., $2U \leq 2c$, which implies that $U \leq c$, which is a contradiction, since $c < U$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 4: $p^s - pr + \sigma r + 1 \le c \le p^s - pr + (\sigma+1)r$, where $r = p^{s-k-1}, 0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_6) = 2(\sigma+2)p^k$, and

$$\begin{aligned}
c &\ge p^s - p^{s-k} + \sigma p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + \sigma p^{s-k-1} + 1 \\
&\ge p^2(3p^k - 1) - 2p^s + \sigma p + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\ge (\sigma+2)^2(3p^k - 1) - 2p^s + \sigma(\sigma+2) + 1 \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+1)(\sigma+2)p^k - 2p^s + (\sigma+2)(3p^k - 2) + 1 \\
&\ge 6(\sigma+2)p^k - 2p^s + 3(3p^k - 2) + 1 \\
&\quad \times (\text{equality when } \sigma = 1) \\
&\ge 3d_{sp}(\mathcal{C}_6) - 2p^s + 4 \ (\text{equality when } k = 0).
\end{aligned}$$

Now, $c \ge 3d_{sp}(\mathcal{C}_6) - U - a - 6$ if and only if $a + U \ge 2p^s - 10$, i.e., equality when $a + U = 2p^s - 10$. Thus, equality occurs when $\sigma = 1, p = 3, k = 0, s = 2, a + U = 2p^s - 10$, i.e., $a + U = 8$ and $c = 4$, i.e., $a + U = 2c$. But we have $U \le a$, i.e., $2U \le a + U$, i.e., $2U \le 2c$, which implies that $U \le c$, which is a contradiction, since $c < U$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 5: $c = p^s - p + \sigma$, where $0 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_6) = (\sigma+2)p^{s-1}$, and

$$\begin{aligned}
c &= p^s - p + \sigma \\
&= p(3p^{s-1} - 1) - 2p^s + \sigma \\
&\ge (\sigma+2)(3p^{s-1} - 1) - 2p^s + \sigma \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+2)p^{s-1} - 2p^s - 2 \\
&= 3d_{sp}(\mathcal{C}_6) - 2p^s - 2.
\end{aligned}$$

Now, $c \ge 3d_{sp}(\mathcal{C}_6) - U - a - 6$ if and only if $a + U \ge 2p^s - 4$, i.e., equality when $a + U = 2p^s - 4$. Thus, equality occurs when $\sigma = p-2, a + U = 2p^s - 4$, i.e., $c = p^s - 2$ and $a + U = 2p^s - 4$, i.e., $a + U = 2c$. But we have $U \le a$, i.e., $2U \le a + U$, i.e., $2U \le 2c$, which implies that $U \le c$, which is a contradiction, since $c < U$. Thus, no MDS symbol-pair constacyclic code exists in this case. Hence, MDS symbol-pair code does not exist for γ-constacyclic codes of Type 6. This completes the proof. □

G. **Type 7 ($\mathcal{C}_7$)**:

Here, we have $\mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$, where $0 \leq b < a \leq p^s-1$, $0 \leq t_1 < b$, $0 \leq t_2 < b$, $0 \leq t_3 < b$, either $h_1(x), h_2(x), h_3(x)$ are 0 or are units in $\mathcal{R}_\gamma$. We note, by Theorem 3.3, that $|\mathcal{C}_7| = p^{m(3p^s-a-b-W)}$. From this and by (2.2), we see that the code $\mathcal{C}_7$ is a symbol-pair MDS code if and only if $p^{m(3p^s-a-b-W)} = p^{3m(p^s-d_{sp}(\mathcal{C}_7)+2)}$, which holds if and only if

$$W = 3d_{sp}(\mathcal{C}_7) - b - a - 6.$$

Hence, follows the theorem.

Theorem 5.17 Let $\mathcal{C}_7 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x)\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 7 (as classified in Theorem 3.1). Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $W = 3d_{sp}(\mathcal{C}_7) - b - a - 6$. The symbol-pair distance $d_{sp}(\mathcal{C}_7)$ of Type 7 γ-constacyclic code is established in Theorem 5.6. Now, we consider the cases according to the range of W.

Case 1: $W = 0$, then $d_{sp}(\mathcal{C}_7) = 2$. Thus $\mathcal{C}_7$ is a symbol-pair MDS code if and only if $a = -b$, which is not possible.

Case 2: $W = p^s - p^{s-k} + 1$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_7) = 3p^k$, and

$$\begin{aligned}
W &= p^s - p^{s-k} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + 1 \\
&\geq p^2(3p^k - 1) - 2p^s + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\geq 4(3p^k - 1) - 2p^s + 1 \ (\text{equality when } p = 2) \\
&= 3d_{sp}(\mathcal{C}_7) - 2p^s + 3p^k - 3 \\
&\geq 3d_{sp}(\mathcal{C}_7) - 2p^s \ (\text{equality when } k = 0)
\end{aligned}$$

Now, $W \geq 3d_{sp}(\mathcal{C}_7) - b - a - 6$ if and only if $a + b \geq 2p^s - 6$, i.e., equality when $a + b = 2p^s - 6$. Thus, equality occurs when $p = 2, k = 0, s = 2, a + b = 2p^s - 6$, i.e., $W = 1$ and $a + b = 2$, i.e., $a = 2$ and $b = 0$ (because $0 \leq b < a$), which is a contradiction, since $W \leq b$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 3: $p^s - p^{s-k} + 2 \le W \le p^s - p^{s-k} + p^{s-k-1}$, where $0 \le k \le s-2$. Then $d_{sp}(\mathcal{C}_7) = 4p^k$, and

$$\begin{aligned} W &= p^s - p^{s-k} + 2 \\ &= p^{s-k}(3p^k - 1) - 2p^s + 2 \\ &\ge p^2(3p^k - 1) - 2p^s + 2 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\ge 4(3p^k - 1) - 2p^s + 2 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(\mathcal{C}_7) - 2p^s - 2. \end{aligned}$$

Now, $W \ge 3d_{sp}(\mathcal{C}_7) - b - a - 6$ if and only if $a + b \ge 2p^s - 4$, i.e., equality when $a + b = 2p^s - 4$. Thus, equality occurs when $p = 2, k = s-2, a+b = 2p^s-4$, i.e., $W = 2^s - 2$ and $a+b = 2^{s+1}-4$, i.e., $a+b = 2W$. But we have $b < a$, i.e., $2b < a+b$, i.e., $2b < 2W$, which implies that $b < W$, which is a contradiction, since $W \le b$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 4: $p^s - pr + \sigma r + 1 \le W \le p^s - pr + (\sigma+1)r$, where $r = p^{s-k-1}, 0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_7) = 2(\sigma+2)p^k$, and

$$\begin{aligned} W &\ge p^s - p^{s-k} + \sigma p^{s-k-1} + 1 \\ &= p^{s-k}(3p^k - 1) - 2p^s + \sigma p^{s-k-1} + 1 \\ &\ge p^2(3p^k - 1) - 2p^s + \sigma p + 1 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\ge (\sigma+2)^2(3p^k - 1) - 2p^s + \sigma(\sigma+2) + 1 \\ &\quad \times (\text{equality when } \sigma = p-2) \\ &= 3(\sigma+1)(\sigma+2)p^k - 2p^s + (\sigma+2)(3p^k - 2) + 1 \\ &\ge 6(\sigma+2)p^k - 2p^s + 3(3p^k - 2) + 1 \\ &\quad \times (\text{equality when } \sigma = 1) \\ &\ge 3d_{sp}(\mathcal{C}_7) - 2p^s + 4 \ (\text{equality when } k = 0). \end{aligned}$$

Now, $W \ge 3d_{sp}(\mathcal{C}_7) - b - a - 6$ if and only if $a + b \ge 2p^s - 10$, i.e., equality when $a + b = 2p^s - 10$. Thus, equality occurs when $\sigma = 1, p = 3, k = 0, s = 2, a+b = 2p^s-10$, i.e., $a+b = 8$ and $W = 4$, i.e., $a+b = 2W$. But we have $b < a$, i.e., $2b < a+b$, i.e., $2b < 2W$, which implies that $b < W$, which is a contradiction, since $W \le b$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 5: $W = p^s - p + \sigma$, where $0 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_7) = (\sigma+2)p^{s-1}$, and

$$\begin{aligned} W &= p^s - p + \sigma \\ &= p(3p^{s-1}-1) - 2p^s + \sigma \\ &\ge (\sigma+2)(3p^{s-1}-1) - 2p^s + \sigma \\ &\quad \times (\text{equality when } \sigma = p-2) \\ &= 3(\sigma+2)p^{s-1} - 2p^s - 2 \\ &= 3d_{sp}(\mathcal{C}_7) - 2p^s - 2. \end{aligned}$$

Now, $W \ge 3d_{sp}(\mathcal{C}_7) - b - a - 6$ if and only if $a + b \ge 2p^s - 4$, i.e., equality when $a + b = 2p^s - 4$. Thus, equality occurs when $\sigma = p-2, a+b = 2p^s-4$, i.e., $W = p^s - 2$ and $a + b = 2p^s - 4$, i.e., $a+b = 2W$. But we have $b < a$, i.e., $2b < a+b$, i.e., $2b < 2W$, which implies that $b < W$, which is a contradiction, since $W \le b$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Hence, MDS symbol-pair code does not exist for γ-constacyclic codes of Type 7. This completes the proof. □

H. **Type 8 ($\mathcal{C}_8$)**:

Here, we have $\mathcal{C}_8 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$, where $0 \le c < b < a \le p^s - 1$, $0 \le t_1 < b$, $0 \le t_2 < c$, $0 \le t_3 < c$, either $h_1(x), h_2(x), h_3(x)$ are 0 or are units in $\mathcal{R}_\gamma$. And $|\mathcal{C}_8| = p^{m(3p^s-a-b-c)}$. Thus by (2.2), $\mathcal{C}_8$ is a symbol-pair MDS code if and only if $p^{m(3p^s-a-b-c)} = p^{3m(p^s-d_{sp}(\mathcal{C}_8)+2)}$, i.e.,

$$c = 3d_{sp}(\mathcal{C}_8) - b - a - 6.$$

Hence, follows the theorem.

Theorem 5.18 Let $\mathcal{C}_8 = \langle (x-\gamma_0)^a + u(x-\gamma_0)^{t_1}h_1(x) + u^2(x-\gamma_0)^{t_2}h_2(x), u(x-\gamma_0)^b + u^2(x-\gamma_0)^{t_3}h_3(x), u^2(x-\gamma_0)^c\rangle$ be a γ-constacyclic codes of length p^s over $\mathcal{R}$ of Type 8 (as classified in Theorem 3.1). Then no MDS symbol-pair constacyclic code exists.

Proof We get MDS code for $c = 3d_{sp}(\mathcal{C}_8) - b - a - 6$. The symbol-pair distance $d_{sp}(\mathcal{C}_8)$ of Type 8 γ-constacyclic code is established in Theorem 5.7. Now, we consider the cases according to the range of c.

Case 1: $c = 0$, then $d_{sp}(\mathcal{C}_8) = 2$. Thus $\mathcal{C}_8$ is a symbol-pair MDS code if and only if $a = -b$, which is not possible.

Case 2: $c = p^s - p^{s-k} + 1$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_8) = 3p^k$, and

$$\begin{aligned} c &= p^s - p^{s-k} + 1 \\ &= p^{s-k}(3p^k - 1) - 2p^s + 1 \\ &\geq p^2(3p^k - 1) - 2p^s + 1 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\geq 4(3p^k - 1) - 2p^s + 1 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(\mathcal{C}_8) - 2p^s + 3p^k - 3 \\ &\geq 3d_{sp}(\mathcal{C}_8) - 2p^s \ (\text{equality when } k = 0) \end{aligned}$$

Now, $c \geq 3d_{sp}(\mathcal{C}_8) - b - a - 6$ if and only if $a + b \geq 2p^s - 6$, i.e., equality when $a + b = 2p^s - 6$. Thus, equality occurs when $p = 2, k = 0, s = 2, a + b = 2p^s - 6$, i.e., $c = 1$ and $a + b = 2$, i.e., $a = 2$ and $b = 0$ (because $0 \leq b < a$), which is a contradiction, since $c < b$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 3: $p^s - p^{s-k} + 2 \leq c \leq p^s - p^{s-k} + p^{s-k-1}$, where $0 \leq k \leq s-2$. Then $d_{sp}(\mathcal{C}_8) = 4p^k$, and

$$\begin{aligned} c &= p^s - p^{s-k} + 2 \\ &= p^{s-k}(3p^k - 1) - 2p^s + 2 \\ &\geq p^2(3p^k - 1) - 2p^s + 2 \\ &\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\ &\geq 4(3p^k - 1) - 2p^s + 2 \ (\text{equality when } p = 2) \\ &= 3d_{sp}(\mathcal{C}_8) - 2p^s - 2. \end{aligned}$$

Now, $c \geq 3d_{sp}(\mathcal{C}_8) - b - a - 6$ if and only if $a + b \geq 2p^s - 4$, i.e., equality when $a + b = 2p^s - 4$. Thus, equality occurs when $p = 2, k = s-2, a + b = 2p^s - 4$, i.e., $c = 2^s - 2$ and $a + b = 2^{s+1} - 4$, i.e., $a + b = 2c$. But we have $b < a$, i.e., $2b < a + b$, i.e., $2b < 2c$, which implies that $b < c$, which is a contradiction, since $c < b$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 4: $p^s - pr + \sigma r + 1 \le c \le p^s - pr + (\sigma+1)r$, where $r = p^{s-k-1}, 0 \le k \le s-2$ and $1 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_8) = 2(\sigma+2)p^k$, and

$$\begin{aligned}
c &\ge p^s - p^{s-k} + \sigma p^{s-k-1} + 1 \\
&= p^{s-k}(3p^k - 1) - 2p^s + \sigma p^{s-k-1} + 1 \\
&\ge p^2(3p^k - 1) - 2p^s + \sigma p + 1 \\
&\quad \times (\text{equality when } k = s-2, \text{or } s = 2) \\
&\ge (\sigma+2)^2(3p^k - 1) - 2p^s + \sigma(\sigma+2) + 1 \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+1)(\sigma+2)p^k - 2p^s + (\sigma+2)(3p^k - 2) + 1 \\
&\ge 6(\sigma+2)p^k - 2p^s + 3(3p^k - 2) + 1 \\
&\quad \times (\text{equality when } \sigma = 1) \\
&\ge 3d_{sp}(\mathcal{C}_8) - 2p^s + 4 \ (\text{equality when } k = 0).
\end{aligned}$$

Now, $c \ge 3d_{sp}(\mathcal{C}_8) - b - a - 6$ if and only if $a + b \ge 2p^s - 10$, i.e., equality when $a + b = 2p^s - 10$. Thus, equality occurs when $\sigma = 1, p = 3, k = 0, s = 2, a + b = 2p^s - 10$, i.e., $a + b = 8$ and $c = 4$, i.e., $a + b = 2c$. But we have $b < a$, i.e., $2b < a + b$, i.e., $2b < 2c$, which implies that $b < c$, which is a contradiction, since $c < b$. Thus, no MDS symbol-pair constacyclic code exists in this case.

Case 5: $c = p^s - p + \sigma$, where $0 \le \sigma \le p-2$. Then $d_{sp}(\mathcal{C}_8) = (\sigma+2)p^{s-1}$, and

$$\begin{aligned}
c &= p^s - p + \sigma \\
&= p(3p^{s-1} - 1) - 2p^s + \sigma \\
&\ge (\sigma+2)(3p^{s-1} - 1) - 2p^s + \sigma \\
&\quad \times (\text{equality when } \sigma = p-2) \\
&= 3(\sigma+2)p^{s-1} - 2p^s - 2 \\
&= 3d_{sp}(\mathcal{C}_8) - 2p^s - 2.
\end{aligned}$$

Now, $c \ge 3d_{sp}(\mathcal{C}_8) - b - a - 6$ if and only if $a + b \ge 2p^s - 4$, i.e., equality when $a + b = 2p^s - 4$. Thus, equality occurs when $\sigma = p-2, a + b = 2p^s - 4$, i.e., $c = p^s - 2$ and $a + b = 2p^s - 4$, i.e., $a + b = 2c$. But we have $b < a$, i.e., $2b < a + b$, i.e., $2b < 2c$, which implies that $b < c$, which is a contradiction, since $c < b$. Thus, no MDS symbol-pair constacyclic code exists in this case. Hence, MDS symbol-pair code does not exist for γ-constacyclic codes of Type 8. This completes the proof. □

5.4 Some examples

In this section, we present some examples of symbol-pair distance distributions of constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m} (u^3 = 0)$.

Example 5.2 Using the results in Section 5.2, we list the symbol-pair distances d_{sp} of all γ-constacyclic codes $\mathcal{C}$ of length 3 over the chain ring $\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$, where $\gamma \in \{1, 2\}$. We also give all MDS symbol-pair and non-MDS symbol-pair codes (Table 5.8). In all codes we have $h_0, a_0, b_0, c_0 \in \{1, 2\}$ and $b_1 \in \{0, 1, 3\}$.

Example 5.3 Let us consider the example 5.1. Here, we consider symbol-pair γ-constacyclic codes of length 49 over the chain ring $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$, where $p = 7$, $m = 1$, $s = 2$ and $\gamma \in \mathbb{F}_7^*$. In example 5.1, we determined all the symbol-pair distances for all the ranges of τ, L, ω, V, W and c. From the values of τ, L, ω, V, W, c and $d_{sp}(C_i)$, where $i \in \{1, \ldots, 8\}$, we have the following list of MDS symbol-pair γ-constacyclic codes:

- $\langle 1\rangle$,
- $\langle (x-\gamma)\rangle$,
- $\langle (x-\gamma)^2\rangle$,
- $\langle (x-\gamma)^{47}\rangle$,
- $\langle (x-\gamma) + b_0u^2\rangle$,
- $\langle (x-\gamma)^2 + b_0u^2 + b_1u^2(x-\gamma)\rangle$,
- $\langle (x-\gamma)^2 + b_0u^2(x-\gamma)\rangle$,
- $\langle (x-\gamma)^{47} + b_0u^2(x-\gamma)^{45} + b_1u^2(x-\gamma)^{46}\rangle$,
- $\langle (x-\gamma)^{47} + b_0u^2(x-\gamma)^{46}\rangle$,
- $\langle (x-\gamma) + a_0u\rangle$,
- $\langle (x-\gamma) + a_0u + b_0u^2\rangle$,
- $\langle (x-\gamma)^2 + a_0u + a_1u(x-\gamma)\rangle$,
- $\langle (x-\gamma)^2 + a_0u + a_1u(x-\gamma) + b_0u^2 + b_1u^2(x-\gamma)\rangle$,
- $\langle (x-\gamma)^2 + a_0u + a_1u(x-\gamma) + b_0u^2(x-\gamma)\rangle$,
- $\langle (x-\gamma)^2 + a_0u(x-\gamma)\rangle$,
- $\langle (x-\gamma)^2 + a_0u(x-\gamma) + b_0u^2 + b_1u^2(x-\gamma)\rangle$,
- $\langle (x-\gamma)^2 + a_0u(x-\gamma) + b_0u^2(x-\gamma)\rangle$,
- $\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{45} + a_1u(x-\gamma)^{46}\rangle$,

- $\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{45} + a_1u(x-\gamma)^{46} + u^2(x-\gamma)^{t_2}\sum_{j=0}^{46-t_2} b_j(x-\gamma)^j\rangle$,
- $\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{46}\rangle$,
- $\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{46} + u^2(x-\gamma)^{t_2}\sum_{j=0}^{46-t_2} b_j(x-\gamma)^j\rangle$.

where $0 \leq t_2 \leq 46$, $a_0, b_0 \in \{1,\ldots,6\}$ and $a_1, b_j \in \{0,1,\ldots,6\}$.

$\rightsquigarrow$ Table 5.9 shows the representation of some γ-constacyclic codes of length 49 over the chain ring $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$, together with the symbol-pair distances d_{sp} of such codes. We also give all MDS symbol-pair and non-MDS symbol-pair codes.

Table 5.8 – Symbol-pair distance of γ-constacyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$

Ideal $(\mathcal{C})$	d_{sp}	MDS
$\rightarrow$ Type 1 :		
$*\langle 0\rangle$	0	No
$*\langle 1\rangle$	2	Yes
$\rightarrow$ Type 2 :		
$*\langle u^2\rangle$	2	No
$*\langle u^2(x-\gamma)\rangle$	3	No
$*\langle u^2(x-\gamma)^2\rangle$	3	No
$\rightarrow$ Type 3 :		
$*\langle u\rangle$	2	No
$*\langle u(x-\gamma)\rangle$; $*\langle u(x-\gamma)+h_0u^2\rangle$; $*\langle u(x-\gamma)^2+h_0u^2\rangle$	3	No
$*\langle u(x-\gamma)^2\rangle$;$*\langle u(x-\gamma)^2+h_0u^2(x-\gamma)\rangle$	3	No
$\rightarrow$ Type 4 :		
$*\langle u(x-\gamma),u^2\rangle$; $*\langle u(x-\gamma)^2,u^2\rangle$	2	No
$*\langle u(x-\gamma)^2,u^2(x-\gamma)\rangle$	3	No
$\rightarrow$ Type 5 :		
$*\langle (x-\gamma)\rangle$; $*\langle (x-\gamma)+b_0u^2\rangle$; $*\langle (x-\gamma)+a_0u\rangle$; $*\langle (x-\gamma)+a_0u+b_0u^2\rangle$	3	Yes
$*\langle (x-\gamma)^2\rangle$; $*\langle (x-\gamma)^2+b_0u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2(x-\gamma)\rangle$	3	No
$*\langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2+b_1u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma)\rangle$	3	No
$*\langle (x-\gamma)^2+b_0u^2\rangle$; $*\langle (x-\gamma)^2+a_0u\rangle$; $*\langle (x-\gamma)^2+a_0u+b_0u^2\rangle$	3	No
$\rightarrow$ Type 6 :		
$*\langle (x-\gamma),u^2\rangle$; $*\langle (x-\gamma)^2,u^2\rangle$; $*\langle (x-\gamma)+a_0u,u^2\rangle$; $*\langle (x-\gamma)^2+a_0u,u^2\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma),u^2\rangle$	2	No
$*\langle (x-\gamma)^2,u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma),u^2(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+a_0u(x-\gamma)+b_0u^2,u^2(x-\gamma)\rangle$	3	No
$\rightarrow$ Type 7 :		
$*\langle (x-\gamma),u\rangle$; $*\langle (x-\gamma)^2,u\rangle$	2	No
$*\langle (x-\gamma)^2,u(x-\gamma)\rangle$; $*\langle (x-\gamma)^2,u(x-\gamma)+c_0u^2\rangle$	3	No
$*\langle (x-\gamma)^2+b_0u^2,u(x-\gamma)\rangle$; $*\langle (x-\gamma)^2+b_0u^2,u(x-\gamma)+c_0u^2\rangle$	3	No
$\rightarrow$ Type 8 :		
$*\langle (x-\gamma)^2,u(x-\gamma),u^2\rangle$	2	No

Table 5.9 – Some γ-constacyclic codes of length **49** over the chain ring $\mathbb{F}_7 + u\mathbb{F}_7 + u^2\mathbb{F}_7$.

Ideal ($\mathcal{C}$)	d_{sp}	MDS
↬ Type 1 :		
$*\langle 0\rangle$	0	No
$*\langle 1\rangle$	2	Yes
↬ Type 2 :		
$*\langle u^2(x-\gamma)^{30}\rangle$	12	No
$*\langle u^2(x-\gamma)^{46}\rangle$	42	No
$*\langle u^2(x-\gamma)^{48}\rangle$	49	No
↬ Type 3 :		
$*\langle u(x-\gamma)^{11}\rangle$	6	No
$*\langle u(x-\gamma)^{30} + h_0u^2(x-\gamma)^{27} + h_1u^2(x-\gamma)^{28} + h_2u^2(x-\gamma)^{29}\rangle$	12	No
$*\langle u(x-\gamma)^{48} + h_0u^2(x-\gamma)^{42}\rangle$	21	No
↬ Type 4 :		
$*\langle u(x-\gamma)^{48}, u^2(x-\gamma)^5\rangle$	4	No
$*\langle u(x-\gamma)^{31}, u^2(x-\gamma)^{29}\rangle$	10	No
$*\langle u(x-\gamma)^{46} + h_0u^2(x-\gamma)^{42} + h_1u^2(x-\gamma)^{43}, u^2(x-\gamma)^{44}\rangle$	28	No
↬ Type 5 :		
$*\langle (x-\gamma) + a_0u + b_0u\rangle$	3	Yes
$*\langle (x-\gamma)^2 + a_0u(x-\gamma)\rangle$	4	Yes
$*\langle (x-\gamma)^2 + a_0u + a_1u(x-\gamma) + b_0u^2 + b_1u^2(x-\gamma)\rangle$	4	Yes
$*\langle (x-\gamma)^{44}\rangle$	28	No
$*\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{45} + a_1u(x-\gamma)^{46} + b_0u^2(x-\gamma)^{46}\rangle$	49	Yes
$*\langle (x-\gamma)^{47} + a_0u(x-\gamma)^{46} + b_0u^2(x-\gamma)^{45} + b_1u^2(x-\gamma)^{46}\rangle$	49	Yes
↬ Type 6 :		
$*\langle (x-\gamma)^{44} + b_0u^2(x-\gamma)^{41}, u^2(x-\gamma)^{42}\rangle$	14	No
$*\langle (x-\gamma)^{48} + a_0u(x-\gamma)^{47} + b_0u^2(x-\gamma)^{42} + b_1u^2(x-\gamma)^{43}, u^2(x-\gamma)^{44}\rangle$	28	No
$*\langle (x-\gamma)^{48}, u^2(x-\gamma)^{47}\rangle$	49	No
↬ Type 7 :		
$*\langle (x-\gamma)^{31} + a_0u(x-\gamma)^{18} + a_1u(x-\gamma)^{19}, u(x-\gamma)^{20}\rangle$	8	No
$*\langle (x-\gamma)^{46}, u(x-\gamma)^{44}\rangle$	28	No
$*\langle (x-\gamma)^{47} + b_0u^2(x-\gamma)^{43} + b_1u^2(x-\gamma)^{44}, u(x-\gamma)^{46}\rangle$	35	No
↬ Type 8 :		
$*\langle (x-\gamma)^{39} + a_0u(x-\gamma)^{18} + a_1u(x-\gamma)^{19}, u(x-\gamma)^{20} + c_0u^2(x-\gamma)^7, u^2(x-\gamma)^8\rangle$	6	No
$*\langle (x-\gamma)^{34}, u(x-\gamma)^{29} + c_0u^2(x-\gamma)^{24} + c_1u^2(x-\gamma)^{25}, u^2(x-\gamma)^{26}\rangle$	10	No
$*\langle (x-\gamma)^{48}, u(x-\gamma)^{47}, u^2(x-\gamma)^{46}\rangle$	42	No

Chapter 6

Conclusion and future work

Algebraic codes are of great interest to coding theorists, as they are easy to construct, encode and decode. Classically, algebraic codes have been mainly studied over finite fields. Codes over finite rings got a serious attention in recent years. This motivated many researchers to study constacyclic codes over finite chain rings. However, the algebraic structure of constacyclic codes is known only for some special lengths and over certain special classes of finite chain rings.

To study error-detecting and error-correcting properties of a code with respect to various communication channels, several distances (e.g. Hamming distance, symbol-pair distance, etc.) have been introduced and studied in coding theory. 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 distances.

6.1 Conclusion

Let p be a prime, s, m be positive integers, γ be a nonzero element of the finite field $\mathbb{F}_{p^m}$, and let $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3 \rangle$ be the finite commutative chain ring with unity.

Below we summarize some of the main results derived in the thesis.

$\mapsto$ Algebraic structures of all repeated-root γ-constacyclic codes of prime power lengths over the finite commutative chain ring $\mathcal{R} = \mathbb{F}_{p^m}[u]/\langle u^3 \rangle$ are established, where γ is a nonzero element of the field $\mathbb{F}_{p^m}$. Their sizes are also determined.

$\mapsto$ Hamming distances of repeated-root γ-constacyclic codes of prime power lengths over $\mathcal{R}$ are explicitly determined. Using this result, all MDS Hamming codes belonging

to this special class of constacyclic codes are listed.

$\mapsto$ Symbol-pair distances of all repeated-root γ-constacyclic codes of prime power lengths over $\mathcal{R}$ are obtained. We also identified all MDS constacyclic codes of length p^s over $\mathcal{R}$ with respect to symbol-pair distance.

6.2 Future work

Some of the interesting open problems in this research direction are listed below:

$*$ It would be interesting to determine dual codes of γ-constacyclic codes of length p^s over $\mathcal{R}$ and to study their duality properties.

$*$ In [29], Ding et al. generalized the symbol-pair codes to b-symbol codes. Thus, it would be interesting to determine b-symbol distances of γ-constacyclic codes of length p^s over $\mathcal{R}$. As a generalization of MDS codes and MDS symbol-pair codes, MDS b-symbol codes also have the best possible error-correction capability. it would also be interesting to identify MDS b-symbol codes within this class of constacyclic codes.

$*$ Another interesting problem would be to study algebraic structures of all γ-constacyclic codes of length $N = np^s$ over the ring $\mathcal{R}$, where n is a positive integer with $\gcd(n, p) = 1$. It would also be interesting to obtain their Hamming distances, symbol-pair distances and b-symbol distances, and as an application, we will identify all MDS constacyclic codes of length np^s with respect to those distances.

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] M. F. Atiyah, I. G. MacDonald, Introduction to commutative algebra, Addison Wesley Publishing Company.

[4] C. Bachoc, Application of coding theory to the construction of modular lattices, J. Comb. Theory, Ser. A 78, pp. 92–119, 1997.

[5] 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.

[6] 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.

[7] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, International Workshop on Coding and Cryptography (WCC 2001) (Paris), Discrete Appl. Math. 128, pp. 27–46, 2003.

[8] 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.

[9] B. Boudine, J. Laaouine and M. E. Charkani, New quantum codes from cyclic codes over finite chain ring of length 3. Asian-European Journal of Mathematics, p. 2150175, 2021.

[10] A. R. Calderbank, A. R. Hammons Jr., P. V. Kumar, N. J. A. Sloane and P. Solé, A linear construction for certain Kerdock and Preparata codes, Bull. Amer. Math. Soc. 29(2), pp. 218–222, Oct. 1993.

[11] Y. Cao, On constacyclic codes over finite chain rings, Finite Fields Appl. 24, pp. 124–135, Nov. 2013.

[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] M. E. Charkani, H. Q. Dinh, J. Laaouine and W. Yamaka, Symbol-Pair Distance of Repeated-Root Constacyclic Codes of Prime Power Lengths over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, Mathematics, 2021.

[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] W.E. Clark, A coefficient ring of finite commutative chain rings, Proc. Amer. Math. Soc. 33, pp. 25–27, 1972.

[17] H. Q. Dinh, Negacyclic codes of length 2^s over Galois rings, IEEE Trans. Inf. Theory 51(12), pp. 4252–4262, Dec. 2005.

[18] 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.

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

[20] 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.

[21] 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.

[22] H. Q. Dinh, On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions, Finite Fields Appl. 14, pp. 22–40, 2008.

[23] H. Q. Dinh, Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inf. Theory 55, pp. 1730–1740, 2009.

[24] H. Q. Dinh, S. Dhompongsa, S. Sriboonchitta, Repeated-root constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/\langle u^a \rangle$ and their duals. Discrete Math. 339, pp. 1706–1715, 2016.

[25] H. Q. Dinh, X. Wang, H. Liu, and S. Sriboonchitta, On the b-distance of repeated-root constacyclic codes of prime power lengths, Discrete Math., vol. 343, no. 4, Art. no. 111780, Apr. 2020.

[26] H. Q. Dinh, B. T. Nguyen, A. K. Singh, and S. Sriboonchitta, Hamming and symbol-pair distances of repeated-root constacyclic codes of prime power lengths over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, IEEE Communications Letters, 22, pp. 2400–2403, 2018.

[27] H. Q. Dinh, P. Kumam, P. Kumar, S. Satpati, A. K. Singh and W. Yamaka, MDS Symbol-Pair Repeated-Root Constacylic Codes of Prime Power Lengths Over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, IEEE Access, 7, pp. 145039–145048, 2019.

[28] H. Q. Dinh, J. Laaouine, M. E. Charkani and S. Chinnakum, Hamming distance of constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, IEEE Access, 2021.

[29] 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.

[30] S. T. Dougherty, Y.H. Park, On modular cyclic codes, Finite Fields Appl. 13, pp. 31–57, 2007.

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

[32] 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.

[33] W. C. Huffman and V. Pless, Fundamentals of error-correcting codes, Cambridge University Press, New York, 2003.

[34] K. Guenda and T. A. Gulliver, MDS and self-dual codes over rings, Finite Fields Appl. 18(6), pp. 1061–1075, 2012.

[35] 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.

[36] 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.

[37] J. Laaouine, M. E. Charkani and L. Wang, Complete classification of repeated-root σ-constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/\langle u^3\rangle$, Discrete Mathematics, vol. 344, no 6, pp. 112325, 2021.

[38] J. Laaouine and M. E. Charkani, A note on "H. Q. Dinh et al., Hamming distance of repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$", Applicable Algebra in Engineering, Communication and Computing, pp. 1–7, 2021.

[39] J. Laaouine, On the Hamming and Symbol-Pair Distance of Constacyclic Codes of Length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. In: International Conference on Advanced Communication Systems and Information Security. Springer, Cham, pp. 137–154, 2019.

[40] J. Laaouine, On MDS symbol-pair γ-constacyclic codes of length p^s over $\mathbb{F}_{p^m}[u]/\langle u^2\rangle$, International Journal of Computer Science and Applications, accepted for publication, 2020.

[41] X. Liu and X. Xu, Some classs of repeated-rout Constacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$, J. Korean Math. Soc. 51, pp. 853–866, 2014.

[42] 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.

[43] F. J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes. 10th Impression, North-Holland, Amsterdam, 1998.

[44] B.R. McDonald, Finite rings with identity, Pure and Applied Mathematics, Vol. 28, Marcel Dekker, New York, 1974.

[45] A. A. Nechaev, Kerdock code in a cyclic form, Discrete Math. Appl. 1(4), pp. 365–384, 1991.

[46] 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.

[47] 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.

[48] I. Siap, Linear codes over $\mathbb{F}_2+u\mathbb{F}_2$ and their complete weight enumerators, in: Codes and Designs, Columbus, OH, 2000, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 10, de Gruyter, pp. 259–271, Berlin, 2002.

[49] 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.

[50] 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.

[51] R. C. Singleton, Maximum distance q-ary codes, IEEE Trans. Inform. Theory 10(2), pp. 116–118, Apr. 1964.

[52] R. Sobhani, Z. Sun, L. Wang, S. Zhu, A note on complete classification of $(\delta+\alpha u2)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$, arXiv:1702.04694 [cs.IT].

[53] 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.

[54] P. Udaya, M.U. Siddiqi, Optimal large linear complexity frequency hopping patterns derived from polynomials residue class ring, IEEE Trans. Inform. Theory 44, pp. 1492–1503, 1998.

[55] 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.

[56] 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.