รหัสสกิวคอนสตาไซคลิกบนริงลูกโซ่จำกัด

นายสมพงค์ จิตต์มั่น

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรดุษฎีบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

SKEW-CONSTACYCLIC CODES OVER FINITE CHAIN RINGS

Mr. Somphong Jitman

A Dissertation Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy Program in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2010

Thesis Title	: SKEW-CONSTACYCLIC CODES OVER FINITE CHAIN RINGS
By	: Mr. Somphong Jitman
Field of Study	: Mathematics
Thesis Advisor	: Associate Professor Patanee Udomkavanich, Ph.D.
Thesis Co-Advisor	: Professor San Ling, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Doctoral Degree

S. Hannongbua
..... Dean of Faculty of Science
(Professor Supot Hannongbua, Dr. rer. nat.)

THESIS COMMITTEE

Ajchara Harnchoowong
..... Chairman
(Associate Professor Ajchara Harnchoowong, Ph.D.)

P. Udomkavanich
..... Thesis Advisor
(Associate Professor Patanee Udomkavanich, Ph.D.)

..... Thesis Co-Advisor
(Professor San Ling, Ph.D.)

Sajee Pianskool
..... Examiner
(Assistant Professor Sajee Pianskool, Ph.D.)

Yotsanan Meemark
..... Examiner
(Assistant Professor Yotsanan Meemark, Ph.D.)

Narong Punnim
..... External Examiner
(Professor Narong Punnim, Ph.D.)

สมพงค์ จิตต์มั่น : รหัสสกิวคอนสตาไซคลิกบนริงลูกโซ่จำกัด. (SKEW-CONSTACYCLIC CODES OVER FINITE CHAIN RINGS) อ. ที่ปรึกษาวิทยานิพนธ์หลัก : รศ. ดร. พัฒนี อุดมกะวานิช, อ. ที่ปรึกษาวิทยานิพนธ์ร่วม : Prof. San Ling, Ph.D., 68 หน้า.

พหุนามเสมือนบนฟิลด์จำกัดและบนกาลัวริงเป็นเครื่องมือสำหรับศึกษารหัส ในงานวิจัยนี้ เราขยายแนวคิดดังกล่าวโดยศึกษารหัสบนริงลูกโซ่จำกัด $\mathcal{R}_{(p^m,e)} := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$ ซึ่งมีแคแรกเทอริสติกเป็นจำนวนเฉพาะ p พร้อมกันนี้เราศึกษาภาพเกรย์ของรหัสบนริงนี้อีกด้วย

สำหรับยูนิต $\lambda \in \mathcal{R}_{(p^m,e)}$ เรานำเสนอสมบัติของรหัสสกิวคอนสตาไซคลิกแบบอิสระซึ่งสอดคล้องกับ λ เมื่อ $\lambda^2=1$ เราบอกตัวก่อกำเนิดของรหัสคู่กันของรหัสดังกล่าวทั้งแบบยูคลิดและแบบแอร์มีต พร้อมด้วยเงื่อนไขที่จำเป็นและเพียงพอสำหรับรหัสดังกล่าวที่จะเป็นรหัสคู่กันในตัวทั้งสองแบบ สำหรับผลการศึกษาบนริง $\mathcal{R}_{(p^m,2)} := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ เราได้โครงสร้างของทุกรหัสสกิวคอนสตาไซคลิกอย่างสมบูรณ์ ซึ่งนำไปสู่การแสดงตัวก่อกำเนิดของรหัสคู่กันของรหัสสกิวไซคลิกและรหัสสกิวเนกะไซคลิกในพจน์ของตัวก่อกำเนิดของรหัสดั้งเดิม เราแสดงตัวอย่างทั้งหมดของรหัสสกิวไซคลิกความยาว 2 บนริง $\mathcal{R}_{(3,2)}$ พร้อมด้วยรหัสคู่กันแบบยูคลิดและแบบแอร์มีต

เรานิยามการส่งเกรย์เพื่อเชื่อมโยงรหัสบนริง $\mathcal{R}_{(p^m,e)}$ กับรหัสบนฟิลด์ผลหาร เราแสดงว่าภาพเกรย์ของรหัสคอนสตาไซคลิกแบบ $1-u^{e-1}$ เป็นรหัสควอซีไซคลิกซึ่งระยะทางไม่แปรเปลี่ยนบนฟิลด์ผลหาร เมื่อความยาวของรหัสหารด้วย p ไม่ลงตัว เราแสดงเพิ่มเติมว่าภาพเกรย์ของรหัสไซคลิก และรหัสคอนสตาไซคลิกแบบ $1+u^{e-1}$ สมมูลเชิงเรียงสับเปลี่ยนกับรหัสควอซีไซคลิกบนฟิลด์ผลหาร ส่วนสุดท้าย เราให้ข้อสรุปบางประการเกี่ยวกับภาพเกรย์ของรหัสสกิวคอนสตาไซคลิกบนริง $\mathcal{R}_{(p^m,e)}$

ภาควิชา คณิตศาสตร์ ลายมือชื่อนิสิต .....

สาขาวิชา คณิตศาสตร์ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2553 ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์ร่วม .....

5073885523 : MAJOR MATHEMATICS

KEYWORDS : SKEW-CONSTACYCLIC CODE/ CYCLIC CODE/ FINITE CHAIN RING/ SKEW POLYNOMIAL / GRAY MAP

SOMPHONG JITMAN : SKEW-CONSTACYCLIC CODES OVER FINITE CHAIN RINGS. THESIS ADVISOR : ASSOC. PROF. PATANEE UDOMKAVANICH, PH.D., THESIS CO-ADVISOR : PROF. SAN LING, PH.D., 68 pp.

Skew polynomial rings over finite fields and over Galois rings have been used to study codes. In this work, we extend this concept to $\mathcal{R}_{(p^m,e)} := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$, a finite chain ring of prime characteristic p. The Gray images of codes over this ring are also studied.

Given a unit $\lambda \in \mathcal{R}_{(p^m,e)}$, properties of free skew-constacyclic codes are established corresponding to λ. When $\lambda^2=1$, the generators of Euclidean and Hermitian duals of such codes are determined together with necessary and sufficient conditions for them to be Euclidean and Hermitian self-dual. Of more interest are codes over the ring $\mathcal{R}_{(p^m,2)} := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. The structure of all skew-constacyclic codes is completely determined. This allows us to express generators of Euclidean and Hermitian dual codes of skew-cyclic and skew-negacyclic codes in terms of the generators of the original codes. An illustration of all skew cyclic codes of length 2 over $\mathcal{R}_{(3,2)}$ and their Euclidean and Hermitian duals is also provided.

The Gray map is introduced for $\mathcal{R}_{(p^m,e)}$ to link codes over this ring and over its residue field. We prove that the Gray image of an $(1-u^{e-1})$-constacyclic code over $\mathcal{R}_{(p^m,e)}$ is a distance-invariant quasi-cyclic code over its residue field. When the length of codes is not divisible by p, the Gray images of a cyclic code and an $(1+u^{e-1})$-constacyclic code are permutatively equivalent to quasi-cyclic codes over its residue field. Finally, we give descriptions concerning Gray images of some skew-constacyclic codes over $\mathcal{R}_{(p^m,e)}$.

Department : Mathematics Student's Signature Somphong Jitman

Field of Study : Mathematics Advisor's Signature P. Udomkavanich

Academic Year : 2010 Co-Advisor's Signature

ACKNOWLEDGEMENTS

It is a great pleasure to thank my thesis advisor and my thesis co-advisor, associate professor Patanee Udomkavanich and professor San Ling, for their excellent supervisions, helpful advices and very useful helps. Without their constructive suggestions and knowledgeable guidance in this study, this work would never have successfully been completed. I feel very thankful to the committee of my thesis and all the lecturers during my study.

In particular, I would also thank the Development and Promotion of Science and Technology Talents Project (DPST) and School of Physical and Mathematical Sciences, Nanyang Technological University for providing opportunity and financial support.

Finally, my sincere gratitude and appreciation go to my beloved parents for their support and consistent encouragement throughout my study.

CONTENTS

CHAPTER page

CHAPTER I

INTRODUCTION

The ultimate goal of communication systems is to transmit information from the information source to the destination without any errors like noise, bandwidth, attenuation, limitations, inference etc., which are introduced in the channel. One of the ways of detecting and correcting these errors over a noisy communication channel is by applying the art of Error Correcting Codes which were investigated by R. W. Hamming at Bell Laboratories in 1947.

In the early history of the art of Error Correcting Codes, codes were usually taken over finite fields. In the last two decades, an interest has been shown in linear codes over rings and the so-called Gray maps that mapped these codes into codes over finite fields. In an important work [21], Calderbank, Sloane et al. showed that the Kerdock codes, the Preparata codes and Delsart-Goethals codes can be obtained through the Gray images of linear codes over $\mathbb{Z}_4$. Later on, algebraic structures and properties of codes over $\mathbb{F}_2+u\mathbb{F}_2$, $\mathbb{Z}_{p^m}$, Galois rings and generalized rings in notion of finite chain rings have been established in [17] [14], [18], [28], [34], [35], and [37]. In particular, successful applications of modular lattices using codes over a finite chain ring $\mathbb{F}_p+u\mathbb{F}_p$ [4] and constructions of good sequences from polynomial residue class rings [36] have motivated the study of constacyclic codes over a special family of finite chain rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$ (see, for examples, [3], [6], [15], [16], [23] and [30]).

Cyclic codes, negacyclic codes and constacyclic codes form important classes of linear codes due to their rich algebraic structure. Classically, polynomial rings

over finite fields or over finite rings and their ideals are key to determining the algebraic structures of these codes (e.g., [22], [26] and [27]). In [7], skew (non-commutative) polynomial rings have been used to describe the structure of linear codes closed under a skew-cyclic shift, namely, skew-cyclic codes. Later on, in [10], more properties and good examples of such codes have been established. Recently, in [8], that approach has been extended to codes over Galois rings.

Motivated by these works, we generalize the concept of skew-constacyclic codes to over $\mathcal{R}_{(p^m,e)} := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$, the finite chain ring of characteristic p, nilpotency index e and residue field $\mathbb{F}_{p^m}$. Some algebraic tools and techniques are developed. The structure and properties of free skew-constacyclic codes with respect to a unit λ are studied. In particular, when $\lambda^2 = 1$, the structures of their Euclidean and Hermitian dual codes are determined. Moreover, necessary and sufficient conditions for such codes to be Euclidean and Hermitian self-dual are also given. When the nilpotency index of rings is 2, the structure of all skew-constacyclic codes is completely determined over $\mathcal{R}_{(p^m,2)} := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. This allows us to express generators of Euclidean and Hermitian dual codes of skew-cyclic and skew-negacyclic codes in terms of the generators of the original codes.

Codes over finite rings are linked to codes over finite fields using the Gray maps defined in different ways. The classical Gray map over $\mathbb{Z}_4$ is first generalized to finite chain rings in [19]. Qian, Zhang and Zhu have characterized the Gray images of $(1+u)$-constacyclic and cyclic codes over the ring $\mathcal{R}_{(2,2)} = \mathbb{F}_2 + u\mathbb{F}_2$ in [30] and some constacyclic codes over $\mathcal{R}_{(2,3)} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ in [31]. In [3], Amarra and Nemenzo have generalized the results of [30] over $\mathcal{R}_{(p^m,2)} := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. In [11], Congellenmis have introduced $(1-u^{e-1})$-constacyclic codes over $\mathcal{R}_{(2,e)} = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{e-1}\mathbb{F}_2$ and generalized the results of [30] and [31].

In this work, we generalize these concepts to the case over $\mathcal{R}_{(p^m,e)}$. We focus on $(1-u^{e-1})$-constacyclic, cyclic and $(1+u^{e-1})$-constacyclic codes over this ring and characterize the structure of the Gray images of such codes. Finally, we give descriptions concerning the Gray images of some skew-constacyclic codes.

In Chapter II, some useful definitions and properties concerning finite chain rings, skew polynomials and standard terminologies used for error correcting codes are recalled. The definition and some basic properties of a skew-constacyclic code are introduced over $\mathcal{R}_{(p^m,e)}$.

In Chapter III, we determine necessary and sufficient conditions for skew-constacyclic codes over $\mathcal{R}_{(p^m,e)}$ to be free. Based on these conditions, the algebraic structure and some properties of free skew-constacyclic codes over this ring are established. In many cases, the structure of the Euclidean and Hermitian dual codes of free skew-constacyclic codes are given. Necessary and sufficient conditions for such codes to be Euclidean and Hermitian self-dual are determined as well.

In Chapter IV, we restrict our study to the case over $\mathcal{R}_{(p^m,2)} := \mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. We characterize the structure of all skew-constacyclic codes over this ring. Moreover, the structures of Euclidean and Hermitian dual codes of skew-cyclic and skew-negacyclic codes are determined. Based on this characterization, an illustration skew cyclic codes of length 2 over $\mathbb{F}_3+u\mathbb{F}_3$ and their duals is also provided

Finally, in Chapter V, the Gray map is introduced for $\mathcal{R}_{(p^m,e)}$ to link codes over this ring and its residue field. We prove that the Gray image of an $(1-u^{e-1})$-constacyclic code over $\mathcal{R}_{(p^m,e)}$ is a distance-invariant quasi-cyclic code over its residue field. When the length n of codes is not divisible by p, the Gray images of a cyclic code and an $(1+u^{e-1})$-constacyclic code are permutatively equivalent to quasi-cyclic codes over its residue field. Lastly, we give descriptions concerning the Gray images of some skew-constacyclic codes over this ring.

CHAPTER II

PRELIMINARIES

In this chapter, we recall some useful definitions and properties concerning finite chain rings, skew polynomials and classical Error Correcting Codes. First, some algebraic properties of finite chain rings of prime characteristic are cursorily given in Section 2.1. In Section 2.2, some useful results concerning skew polynomials over such rings are derived. Finally, the standard terminologies used for error correcting codes are recalled and the definition and some basic properties of a skew-constacyclic code are established over these rings in Section 2.3.

2.1 Finite Chain Rings

A finite commutative ring with identity $1 \neq 0$ is called a *finite chain ring* if its ideals are linearly ordered by inclusion. It is known that every ideal of a finite chain ring is principal and its maximal ideal is unique (see [28]). Let $\boldsymbol{R}$ denote a finite chain ring and γ a generator of its maximal ideal. The the residue field $\boldsymbol{R}/\langle\gamma\rangle$ is isomorphic to $\mathbb{F}_{p^m}$, for some prime number p and positive integer m. With these notations, the ideals of $\boldsymbol{R}$ form the following chain

$$\boldsymbol{R} \supsetneq \langle\gamma\rangle \supsetneq \langle\gamma^2\rangle \supsetneq \cdots \supsetneq \langle\gamma^{e-1}\rangle \supsetneq \langle\gamma^e\rangle = \langle 0\rangle.$$

The integer e is called the *nilpotency index* of $\boldsymbol{R}$. A finite chain ring $\boldsymbol{R}$ with nilpotency index e and residue field $\mathbb{F}_{p^m}$ has cardinality p^{me} and its characteristic is a power of p ([17, Proposition 2.2]). Further details concerning finite chain rings can be found in [5], [12], [13], [28] and [37].

In this work, we focus on the case where the characteristic of $\boldsymbol{R}$ is prime. In this case, finite chain rings of the certain prime characteristic, nilpotency index and residue field are unique up to isomorphism. We denote by $\mathbb{F}_{p^m}[u]$ the ring of polynomials over $\mathbb{F}_{p^m}$ in an indeterminate u.

Lemma 2.1.1 ([13, Lemma 1])**.** *Given a prime number p, and positive integers m and e, $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$ is the only finite chain ring of characteristic p with nilpotency index e and residue field $\mathbb{F}_{p^m}$.*

For simplicity, the ideal notation will be dropped and the ring $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$ will be isomorphically expressed as

$$\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m} = \left\{ \sum_{i=0}^{e-1} u^i a_i \mid a_i \in \mathbb{F}_{p^m} \right\}, \tag{2.1.1}$$

where the addition and multiplication are the usual addition and multiplication of polynomials in $\mathbb{F}_{p^m}[u]$ together with the rule $u^e = 0$, and simply denoted by $\mathcal{R}_{(p^m,e)}$. We note that the element u is a generator of the maximal ideal $\langle u\rangle = u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$. The ideals of $\mathcal{R}_{(p^m,e)}$ form the chain

$$\begin{aligned}
\mathcal{R}_{(p^m,e)} &\supsetneq \langle u\rangle = u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m} \\
&\supsetneq \langle u^2\rangle = u^2\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m} \\
&\ \ \vdots \\
&\supsetneq \langle u^{e-1}\rangle = u^{e-1}\mathbb{F}_{p^m} \\
&\supsetneq \langle u^e\rangle = \langle 0\rangle.
\end{aligned}$$

Note that when $e = 1$, this ring is the finite field $\mathbb{F}_{p^m}$.

Example 2.1.2. We establish here some examples of rings $\mathcal{R}_{(p^m,e)}$ which play an important role in later chapters.

i) For $p = 2, m = 1$ and $e = 2$, the addition and multiplication tables on the ring $\mathcal{R}_{(2,2)} := \mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u\}$ are as follows:

$+$	0	1	u	$1+u$
0	0	1	u	$1+u$
1	1	0	$1+u$	u
u	u	$1+u$	0	1
$1+u$	$1+u$	u	1	0

$\cdot$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

Table 2.1: The ring $\mathcal{R}_{(2,2)}$

ii) For $p=3, m=1$ and $e=2$,

$$\mathcal{R}_{(3,2)} := \mathbb{F}_3 + u\mathbb{F}_3 = \{0, 1, 2, u, u2, 1+u, 1+u2, 2+u, 2+u2\}.$$

In [2], the structure of the automorphism group $\mathrm{Aut}(\mathcal{R}_{(p^m,e)})$ of $\mathcal{R}_{(p^m,e)}$ has been characterized. For $\theta \in \mathrm{Aut}(\mathbb{F}_{p^m})$, $\beta \in \mathbb{F}_{p^m}$ and $w \in \mathcal{R}_{(p^m,e)}$, let

$$\Theta_{\theta,\beta,w} : \mathcal{R}_{(p^m,e)} \to \mathcal{R}_{(p^m,e)}$$

be the automorphism defined by

$$\Theta_{\theta,\beta,w}(\sum_{i=0}^{e-1} a_i u^i) = \sum_{i=0}^{e-1} u^i \beta^i w^i \theta(a_i).$$

Proposition 2.1.3 ([2, Proposition 1]). $\mathrm{Aut}(\mathcal{R}_{(p^m,e)}) = \{\Theta_{\theta,\beta,w} \mid \theta \in \mathrm{Aut}(\mathbb{F}_{p^m}), \beta \in \mathbb{F}_{p^m}^* \text{ and } w \in 1 + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}\}$, *where* $\mathbb{F}_{p^m}^*$ *denotes the group of units in* $\mathbb{F}_{p^m}$.

It is easy to see that the automorphisms $\Theta_{\theta_1,\beta_1,w_1}$ and $\Theta_{\theta_2,\beta_2,w_2}$ of $\mathcal{R}_{(p^m,e)}$ are equal if and only if $\theta_1 = \theta_2$, $\beta_1 = \beta_2$ and $w_1 \equiv w_2 \bmod u^{e-1}$. Then

$$\begin{aligned} |\mathrm{Aut}(\mathcal{R}_{(p^m,e)})| &= |\mathrm{Aut}(\mathbb{F}_{p^m})||\mathbb{F}_{p^m}^*||1 + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}|/|\mathbb{F}_{p^m}| \\ &= m(p^m-1)p^{(e-2)m}, \end{aligned}$$

and hence the next corollary follows.

Corollary 2.1.4. $\mathrm{Aut}(\mathcal{R}_{(p^m,e)})$ *is non-trivial if an only if* $m \geq 2$ *or* p *is odd or* $e \geq 3$.

When $e = 2$, automorphisms $\Theta_{\theta,\beta,w}$ and $\Theta_{\theta,\beta,1}$ are equal, for all $\theta \in \mathrm{Aut}(\mathbb{F}_{p^m})$, $\beta \in \mathbb{F}_{p^m}^*$ and $w \in 1 + u\mathbb{F}_{p^m}$. For simplicity, we will drop w. Then $\mathrm{Aut}(\mathcal{R}_{(p^m,2)}) = \{\Theta_{\theta,\beta} \mid \theta \in \mathrm{Aut}(\mathbb{F}_{p^m}) \text{ and } \beta \in \mathbb{F}_{p^m}^*\}$.

Example 2.1.5. i) The automorphism group of $\mathcal{R}_{(2,2)}$ is trivial.

ii) The ring $\mathcal{R}_{(3,2)}$ is the smallest finite chain ring (which is not a field) having non-trivial automorphism group $\mathrm{Aut}(\mathcal{R}_{(3,2)}) = \{\Theta_{\mathrm{id},1}, \Theta_{\mathrm{id},2}\}$, where

$$\Theta_{\mathrm{id},1}(a + ub) = a + ub \text{ and } \Theta_{\mathrm{id},2}(a + ub) = a + u2b,$$

for all $a + ub \in \mathcal{R}_{(3,2)}$.

If Θ is an automorphism of $\mathcal{R}_{(p^m,e)}$ extended from an automorphism θ of $\mathbb{F}_{p^m}$, then we have

$$\theta(\bar{r}) = \overline{\Theta(r)} \text{ for all } r \in \mathcal{R}_{(p^m,e)},$$

where $\bar{}: \mathcal{R}_{(p^m,e)} \to \mathbb{F}_{p^m}$ is the canonical reduction modulo u.

2.2 Skew Polynomial Rings over $\mathcal{R}_{(p^m,e)}$

In [7], [8], [10] and [28], results concerning skew polynomial rings over finite fields and over Galois rings have been studied. Applying the ideas in these references, the following results over $\mathcal{R}_{(p^m,e)}$ are given as follows.

Given an automorphism Θ of $\mathcal{R}_{(p^m,e)}$, the set $\mathcal{R}_{(p^m,e)}[x;\Theta] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in \mathcal{R}_{(p^m,e)} \text{ and } n \in \mathbb{N}_0\}$ of formal polynomials is a ring under the usual addition of polynomials and the multiplication is given by the rule $xa = \Theta(a)x$. The multiplication is extended to all elements in $\mathcal{R}_{(p^m,e)}[x;\Theta]$ by associativity and

distributivity. The ring $\mathcal{R}_{(p^m,e)}[x;\Theta]$ is called a *skew polynomial ring* over $\mathcal{R}_{(p^m,e)}$ and an element in $\mathcal{R}_{(p^m,e)}[x;\Theta]$ is called a *skew polynomial*. It is easily seen that the ring $\mathcal{R}_{(p^m,e)}[x;\Theta]$ is non-commutative unless Θ is the identity automorphism on $\mathcal{R}_{(p^m,e)}$.

In addition, assume that Θ is extended from an automorphism θ of $\mathbb{F}_{p^m}$. Based on the canonical reduction modulo u, $^-\colon \mathcal{R}_{(p^m,e)} \to \mathbb{F}_{p^m}$, a natural ring epimorphism extension $^-\colon \mathcal{R}_{(p^m,e)}[x;\Theta] \to \mathbb{F}_{p^m}[x;\theta]$ is defined by

$$r_0 + r_1 x + \cdots + r_n x^n \mapsto \bar{r_0} + \bar{r_1} x + \cdots + \bar{r_n} x^n.$$

In other words, for each $f(x) \in \mathcal{R}_{(p^m,e)}[x;\Theta]$, $\overline{f(x)}$ denotes the componentwise reduction modulo u of $f(x)$. Since every skew polynomial in $\mathcal{R}_{(p^m,e)}[x;\Theta]$ can be uniquely viewed as $\sum_{i=0}^{e-1} u^i f_i(x)$, where $f_i(x) \in \mathbb{F}_{p^m}[x;\theta]$ for all $0 \le i < e$, we have $\overline{\sum_{i=0}^{e-1} f_i(x)} = f_0(x) \in \mathbb{F}_{p^m}[x;\theta]$.

The ring $\mathcal{R}_{(p^m,e)}[x;\Theta]$ may not be a unique factorization ring. Moreover, for a reducible skew polynomial in $\mathcal{R}_{(p^m,e)}[x;\Theta]$, the degrees of its irreducible factors are not unique up to permutation as the next example shown.

Example 2.2.1. Refer to the automorphism $\Theta_{\mathrm{id},2}$ of $\mathcal{R}_{(3,2)}$ in Example 2.1.5. The following are two irreducible factorizations of $x^6 - 1$ in $\mathcal{R}_{(3,2)}[x;\Theta_{\mathrm{id},2}]$

$$x^6 - 1 = (x+1)^3(x+2)^3 = (x^2 + ux + 2)^3.$$

The skew polynomial ring $\mathcal{R}_{(p^m,e)}[x;\Theta]$ is neither left nor right Euclidean. However, left and right divisions can be defined in the case where the leading coefficient of the divisor is a unit in $\mathcal{R}_{(p^m,e)}$. Let $f(x) = a_0 + a_1 x + \cdots + a_r x^r$ and $g(x) = b_0 + b_1 x + \cdots + b_s x^s$ be skew polynomials such that b_s is a unit in $\mathcal{R}_{(p^m,e)}$. The *right division* of $f(x)$ by $g(x)$ is defined by reducing literately degree of $f(x)$ as follows:

If $r < s$, then

$$f(x) = 0g(x) + f(x).$$

Suppose that $r \geq s$. First, note that the degree of

$$f(x) - a_r\Theta^{r-s}(b_s^{-1})x^{r-s}g(x)$$

is less than the degree of $f(x)$. Then iterating the above procedure by subtracting further left multiples of $g(x)$ from the result until the degree is less than the degree of $g(x)$, we obtain skew polynomials $q(x)$ and $r(x)$ such that

$$f(x) = q(x)g(x) + r(x) \text{ with } \deg(r(x)) < \deg(g(x)) \text{ or } r(x) = 0.$$

Obviously, $q(x)$ and $r(x)$ are unique and they are called the *right quotient* and *right remainder*, respectively. The above algorithm is called the *right division algorithm* in $\mathcal{R}_{(p^m,e)}[x;\Theta]$.

If $r(x) = 0$, we say that $g(x)$ is a *right divisor* of $f(x)$. In this case, denote by $\dfrac{f(x)}{g(x)}$ the right quotient $q(x)$ of $f(x)$ by $g(x)$. This implies

$$f(x) = \frac{f(x)}{g(x)}g(x). \tag{2.2.1}$$

Similarly, the *left division algorithm* in $\mathcal{R}_{(p^m,e)}[x;\Theta]$ can be defined using the fact that the degree of

$$f(x) - g(x)\Theta^{-s}(a_r b_s^{-1})x^{r-s}$$

is less than the degree of $f(x)$.

For a skew polynomial $f(x)$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]$, let $\langle f(x)\rangle$ denote the left ideal of $\mathcal{R}_{(p^m,e)}[x;\Theta]$ generated by $f(x)$. Note that $\langle f(x)\rangle$ does not need to be two-sided. A sufficient condition for $\langle f(x)\rangle$ to be two-sided is given as follows:

Proposition 2.2.2. *If $f(x) = x^t g(x)$ where $g(x)$ is central and $t \in \mathbb{N}_0$, then $\langle f(x)\rangle$ is a principal two-sided ideal in $\mathcal{R}_{(p^m,e)}[x;\Theta]$.*

Proof. Since $g(x)$ is central, for a skew polynomial $\sum_{i=0}^{n} a_i x^i$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]$, we have $\left(\sum_{i=0}^{n} a_i x^i\right)(x^t g(x)) = x^t \sum_{i=0}^{n} \Theta^{-t}(a_i) x^i g(x) = (x^t g(x)) \sum_{i=0}^{n} \Theta^{-t}(a_i) x^i$. Hence, the result follows. □

Corollary 2.2.3. *If $f(x)$ is a monic central skew polynomial of degree n, then the skew polynomials of degree less than n are canonical representatives of the elements in $\mathcal{R}_{(p^m,e)}[x,\Theta]/\langle f(x)\rangle$.*

Proof. By Proposition 2.2.2, $\langle f(x)\rangle$ is a two-sided ideal and hence the quotient $\mathcal{R}_{(p^m,e)}[x,\Theta]/\langle f(x)\rangle$ is meaningful. Therefore, the desired result follows from the right division algorithm. □

Proposition 2.2.4. *Let n be a positive integer and λ a unit in $\mathcal{R}_{(p^m,e)}$. Then the following statements are equivalent.*

a) $x^n - \lambda$ *is central in* $\mathcal{R}_{(p^m,e)}[x,\Theta]$.

b) $\langle x^n - \lambda\rangle$ *is two-sided.*

c) n *is a multiple of the order of* Θ *and* λ *is fixed by* Θ.

Proof. *a)* $\Rightarrow$ *b)* follows directly from Proposition 2.2.2.

Next, we prove *b)* $\Rightarrow$ *c)*. Assume that $\langle x^n - \lambda\rangle$ is two-sided. Let $r \in \mathcal{R}_{(p^m,e)}$. Then $rx^n - r\lambda = r(x^n - \lambda) = (x^n - \lambda)s = \Theta^n(s)x^n - s\lambda$ for some $s \in \mathcal{R}_{(p^m,e)}$. Comparing the coefficients, we have $r\lambda = s\lambda$. As λ is a unit, it follows that $r = s$, and hence $rx^n - r\lambda = \Theta^n(r)x^n - r\lambda$. Thus, n is a multiple of the order of Θ. Next, we observe that $x^{n+1} - \Theta(\lambda)x = x(x^n - \lambda) = (x^n - \lambda)(ax + b) = \Theta^n(a)x^{n+1} + \Theta^n(b)x^n - a\lambda x - b\lambda$, for some a and b in $\mathcal{R}_{(p^m,e)}$. Then $\Theta^n(a) = 1$ and $\Theta^n(b) = 0$. As Θ is an automorphism, it follows that $a = 1$ and $b = 0$, and hence $x^{n+1} - \Theta(\lambda)x = x^{n+1} - \lambda x$. Therefore, λ is fixed by Θ.

Finally, we prove $c) \Rightarrow a)$. Assume that n is a multiple of the order of Θ and λ is fixed by Θ. Then $x(x^n - \lambda) = x^{n+1} - \Theta(\lambda)x = x^{n+1} - \lambda x = (x^n - \lambda)x$ and $(x^n - \lambda)t = \Theta^n(t)x^n - t\lambda = tx^n - t\lambda = t(x^n - \lambda)$, for all $t \in \mathcal{R}_{(p^m,e)}$. Consequently, $x^n - \lambda$ commutes with any skew polynomial in $\mathcal{R}_{(p^m,e)}[x;\Theta]$. □

Proposition 2.2.5. *Let $h(x), g(x) \in \mathcal{R}_{(p^m,e)}[x;\Theta]$. If $h(x)g(x)$ is a monic central skew polynomial, then $h(x)g(x) = g(x)h(x)$. In particular, if $g(x)$ is a right divisor of a central skew polynomial $f(x)$, then $g(x)$ and the right quotient $\frac{f(x)}{g(x)}$ commute, i.e.,*

$$g(x)\frac{f(x)}{g(x)} = f(x) = \frac{f(x)}{g(x)}g(x). \tag{2.2.2}$$

Proof. Assume that $h(x)g(x)$ is monic and central. Then the leading coefficient of $g(x)$ and $h(x)$ are units. Since $h(x)g(x)$ is central, we have

$$h(x)(h(x)g(x)) = (h(x)g(x))h(x) = h(x)(g(x)h(x)).$$

Thus, $h(x)(h(x)g(x) - g(x)h(x)) = 0$. As the leading coefficient of $h(x)$ is a unit, $h(x)$ is not a zero divisor. Hence, $h(x)g(x) = g(x)h(x)$ as desired. □

The later study of dualities of codes requires the map defined in Proposition 2.2.7 which links between $\mathcal{R}_{(p^m,e)}[x;\Theta]$ and its right localization. First, we ensure that the right localization of $\mathcal{R}_{(p^m,e)}[x;\Theta]$ exists. In the light of Theorem 2 of [33], necessary and sufficient conditions for $\mathcal{R}_{(p^m,e)}[x;\Theta]$ to have the right localization are given as follows.

Theorem 2.2.6 ([33])**.** *Let $S = \{x^i \mid i \in \mathbb{N}\}$. Then $\mathcal{R}_{(p^m,e)}[x;\Theta]$ has the right localization at S if and only if both of the following conditions hold.*

i) For all $x^i \in S$ and $a(x) \in \mathcal{R}_{(p^m,e)}[x;\Theta]$, there exist $x^j \in S$ and $b(x) \in \mathcal{R}_{(p^m,e)}[x;\Theta]$ such that $a(x)x^i = x^j b(x)$.

ii) *Given* $a(x) \in \mathcal{R}[x;\Theta]$ *and* $x^i \in S$, *if* $x^i a(x) = 0$, *then there exists* $x^j \in S$ *such that* $a(x)x^j = 0$.

Condition $i)$ holds because the multiplication rule allows the shifting of powers of x from left to right by changing the coefficients. Since x^i is never a left zero divisor, $a(x)$ in $ii)$ must be zero and hence $ii)$ follows. Then, by Theorem 2.2.6, the right localization $\mathcal{R}_{(p^m,e)}[x;\Theta]S^{-1}$ of $\mathcal{R}_{(p^m,e)}[x;\Theta]$ at S exists. Hence, $ax^{-1} = x^{-1}\Theta(a)$ where x^{-1} is the inverse of x in this right localization.

The following map is key to determining the structure of dual codes.

Proposition 2.2.7. *Let* $\varphi : \mathcal{R}_{(p^m,e)}[x;\Theta] \to \mathcal{R}_{(p^m,e)}[x;\Theta]S^{-1}$ *be defined by*

$$\varphi(\sum_{i=0}^{t} a_i x^i) = \sum_{i=0}^{t} x^{-i} a_i.$$

Then φ *is a ring anti-monomorphism.*

Proof. Clearly, φ is an injection. Let $p(x) = \sum_{i=0}^{r} a_i x^i$ and $q(x) = \sum_{i=0}^{s} b_i x^i$ be skew polynomials in $\mathcal{R}_{(p^m,e)}[x;\Theta]$. Then $\varphi(p(x) + q(x)) = \varphi(p(x)) + \varphi(q(x))$ and

$$\begin{aligned}
\varphi(p(x)q(x)) &= \varphi\left(\sum_{t=0}^{r+s}(\sum_{i+j=t} a_i\Theta^i(b_j))x^t\right) \\
&= \sum_{t=0}^{r+s} x^{-t}(\sum_{i+j=t} a_i\Theta^i(b_j)) \\
&= \sum_{t=0}^{r+s}\sum_{i+j=t} x^{-j}x^{-i}a_i\Theta^i(b_j) \\
&= \sum_{t=0}^{r+s}\sum_{i+j=t} x^{-j}b_j x^{-i}a_i \\
&= \sum_{j=0}^{s} x^{-j}b_j \sum_{i=0}^{r} x^{-i}a_i = \varphi(q(x))\varphi(p(x)).
\end{aligned}$$

Hence, φ is a ring anti-monomorphism. □

2.3 Classical Error Correcting Codes and Codes over $\mathcal{R}_{(p^m,e)}$

Given a finite set $\mathcal{A}$, a *code of length* n over $\mathcal{A}$ is a nonempty subset C of $\mathcal{A}^n$. The *Hamming distance* $d_{Ham}(\boldsymbol{u},\boldsymbol{v})$ between $\boldsymbol{u}$ and $\boldsymbol{v}$ in $\mathcal{A}^n$ is defined to be the number of entries which $\boldsymbol{u}$ and $\boldsymbol{v}$ differ. The *minimum Hamming distance* of a code C, denoted by $d_{Ham}(C)$, is defined by

$$d_{Ham}(C) = \min\{d_{Ham}(\boldsymbol{u},\boldsymbol{v}) \mid \boldsymbol{u},\boldsymbol{v} \in C, \boldsymbol{u} \neq \boldsymbol{v}\}.$$

A code C is said to be $t-$*error-correcting* if it is able to correct t or fewer errors. The minimum Hamming distance of a code plays very important role for its error-correcting capability.

Theorem 2.3.1. *A code C is t-error-correcting if and only if $d_{Ham}(C) \geq 2t+1$.*

A rich algebraic structure of codes leads to efficiency encoding and decoding procedures. In order to study codes with more algebraic structure, $\mathcal{A}$ is assumed to be a finite field or a finite ring. A code C over the finite field (resp., a finite ring) $\mathcal{A}$ is said to be *linear* if it is a subspace (resp., submodule) of the $\mathcal{A}$-vector space (resp., module) $\mathcal{A}^n$. A linear code is said to be *free* if it is a free $\mathcal{A}$-module. We note that every linear code over finite field is free. When codes are studied over finite fields or finite rings, the *Hamming weight* of a codeword $\boldsymbol{v}$, denoted $w_{Ham}(\boldsymbol{v})$, is defined to be the number of nonzero entries of $\boldsymbol{v}$. The *minimum Hamming weight* $w_{Ham}(C)$ of a code C is defined by

$$w_{Ham}(C) = \min\{w_{Ham}(\boldsymbol{u}) \mid \boldsymbol{u} \in C \setminus \{0\}\}.$$

If C is linear, then $d_{Ham}(C) = w_{Ham}(C)$. Further details concerning Error Correcting Codes can be found in [22], [26] and [27].

In this work, we focus on codes over the ring $\mathcal{R}_{(p^m,e)}$. All codes are assumed to be linear unless otherwise stated. Given an automorphism Θ of $\mathcal{R}_{(p^m,e)}$ and

a unit λ in $\mathcal{R}_{(p^m,e)}$, a code C is said to be *skew-constacyclic*, or specifically, Θ-λ-*constacyclic* if C is closed under the Θ-λ-*constacyclic shift*

$$\rho_{\Theta,\lambda} : {\mathcal{R}_{(p^m,e)}}^n \to {\mathcal{R}_{(p^m,e)}}^n$$

defined by

$$\rho_{\Theta,\lambda}((a_0, a_1, \ldots, a_{n-1})) = (\Theta(\lambda a_{n-1}), \Theta(a_0), \ldots, \Theta(a_{n-2})). \tag{2.3.1}$$

In particular, such codes are called *skew-cyclic* and *skew-negacyclic codes* when λ is 1 and -1, respectively. When Θ is the identity automorphism, they become classical constacyclic, cyclic and negacyclic codes.

Analogous to the case of classical constacyclic codes, a characterization of Θ-λ-constacyclic codes will be given in terms of left ideals in the quotient ring $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda\rangle$. However, due to Proposition 2.2.4, $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda\rangle$ is meaningful if and only if $\langle x^n - \lambda\rangle$ is two-sided, or equivalently, n is a multiple of the order of Θ and λ is a unit fixed by Θ.

For this purpose, throughout, we restrict our study to the case where the length n of codes is a multiple of the order of Θ and λ is a unit in $\mathcal{R}^{\Theta}_{(p^m,e)}$, where $\mathcal{R}^{\Theta}_{(p^m,e)}$ denotes the subring of $\mathcal{R}_{(p^m,e)}$ fixed by Θ.

The *skew polynomial representation* of a code C is defined to be $\{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \mid (c_0, c_1, \ldots, c_{n-1}) \in C\}$. For convenience, it will be regarded as C itself. The next theorem is analogous to that for classical constacyclic codes. The proof is omitted.

Theorem 2.3.2. *A code C of length n over $\mathcal{R}_{(p^m,e)}$ is Θ-λ-constacyclic if and only if its skew polynomial representation is a left ideal in $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda\rangle$.*

There are two inner products on ${\mathcal{R}_{(p^m,e)}}^n$ in which we are interested. One is

the *Euclidean inner product* defined by

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \sum_{i=0}^{n-1} u_i v_i,$$

for $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$ in ${\mathcal{R}_{(p^m,e)}}^n$. When the order of Θ is 2, we can also consider the Hermitian inner product which is defined as

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_H = \sum_{i=0}^{n-1} u_i \Theta(v_i).$$

Elements $\boldsymbol{u}$ and $\boldsymbol{v}$ are said to be *Euclidean orthogonal* (resp., *Hermitian orthogonal*) if $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$ (resp., $\langle \boldsymbol{u}, \boldsymbol{v} \rangle_H = 0$). The *Euclidean dual code* of a code C of length n over $\mathcal{R}_{(p^m,e)}$ is defined to be

$$C^{\perp} = \{\boldsymbol{v} \in {\mathcal{R}_{(p^m,e)}}^n \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

Similarly, the *Hermitian dual code* of C is defined as

$$C^{\perp_H} = \{\boldsymbol{v} \in {\mathcal{R}_{(p^m,e)}}^n \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle_H = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

The code C is said to be *Euclidean self-dual* (resp., *Hermitian self-dual*) if $C = C^{\perp}$ (resp., $C = C^{\perp_H}$).

CHAPTER III

FREE SKEW-CONSTACYCLIC CODES OVER $\mathcal{R}_{(p^m,e)}$

In this chapter, we account for the algebraic structure and some properties of free Θ-λ-constacyclic codes of length n over $\mathcal{R}_{(p^m,e)}$, where λ is a unit in $\mathcal{R}_{(p^m,e)}^{\Theta}$ and the length n of codes is a multiple of the order of Θ. We determine necessary and sufficient conditions for Θ-λ-constacyclic codes over $\mathcal{R}_{(p^m,e)}$ to be free. Using these conditions, we extend results on skew-constacyclic codes over Galois rings [8, Sections 4–5 and 7] to the case over $\mathcal{R}_{(p^m,e)}$.

3.1 Structures of Free Skew-Constacyclic Codes

A characterization of free skew-constacyclic codes over $\mathcal{R}_{(p^m,e)}$ is provided in this section. Some properties of free skew-constacyclic codes and necessary and sufficient conditions for them to be constacyclic are also given.

Proposition 3.1.1. *Let C be a non-zero Θ-λ-constacyclic code of length n over $\mathcal{R}_{(p^m,e)}$. Then C is free if and only if C is generated by a monic right divisor of $x^n - \lambda$.*

Proof. First, assume that C is free of rank s, for some positive integer s. Then $C \cong {\mathcal{R}_{(p^m,e)}}^s$ as modules. Hence, $\bar{C} := \{\bar{\boldsymbol{c}} \mid \boldsymbol{c} \in C\} \cong \mathbb{F}_{p^m}^s$ as vector spaces. Moreover, $\bar{C}$ is a skew-constacyclic code of length n over $\mathbb{F}_{p^m}$, i.e., $\bar{C}$ is generated by a monic right divisor $a(x)$ of $x^n - 1$ in $\mathbb{F}_{p^m}[x;\theta]$ provided that Θ is extended from θ [7]. Let $g(x) \in \mathcal{R}_{(p^m,e)}[x;\theta]$ be a monic preimage of $a(x)$. Then $\deg(g(x)) = \deg(a(x)) = n - s$. It is obvious that $\{g(x), xg(x), \ldots, x^{s-1}g(x)\}$ is

linearly independent over $\mathcal{R}_{(p^m,e)}$, hence it is a basis for C. Since $x^s g(x) \in C$ and $g(x), xg(x), \ldots, x^{s-1}g(x)$ form a basis for C, there exist $b_0, b_1, \ldots, b_{s-1} \in \mathcal{R}_{(p^m,e)}$ which not all are zero such that

$$b_0 g(x) + b_1 x g(x) + \cdots + b_{s-1} x^{s-1} g(x) = -x^s g(x).$$

Thus,

$$(b_0 + b_1 x + \cdots + b_{s-1} x^{s-1} + x^s) g(x) = 0 \text{ in } \mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^k - \lambda \rangle.$$

Since $x^n - \lambda$ is central, we have

$$(b_0 + b_1 x + \cdots + b_{s-1} x^{s-1} + x^s) g(x) = (x^n - \lambda) p(x),$$

for some $p(x) \in \mathcal{R}_{(p^m,e)}[x;\Theta]$. By degree consideration, $p(x)$ is a monic skew polynomial of degree 0, i.e., $p(x) = 1$. Consequently, $g(x)$ is a right divisor of $x^n - \lambda$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]$.

Conversely, assume that C is generated by a monic right divisor $g(x)$ of $x^n - \lambda$. Then there exists a monic skew polynomial $h(x)$ such that $x^n - 1 = h(x)g(x)$. Without loss of generality, we assume that $\deg(h(x)) = k$ and $\deg(g(x)) = n - k$. Thus, for all $t \geq k$, $x^t g(x)$ is a linear combination of $g(x), xg(x), \ldots, x^{k-1}g(x)$. Hence, every element in C (as a left ideal in $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda \rangle$) is a linear combination of $g(x), xg(x), \ldots, x^{k-1}g(x)$. Let $a_0, a_1, \ldots, a_{k-1} \in \mathcal{R}_{(p^m,e)}$ be such that

$$a_0 g(x) + a_1 x g(x) + \cdots + a_{k-1} x^{k-1} g(x) = 0 \text{ in } \mathcal{R}_{(p^m,e)}[x;\theta]/\langle x^k - \lambda \rangle.$$

Since $x^n - \lambda$ is central, we have

$$(a_0 + a_1 x + \cdots + a_{m-1} x^{k-1}) g(x) = (x^n - \lambda) p(x),$$

for some $p(x) \in \mathcal{R}_{(p^m,e)}[x;\Theta]$. By degree condition, $p(x)$ is the zero skew polynomial, and hence $a_0 = a_1 = \cdots = a_{k-1} = 0$. Therefore, C is free of rank $k = n - \deg(g(x))$ with a basis $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$. $\square$

Given a right divisor $g(x) = \sum_{i=0}^{n-k-1} g_i x^i + x^{n-k}$ of $x^n - \lambda$, a generator matrix of the free Θ-λ-constacyclic code C generated by $g(x)$ is given by

$$G = \begin{bmatrix} g_0 & \dots & g_{n-k-1} & 1 & 0 & \dots & 0 \\ 0 & \Theta(g_0) & \dots & \Theta(g_{n-k-1}) & 1 & \dots & 0 \\ 0 & \dots & \dots & \dots & \Theta^2(g_{n-k-1}) & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \Theta^{k-1}(g_0) & \dots & \Theta^{k-1}(g_{n-k-1}) & 1 \end{bmatrix}.$$

A parity-check matrix for C is determined in the next proposition.

Proposition 3.1.2. *Let C be the free Θ-λ-constacyclic code generated by a monic right divisor $g(x)$ of $x^n - \lambda$ and $h(x) := \dfrac{x^n - \lambda}{g(x)}$. Then the following statements hold.*

i) For $c(x) \in \mathcal{R}[x;\Theta]$, we have $c(x) \in C$ if and only if $c(x)h(x) = 0$ in $\mathcal{R}[x;\Theta]/\langle x^n - \lambda \rangle$.

ii) If $h(x) = \sum_{i=0}^{k-1} h_i x^i + x^k$, then the following matrix

$$H = \begin{bmatrix} 1 & \Theta(h_{k-1}) & \dots & \Theta^k(h_0) & 0 & \dots & 0 \\ 0 & 1 & \Theta^2(h_{k-1}) & \dots & \Theta^{k+1}(h_0) & \dots & 0 \\ 0 & 0 & \dots & \dots & \dots & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \Theta^{n-k}(h_{k-1}) & \dots & \Theta^{n-1}(h_0) \end{bmatrix}$$

is a parity-check matrix for C.

Proof. Since n is a multiple of the order of Θ and $\lambda \in \mathcal{R}^\Theta$, $x^n - \lambda$ is central and it follows from Proposition 2.2.5 that $x^n - \lambda = h(x)g(x) = g(x)h(x)$.

First, we prove $i)$. Assume that $c(x) = p(x)g(x)$ for some $p(x)$ in $\mathcal{R}[x;\Theta]$. Then $c(x)h(x) = (p(x)g(x))h(x) = p(x)(x^n - \lambda) = 0$ in $\mathcal{R}[x;\Theta]/\langle x^n - \lambda \rangle$.

Conversely, assume that $c(x)h(x) = 0$ in $\mathcal{R}[x;\Theta]/\langle x^n - \lambda\rangle$. Then there exists $p(x) \in \mathcal{R}[x;\Theta]$ such that $c(x)h(x) = p(x)(x^n - \lambda) = p(x)g(x)h(x)$. As the leading coefficient of $h(x)$ is a unit, we then have $c(x) = p(x)g(x) \in C$.

To prove $ii)$, let $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in C$ and $[\, s_k \; s_{k+1} \; \cdots \; s_{n-1} \,] = [\, c_0 \; c_1 \; \cdots \; c_{n-1} \,]H^T$. Then, for $l \in \{k, k+1, \ldots, n-1\}$,

$$s_l = c_{l-k} + \sum_{j=0}^{k-1} c_{l-j}\Theta^{l-j}(h_j)$$

which equals the coefficient of x^l in $c(x)h(x)$.

Since $c(x) \in C$, it follows from $i)$ that $c(x)h(x) = 0$ in $\mathcal{R}[x;\Theta]/\langle x^n - \lambda\rangle$. Then there exists $q(x) \in \mathcal{R}[x;\Theta]$ such that $q(x)(x^n - \lambda) = c(x)h(x)$ having degree less than $n+k$. Therefore, the coefficients of the monomials $x^k, x^{k+1}, \ldots, x^{n-1}$ in this product must be zero, i.e., $[\, s_k \; s_{k+1} \; \cdots \; s_{n-1} \,]$ is the zero matrix.

Since the rank of H is $n-k$, the result follows. □

When Θ is the identity automorphism, a Θ-λ-constacyclic code becomes λ-constacyclic. However, the converse does not need to be true. Here, necessary and sufficient conditions for a free Θ-λ-constacyclic code generated by a right divisor of $x^n - \lambda$ to be λ-constacyclic are given.

Proposition 3.1.3. *Let $g(x)$ be a monic right divisor of $x^n - \lambda$ in $\mathcal{R}[x;\Theta]$. The free Θ-λ-constacyclic code generated by $g(x)$ is λ-constacyclic if and only if $g(x) \in \mathcal{R}^{\Theta}[x;\Theta]$.*

Proof. Suppose $g(x) = \sum_{i=0}^{n-k-1} g_i x^i + x^{n-k}$ and C is the free Θ-λ-constacyclic code generated by $g(x)$.

Assume that C is λ-constacyclic. Then $xg(x), g(x)x \in C$. Since C is linear, $xg(x) - g(x)x \in C$ and hence

$$(\Theta(g_0) - g_0)x + (\Theta(g_1) - g_1)x^2 + \cdots + (\Theta(g_{n-k-1}) - g_{n-k-1})x^{n-k} = p(x)g(x),$$

for some $p(x) \in \mathcal{R}[x;\Theta]$ such that $\deg(p(x)) < k$. Thus, $\deg(p(x)g(x)) < n$ which implies that $p(x)$ is constant such that $p(x)g_0 = 0$. Since $g(x)$ is a right divisor of $x^n - \lambda$ and λ is a unit, g_0 is not a zero divisor. Thus, $p(x)$ is zero and hence g_i is fixed by Θ for all i.

Conversely, assume that $g(x) \in \mathcal{R}^{\Theta}[x;\Theta]$. Then $g_i x = x g_i$ for all $i = 0, 1, \ldots, n-k$. Thus, $g(x)x = xg(x) \in C$ and the desired result follows. □

3.2 Euclidean Dual Codes of Free Skew-Constacyclic Codes

We now study Euclidean dual codes of free Θ-λ-constacyclic codes over $\mathcal{R}_{(p^m,e)}$. In particular, when $\lambda^2 = 1$, a generator of the Euclidean dual code of a free Θ-λ-constacyclic code is determined. Furthermore, necessary and sufficient conditions for such a code to be Euclidean self-dual are given.

Lemma 3.2.1. *Let C be a code of length n over $\mathcal{R}_{(p^m,e)}$. Then C is Θ-λ-constacyclic if and only if $C^{\perp}$ is Θ-λ^{-1}-constacyclic. In particular, if $\lambda^2 = 1$, then C is Θ-λ-constacyclic if and only if $C^{\perp}$ is Θ-λ-constacyclic.*

Proof. We note that, for each unit α in $\mathcal{R}_{(p^m,e)}$, $\alpha \in \mathcal{R}^{\Theta}$ if and only if $\alpha^{-1} \in \mathcal{R}^{\Theta}_{(p^m,e)}$. Since $\lambda \in \mathcal{R}^{\Theta}_{(p^m,e)}$, we have $\lambda^{-1} \in \mathcal{R}^{\Theta}_{(p^m,e)}$. Let $u = (u_0, u_1, \ldots, u_{n-1}) \in C$ and $v = (v_0, v_1, \ldots, v_{n-1}) \in C^{\perp}$. Since

$$(\Theta^{n-1}(\lambda u_1), \Theta^{n-1}(\lambda u_2), \ldots, \Theta^{n-1}(\lambda u_{n-1}), \Theta^{n-1}(u_0)) = \rho^{n-1}_{\Theta,\lambda}(u) \in C,$$

we have

$$\begin{aligned}
0 &= \langle \rho^{n-1}_{\Theta,\lambda}(u), v \rangle \\
&= \langle (\Theta^{n-1}(\lambda u_1), \Theta^{n-1}(\lambda u_2), \ldots, \Theta^{n-1}(\lambda u_{n-1}), \Theta^{n-1}(u_0)), (v_0, v_1, \ldots, v_{n-1}) \rangle \\
&= \lambda \langle (\Theta^{n-1}(u_1), \Theta^{n-1}(u_2), \ldots, \Theta^{n-1}(u_{n-1}), \Theta^{n-1}(\lambda^{-1} u_0)), (v_0, v_1, \ldots, v_{n-1}) \rangle \\
&= \lambda (\Theta^{n-1}(\lambda^{-1} u_0) v_{n-1} + \sum_{i=1}^{n-1} \Theta^{n-1}(u_i) v_{i-1}).
\end{aligned}$$

It follows from n is a multiple of the order of Θ and λ^{-1} is fixed by Θ that

$$\begin{aligned} 0 = \Theta(0) &= \Theta(\lambda(\Theta^{n-1}(\lambda^{-1}u_0)v_{n-1} + \sum_{i=1}^{n-1}\Theta^{n-1}(u_i)v_{i-1})) \\ &= \lambda(u_0\Theta(\lambda^{-1}v_{n-1}) + \sum_{i=1}^{n-1}u_i\Theta(v_{i-1})) \\ &= \lambda\langle\rho_{\Theta,\lambda^{-1}}(v), u\rangle. \end{aligned}$$

Therefore, $\rho_{\Theta,\lambda^{-1}}(v) \in C^{\perp}$.

The converse follows from the fact that $(C^{\perp})^{\perp} = C$.

In addition, assume that $\lambda^2 = 1$. Then $\lambda = \lambda^{-1}$ and hence the last statement follows immediately from the main result. □

If $\lambda^2 = 1$, we obtain from the previous lemma that the Euclidean dual $C^{\perp}$ of a Θ-λ-constacyclic code C is again Θ-λ-constacyclic. In this case, a generator of $C^{\perp}$ is given through the ring anti-monomorphism φ defined in Proposition 2.2.7, where $\varphi(\sum_{i=0}^{t} a_i x^i) = \sum_{i=0}^{t} x^{-i}a_i$. The next lemma is key to obtaining the main result.

Lemma 3.2.2. *Assume that $\lambda^2 = 1$. Let $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ and $b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ be in $\mathcal{R}_{(p^m,e)}[x;\Theta]$. Then the following statements are equivalent.*

a) The coefficient vector of $a(x)$ is Euclidean orthogonal to the coefficient vector of $x^i(x^{n-1}\varphi(b(x)))$ for all $i \in \{0, 1, \ldots, n-1\}$.

b) $(a_0, a_1, \ldots, a_{n-1})$ is Euclidean orthogonal to $(b_{n-1}, \Theta(b_{n-2}), \ldots, \Theta^{n-1}(b_0))$ and all its Θ-λ-constacyclic shifts.

c) $a(x)b(x) = 0$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda\rangle$.

Proof. The definition of φ gives that $a)$ is equivalent to $b)$. We prove $b)$ is equivalent to $c)$. Let $a(x)b(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda\rangle$.

Since $\lambda \in \mathcal{R}^{\Theta}_{(p^m,e)}$ such that $\lambda^2 = 1$ and n is a multiple of the order of Θ, it follows that, for each $k \in \{0, 1, \ldots, n-1\}$,

$$\begin{aligned}
c_k &= \sum_{\substack{i+j=k \\ 0\le i\le n-1 \\ 0\le j\le n-1}} a_i\Theta^i(b_j) + \sum_{\substack{i+j=k+n \\ 0\le i\le n-1 \\ 0\le j\le n-1}} \lambda a_i\Theta^i(b_j) \\
&= \lambda\left(\sum_{\substack{i+j=k \\ 0\le i\le n-1 \\ 0\le j\le n-1}} a_i\Theta^{k-j}(\lambda b_j) + \sum_{\substack{i+j=k+n \\ 0\le i\le n-1 \\ 0\le j\le n-1}} a_i\Theta^{n+k-j}(b_j)\right) \\
&= \lambda\langle(a_0, a_1, \ldots, a_{n-1}), (\lambda b_k, \Theta(\lambda b_{m-1}), \ldots, \Theta^k(\lambda b_0), \Theta^{k+1}(b_{n-1}), \ldots, \Theta^{n-1}(b_{k+1}))\rangle \\
&= \lambda\langle(a_0, a_1, \ldots, a_{n-1}), (\Theta^{(n-k)+k}(\lambda b_k), \\
&\qquad \Theta^{(n-k+1)+k}(\lambda b_{m-1}), \ldots, \Theta^k(\lambda b_0), \Theta^{1+k}(b_{n-1}), \ldots, \Theta^{(n-k-1)+k}(b_{k+1}))\rangle.
\end{aligned}$$

Hence, $a(x)b(x) = 0$ if and only if $c_k = 0$ for all $k \in \{0, 1, \ldots, n-1\}$, which is true if and only if $(a_0, a_1, \ldots, a_{n-1})$ is Euclidean orthogonal to

$$(b_{n-1}, \Theta(b_{n-2}), \ldots, \Theta^{n-1}(b_0))$$

and all its Θ-λ-constacyclic shifts. □

Theorem 3.2.3. *Assume that $\lambda^2 = 1$. Let $g(x)$ be a right divisor of $x^n - \lambda$ and $h(x) := \dfrac{x^n - \lambda}{g(x)}$. Let C be the free Θ-λ-constacyclic code generated by $g(x)$. Then the following statements hold.*

i) The skew polynomial $x^{\deg(h(x))}\varphi(h(x))$ is a right divisor of $x^n - \lambda$.

ii) The Euclidean dual $C^{\perp}$ is a Θ-λ-constacyclic code generated by

$$x^{\deg(h(x))}\varphi(h(x)).$$

Proof. First, we prove $i)$. Using the assumptions that n is a multiple of the order

of Θ and $\lambda \in \mathcal{R}^{\Theta}_{(p^m,e)}$, we observe that

$$\begin{aligned}(\varphi(g(x))(-\lambda)x^{n-\deg(h(x))})(x^{\deg(h(x))}\varphi(h(x))) &= \varphi(g(x))(-\lambda)x^n\varphi(h(x)) \\ &= -\lambda x^n\varphi(g(x))\varphi(h(x)) \\ &= -\lambda x^n\varphi(h(x)g(x)), \\ &\text{(since } \varphi \text{ is a ring anti-monomorphism)} \\ &= -\lambda x^n\varphi(x^n-\lambda) \\ &= -\lambda x^n(x^{-n}-\lambda) \\ &= x^n-\lambda.\end{aligned}$$

Since $\varphi(g(x))(-\lambda)x^{n-\deg(h(x))}$ and $x^{\deg(h(x))}\varphi(h(x))$ belong to $\mathcal{R}_{(p^m,e)}[x;\Theta]$, we have $x^{\deg(h(x))}\varphi(h(x))$ is a right divisor of $x^n-\lambda$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]$.

Next, we prove *ii)*. Since $g(x)h(x) = x^n-\lambda = 0$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n-\lambda\rangle$, by Lemma 3.2.2, $\langle x^{\deg(h(x))}\varphi(h(x))\rangle \subseteq C^{\perp}$. Moreover, $x^{\deg(h(x))}\varphi(h(x))$ is a right divisor of $x^n-\lambda$, by Proposition 3.1.1, we have

$$|\langle x^{\deg(h(x))}\varphi(h(x))\rangle| = |\mathcal{R}_{(p^m,e)}|^{n-\deg(h(x))} = |C^{\perp}|.$$

Therefore, $\langle x^{\deg(h(x))}\varphi(h(x))\rangle = C^{\perp}$. □

We give necessary and sufficient conditions for a free Θ-λ-constacyclic code to be Euclidean self-dual in the next theorem.

Theorem 3.2.4. *Assume that $\lambda^2 = 1$ and $n = 2k$ is even. Let $g(x) = \sum_{i=0}^{k-1} g_i x^i + x^k$ be a right divisor of $x^n-\lambda$. Then the free Θ-λ-constacyclic code generated by $g(x)$ is Euclidean self-dual if and only if*

$$\left(\sum_{i=0}^{k-1} g_i x^i + x^k\right)\left(\sum_{i=0}^{k-1} \Theta^{i-k}(g_0^{-1}g_{k-i})x^i + x^k\right) = x^n-\lambda. \tag{3.2.1}$$

Proof. Let C be the Θ-λ-constacyclic code generated by $g(x)$ and let $g^{\perp}(x)$ be the generator polynomial of the Euclidean dual code $C^{\perp}$. Denote by $h(x) := \sum_{i=0}^{k-1} h_i x^i + x^k$ the right quotient $\dfrac{x^n - \lambda}{g(x)}$. It follows from Theorem 3.2.3 that

$$g^{\perp}(x) = x^k \varphi(h(x)) = \Theta^k(h_0)x^k + \cdots + \Theta(h_{k-1})x + 1. \tag{3.2.2}$$

Assume that C is Euclidean self-dual. It is easily seen that $g(x)$ is the unique monic generator of minimal degree in C. Then $g^{\perp}(x)$ is a scalar multiple of $g(x)$ of the form

$$g^{\perp}(x) = \Theta^k(h_0)g(x) = \Theta^k(h_0)(\sum_{i=0}^{k-1} g_i x^i + x^k). \tag{3.2.3}$$

Comparing the coefficients in (3.2.2) and (3.2.3), we obtain $\Theta^k(h_0)g_0 = 1$ and $\Theta^k(h_0)g_i = \Theta^i(h_{k-i})$, for all $i = 1, 2, \ldots, k-1$. Consequently, $h_0 = \Theta^{-k}(g_0^{-1})$ and $h_i = \Theta^i(h_0)\Theta^{i-k}(g_{k-i}) = \Theta^{i-k}(g_0^{-1})\Theta^{i-k}(g_{k-i}) = \Theta^{i-k}(g_0^{-1}g_{k-i})$, for all $i = 1, 2, \ldots, k-1$. and $h(x) = \Theta^{-k}(g_0^{-1}) + \sum_{i=1}^{k-1} \Theta^{i-k}(g_0^{-1}g_{k-i})x^i + x^k$. Therefore, (3.2.1) holds.

On the other hands, assume that (3.2.1) holds. Then

$$h(x) = \Theta^{-k}(g_0^{-1}) + \sum_{i=1}^{k-1} \Theta^{i-k}(g_0^{-1}g_{k-i})x^i + x^k.$$

Hence, by Theorem 3.2.3,

$$g^{\perp}(x) = x^k \varphi(h(x)) = \sum_{i=1}^{k} (g_0^{-1}g_i)x^i + 1 = g_0^{-1}g(x).$$

This completes the proof. □

Remark 3.2.5. From Theorem 3.2.4, we observe that if there is a Euclidean self-dual Θ-λ-constacyclic code, then $-\lambda = g_0\Theta^{-k}(g_0^{-1}) = \Theta^k(g_0)g_0^{-1}$. Thus, if the order of Θ divides k and $\lambda \neq -1$, then there are no Euclidean self-dual Θ-λ-constacyclic codes of length $2k$. In particular, if Θ is the identity automorphism and $\lambda \neq -1$, then there are no Euclidean self-dual Θ-λ-constacyclic codes of any length.

3.3 Hermitian Dual Codes of Free Skew-Constacyclic Codes

Due to the constraint in the definition of the Hermitian inner product, the Hermitian dual codes of skew-constacyclic codes are studied only when the order of Θ is 2. Using arguments similar to those in the previous proofs, the following results concerning the Hermitian duality are obtained.

Lemma 3.3.1. *Let C be a code of even length n over $\mathcal{R}_{(p^m,e)}$. Assume that the order of Θ is 2. Then C is Θ-λ-constacyclic if and only if $C^{\perp_H}$ is Θ-λ^{-1}-constacyclic. In particular, if $\lambda^2 = 1$, then C is Θ-λ-constacyclic if and only if $C^{\perp_H}$ is Θ-λ-constacyclic.*

When $\lambda^2 = 1$, a generator of the Hermitian dual code of a Θ-λ-constacyclic code is determined through the ring anti-monomorphism φ defined in Proposition 2.2.7 and a ring automorphism Φ on $\mathcal{R}_{(p^m,e)}[x;\Theta]$ defined by

$$\Phi(\sum_{i=0}^{t} a_i x^i) = \sum_{i=0}^{t} \Theta(a_i) x^i. \tag{3.3.1}$$

Lemma 3.3.2. *Assume that the order of Θ is 2 and $\lambda^2 = 1$. Let $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ and $b(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ be in $\mathcal{R}_{(p^m,e)}[x;\Theta]$. Then the following statements are equivalent.*

a) The coefficient vector of $a(x)$ is Hermitian orthogonal to the coefficient vector of $x^i\Phi(x^{n-1}\varphi(b(x)))$ for all $i \in \{0, 1, \ldots, n-1\}$.

b) $(a_0, a_1, \ldots, a_{n-1})$ is Hermitian orthogonal to $(\Theta^{-1}(b_{n-1}), b_{n-2}, \ldots, \Theta^{n-2}(b_0))$ and all its Θ-λ-constacyclic shifts.

c) $a(x)b(x) = 0$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda\rangle$.

Theorem 3.3.3. *Assume that the order of Θ is 2 and $\lambda^2 = 1$. Let $g(x)$ be a right divisor of $x^n - \lambda$ and $h(x) := \dfrac{x^n - \lambda}{g(x)}$. Let C be the Θ-λ-constacyclic code generated by $g(x)$. Then the following statements hold.*

i) *The skew polynomial* $\Phi(x^{\deg(h(x))}\varphi(h(x)))$ *is a right divisor of* $x^n - \lambda$.

ii) *The Hermitian dual* $C^{\perp_H}$ *is a* Θ*-*λ*-constacyclic code generated by*

$$\Phi(x^{\deg(h(x))}\varphi(h(x))).$$

Proof. From the proof of Theorem 3.2.3, we have

$$\varphi(g(x))(-\lambda x^{n-\deg(h)})x^{\deg(h)}\varphi(h(x)) = x^n - \lambda.$$

Then

$$\Phi(\varphi(g(x))(-\lambda x^{n-\deg(h)}))\Phi(x^{\deg(h(x))}\varphi(h(x))) = \Phi(x^n - \lambda) = x^n - \lambda.$$

Hence, $\Phi(x^{\deg(h(x))}\varphi(h(x)))$ is a right divisor of $x^n - \lambda$, which yields $i)$. Since $g(x)h(x) = x^n - \lambda = 0$ in $\mathcal{R}_{(p^m,e)}[x;\Theta]/\langle x^n - \lambda\rangle$, by Lemma 3.3.2,

$$\langle \Phi(x^{\deg(h(x))}\varphi(h(x)))\rangle \subseteq C^{\perp_H}.$$

Since $\phi(x^{\deg(h(x))}\varphi(h(x)))$ is a right divisor of $x^n - \lambda$, by Proposition 3.1.1,

$$|\langle \phi(x^{\deg(h(x))}\varphi(h(x)))\rangle| = |\mathcal{R}_{(p^m,e)}|^{n-\deg(h(x))} = |C^{\perp_H}|.$$

Therefore, $\langle \phi(x^{\deg(h(x))}\varphi(h(x)))\rangle = C^{\perp_H}$. This proves $ii)$. □

Next, we give necessary and sufficient conditions for a free Θ-λ-constacyclic code to be Hermitian self-dual. Using the definition of the Hermitian inner product and the arguments similar to those in the proof of Theorem 3.2.4, we have the following theorem.

Theorem 3.3.4. *Assume that the order of* Θ *is* 2, $\lambda^2 = 1$ *and* n *is even, denoted by* $n = 2k$. *Let* $g(x) = \sum_{i=0}^{k-1} g_i x^i + x^k$ *be a right divisor of* $x^n - \lambda$. *Then the* Θ*-*λ*-constacyclic code generated by* $g(x)$ *is Hermitian self-dual if and only if*

$$\left(\sum_{i=0}^{k-1} g_i x^i + x^k\right)\left(\sum_{i=0}^{k-1} \Theta^{i-k-1}(g_0^{-1}g_{k-i})x^i + x^k\right) = x^n - \lambda.$$

Remark 3.3.5. Suppose there is a Hermitian self-dual Θ-λ-constacyclic code. Then, by Theorem 3.3.4, we have $-\lambda = g_0\Theta^{-k-1}(g_0^{-1})$. Since λ is fixed by Θ, it follows that $\lambda = -\Theta^{k+1}(g_0)g_0^{-1}$. Recall that the order of Θ is 2, so

$$\lambda = \begin{cases} -1 & \text{if } k \text{ is odd,} \\ -\Theta(g_0)g_0^{-1} & \text{if } k \text{ is even.} \end{cases}$$

Therefore, if k is odd and $\lambda \neq -1$, then there are no Hermitian self-dual Θ-λ-constacyclic codes of length $2k$.

CHAPTER IV

SKEW-CONSTACYCLIC CODES OVER $\mathcal{R}_{(p^m,2)}$

The class of finite chain rings of the form $\mathcal{R}_{(p^m,e)}$ has widely been used as alphabet in certain constacyclic codes (see, for example, [3], [6], [15], [16], [23] and [30]). In order to avoid a tedious computation, we restrict our study to the case $e = 2$ and we use the notation $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ instead of $\mathcal{R}_{(p^m,2)}$. We characterize the structure of all Θ-λ-constacyclic codes over the ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ under the conditions where λ is a unit in $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ fixed by a given automorphism Θ and the length n of codes is a multiple of the order of Θ. Moreover, the structures of Euclidean and Hermitian dual codes of skew -cyclic and skew-negacyclic codes over this ring are determined.

Recall that $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ is a finite chain ring of nilpotency index 2 and characteristic p. Its only maximal ideal is $u\mathbb{F}_{p^m}$ and its residue field is the subfield $\mathbb{F}_{p^m}$ of $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Every automorphism of $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ is of the form $\Theta_{\theta,\beta}(a + bu) = \theta(a) + \beta\theta(b)u$, where $\theta \in \mathrm{Aut}(\mathbb{F}_{p^m})$ and $\beta \in \mathbb{F}_{p^m}^*$. For simplicity, where no confusion arises, the subscripts θ and β will be dropped.

Let $f(x)$ in $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]$. Then the multiplication rule allows the shifting of u and powers of x from the left to the right of $f(x)$ (and vice versa) by changing the coefficients of $f(x)$. Thus, for $\Omega \in \{u, x^i \mid i \in \mathbb{N}\}$, we may write

i) $\overleftarrow{f(x)}^{\Omega}$ for the skew polynomial satisfying $f(x)\Omega = \Omega\overleftarrow{f(x)}^{\Omega}$, and

ii) $\overrightarrow{f(x)}^{\Omega}$ for the skew polynomial satisfying $\Omega f(x) = \overrightarrow{f(x)}^{\Omega}\Omega$.

4.1 Classification of Skew-Constacyclic Codes

In this section, the classification of Θ-λ-constacyclic codes is given in terms of generators of left ideals in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$. These generators are uniquely determined under some conditions. Furthermore, we study their properties.

Let C be a non-zero left ideal in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$ and let A denote the set of all non-zero skew polynomials of minimal degree in C. Clearly, A is non-empty. We consider three cases: when there is a monic skew polynomial in A, when there are no monic skew polynomials in C, and when there are no monic skew polynomials in A but there is a monic skew polynomial in C.

Theorem 4.1.1. *Let C and A be as above. Then:*

i) If there exists a monic skew polynomial in A, then it is unique in A. In this case, $C = \langle g(x)\rangle$, where $g(x)$ is the unique such skew polynomial.

ii) If there are no monic skew polynomials in C, then there exists a unique skew polynomial $g(x) = ug_1(x)$ in A with leading coefficient u. In this case, $C = \langle g(x)\rangle$.

iii) If there are no monic skew polynomials in A but there exists a monic skew polynomial in C, then there exist a unique skew polynomial $g(x) = ug_1(x)$ in A with leading coefficient u and a unique monic skew polynomial $f(x) = f_0(x) + uf_1(x)$ of minimal degree in C such that $\deg(f_1(x)) < \deg(g_1(x))$. In this case, $C = \langle g(x), f(x)\rangle$.

Proof. To prove $i)$, assume that $g(x)$ and $g'(x)$ are monic skew polynomials in A. Then the degree of $g(x) - g'(x)$ is less than the degree of $g(x)$. By the minimality of $\deg(g(x))$, $g(x) - g'(x) = 0$. Hence, $g(x)$ is the unique monic skew polynomial in A.

Let $c(x) \in C$. Then by the right division algorithm, there exist unique skew polynomials $q(x)$ and $r(x)$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$ such that

$$c(x) = q(x)g(x) + r(x),$$

and $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Then

$$r(x) = c(x) - q(x)g(x) \in C.$$

By the minimality of $\deg(g(x))$, $r(x) = 0$. Hence, $c(x) = q(x)g(x)$, i.e., $C = \langle g(x) \rangle$.

To prove $ii)$, assume there are no monic skew polynomials in C. Without loss of generality, let $g(x)$ be a skew polynomial in A with leading coefficient u. First, we show that $g(x)$ is a right multiple of u. Suppose that $g(x)$ has a unit coefficient a_i for some $i < \deg(g(x))$. Then $ug(x) \in C$ is a non-zero skew polynomial having degree less than $\deg(g(x))$, which contradicts the minimality of $\deg(g(x))$. Hence, $g(x)$ is a right multiple of u, and we write $g(x) = ug_1(x)$, where $g_1(x)$ is a monic skew polynomial in $\mathbb{F}_{p^m}[x;\theta]$.

For the uniqueness, suppose that $g'(x)$ is a skew polynomial in A with leading coefficient u. Then the degree of $g(x) - g'(x)$ is less than the degree of $g(x)$. By the minimality of $\deg(g(x))$, $g(x) - g'(x) = 0$. Hence, $g(x) = ug_1(x)$ is the unique skew polynomial in A with leading coefficient u.

Now, we show that C is generated by $g(x) = ug_1(x)$. Suppose that there exists $h(x)$ in C of minimal degree ℓ which is not a left multiple of $g(x) = ug_1(x)$. Moreover, $h(x)$ can be chosen to have leading coefficient u. Then

$$\begin{aligned} k(x) :&= h(x) - ux^{\ell - \deg(g(x))}g_1(x) \\ &= h(x) - \overrightarrow{x^{\ell-\deg(g(x))}}^{u} ug_1(x) \\ &= h(x) - \overrightarrow{x^{\ell-\deg(g(x))}}^{u} g(x) \in C. \end{aligned}$$

If $k(x) = 0$, then $h(x) = \overrightarrow{x^{\ell-\deg(g(x))}}^{u} g(x)$ which contradicts the assumption. Suppose $k(x) \neq 0$. Then the degree of $k(x)$ is less than ℓ and $k(x)$ is not a left multiple of $g(x)$ which contradicts the choice of $h(x)$.

Finally, we prove *iii)*. Assume there are no monic skew polynomials in A but there exists a monic skew polynomial in C. It can be shown as in *ii)* that there is a unique skew polynomial $g(x) = ug_1(x)$ in A with leading coefficient u.

Let $F(x)$ be a monic skew polynomial of minimal degree in C. We view $F(x) = F_0(x) + uF_1(x)$, where $F_0(x), F_1(x) \in \mathbb{F}_{p^m}[x;\theta]$. By the right division algorithm, there exist unique skew polynomials $q(x)$ and $r(x)$ in $\mathbb{F}_{p^m}[x;\theta]$ such that

$$F_1(x) = q(x)g_1(x) + r(x),$$

and $r(x) = 0$ or $\deg(r(x)) < \deg(g_1(x))$. Thus,

$$F(x) = F_0(x) + uF_1(x) = F_0(x) + uq(x)g_1(x) + ur(x).$$

We choose $f(x) = F(x) - uq(x)g_1(x)$, $f_0(x) = F_0(x)$ and $f_1(x) = r(x)$. Then $f(x) = f_0(x) + uf_1(x)$ is a monic skew polynomial of minimal degree in C such that $\deg(f_1(x)) < \deg(g_1(x))$.

The uniqueness of $ug_1(x)$ can be shown as in the proof of *ii)*. Suppose $t_0(x) + ut_1(x)$ is a monic skew polynomial of minimal degree in C such that $\deg(t_1(x)) < \deg(g_1(x))$. Then $\langle uf_0(x)\rangle = uC = \langle ut_0(x)\rangle$. Hence, by the proof of *ii)*, $f_0(x) = t_0(x)$. Note that $u(f_1(x) - t_1(x)) = (f_0(x) + uf_1(x)) - (t_0(x) + ut_1(x)) \in C$. Then $u(f_1(x) - t_1(x))$ is the zero or $\deg(f_1(x) - t_1(x)) \leq \max\{\deg(f_1(x)), \deg(t_1(x))\}$. If the later case occurs, then $\deg(f_1(x) - t_1(x)) < \deg(g_1(x))$, which contradicts the minimality of $\deg(g_1(x))$. Hence, $f_1(x) - t_1(x) = 0$.

Let B be the set of all non-zero skew polynomials in C with degree less than $\deg(f(x))$. Then the leading coefficients of all skew polynomials in B are multiple

of u. Since $ug_1 \in A$, we have $\deg(ug_1(x)) < \deg(f(x))$, and hence $ug_1(x) \in B$. We show that B is contained in the left ideal generated by $ug_1(x)$. Suppose there exists $h(x)$ in B of minimal degree $\ell < s$ which is not a left multiple of $g(x) = ug_1(x)$. Moreover, $h(x)$ can be chosen to have leading coefficient u. Thus,

$$\begin{aligned} k(x) :&= h(x) - ux^{\ell-\deg(g(x))}g_1(x) \\ &= h(x) - \overrightarrow{x^{\ell-\deg(g(x))}}^{u} ug_1(x) \\ &= h(x) - \overrightarrow{x^{\ell-\deg(g(x))}}^{u} g(x) \in C. \end{aligned}$$

If $k(x) = 0$, then $h(x) = \overrightarrow{x^{\ell-\deg(g(x))}}^{u} g(x)$, which contradicts the assumption. Suppose $k(x) \neq 0$. Then the degree of $k(x)$ is less than $\ell < s$. Hence, $k(x) \in B$ and $k(x)$ is not a left multiple of $g(x)$, which contradict the minimality of ℓ. Therefore, B is contained in the left ideal generated by $g(x) = ug_1(x)$.

To show that C is generated by $\{g(x) = ug_1(x), f(x) = g_0(x) + ug_1(x)\}$, let $c(x) \in C$. Then there exist unique skew polynomials $q'(x)$ and $r'(x)$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$ such that

$$c(x) = q'(x)f(x) + r'(x),$$

and $r'(x) = 0$ or $\deg(r'(x)) < \deg(f(x))$. If $r'(x) = 0$, we are done. Assume that $\deg(r'(x)) < \deg(f(x))$. Then $r'(x) \in B$ and so $r'(x) = m(x)g(x)$ for some $m(x) \in (\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$. Hence,

$$c(x) = q'(x)f(x) + r'(x) = q'(x)f(x) + m(x)g(x).$$

Therefore, C is generated by $\{g(x) = ug_1(x), f(x) = f_0(x) + uf_1(x)\}$. □

Following Theorem 4.1.1, we distinguish three types of the left ideals in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$. Type LI-1 refers to the zero ideal or a left ideal satisfying $i)$, type LI-2 refers to a left ideal satisfying $ii)$, and type LI-3 refers to a left ideal satisfying $iii)$.

Further properties of left ideals of each type are given in the following propositions.

Proposition 4.1.2. *A left ideal of type* LI-1 *is principal and generated by a monic right divisor $g(x)$ of $x^n - \lambda$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$. Moreover, if we view $g(x) = g_0(x) + ug_1(x)$, where $g_0(x), g_1(x) \in \mathbb{F}_{p^m}[x;\theta]$, then $\deg(g_1(x)) < \deg(g_0(x))$ and $g_0(x)$ is a monic right divisor of $x^n - \overline{\lambda}$ in $\mathbb{F}_{p^m}[x;\theta]$.*

Proof. Let C be a left ideal of type LI-1. If $C = \{0\}$, then $C = \langle 0\rangle = \langle x^n - \lambda\rangle$ has the desired properties.

Suppose C is non-zero. We prove that the generator polynomial $g(x)$ in Theorem 4.1.1 *i)* satisfies these properties. Recall that $g(x)$ is the unique monic skew polynomial in A, the set of all non-zero skew polynomials of minimal degree in C.

First, we show that $g(x)$ is a right divisor of $x^n - \lambda$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$. By the right division algorithm, there exist unique skew polynomials $q(x)$ and $r(x)$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$ such that

$$x^n - \lambda = q(x)g(x) + r(x),$$

and $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Then

$$r(x) = -q(x)g(x) + (x^n - \lambda) \in C.$$

By the minimality of $\deg(g(x))$, $r(x) = 0$. Hence, $g(x)$ is a right divisor of $x^n - \lambda$.

Finally, we write $g(x) = g_0(x) + ug_1(x)$, where $g_0(x), g_1(x) \in \mathbb{F}_{p^m}[x;\theta]$. Since $g(x)$ is monic, it is clear that $g_0(x)$ is monic and $\deg(g_1(x)) < \deg(g(x)) = \deg(g_0(x))$. Since $g(x)$ is a right divisor of $x^n - \lambda$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$, there exists $p(x)$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$ such that

$$x^n - \lambda = p(x)(g_0(x) + ug_1(x)).$$

Reducing modulo u, we have $x^n - \overline{\lambda} = \overline{p(x)}g_0(x)$ in $\mathbb{F}_{p^m}[x;\theta]$. This means $g_0(x)$ is a monic right divisor of $x^n - \overline{\lambda}$ in $\mathbb{F}_{p^m}[x;\theta]$. □

Proposition 4.1.3. *A left ideal of type* LI-2 *is principal and generated by* $g(x) = ug_1(x)$*, where* $g_1(x)$ *is a monic right divisor of* $x^n - \overline{\lambda}$ *in* $\mathbb{F}_{p^m}[x;\theta]$ *such that* $\deg(g_1(x)) < n$*.*

Proof. Let C be a left ideal of type LI-2. We prove that the generator polynomial $g(x) = ug_1(x)$ in Theorem 4.1.1 *ii)* satisfies the desired properties. Recall that $g(x) = ug_1(x)$ is the unique skew polynomial with leading coefficient u in A, the set of all non-zero skew polynomials of minimal degree in C. Clearly, $\deg(g_1(x)) < n$. By the right division algorithm, there exist unique skew polynomials $q(x)$ and $r(x)$ in $\mathbb{F}_{p^m}[x;\theta]$ such that

$$x^n - \overline{\lambda} = q(x)g_1(x) + r(x),$$

and $r(x) = 0$ or $\deg(r(x)) < \deg(g_1(x))$. Since $u(x^n - \bar{\lambda}) = u(x^n - \lambda)$, we have

$$\begin{aligned} ur(x) &= -uq(x)g_1(x) + u(x^n - \bar{\lambda}) \\ &= -\overrightarrow{q(x)}^u ug_1(x) + u(x^n - \lambda) \\ &= -\overrightarrow{q(x)}^u g(x) + u(x^n - \lambda) \in C. \end{aligned}$$

By the minimality of $\deg(g(x))$, $ur(x) = 0$. As $r(x) \in \mathbb{F}_{p^m}[x;\theta]$, $r(x) = 0$. Hence, $g_1(x)$ is a right divisor of $x^n - \overline{\lambda}$ in $\mathbb{F}_{p^m}[x;\theta]$. □

Proposition 4.1.4. *A left ideal of type* LI-3 *is generated by* $\{g(x) = ug_1(x), f(x) = f_0(x) + uf_1(x)\}$*, where* $f_0(x)$, $f_1(x)$, $g_1(x) \in \mathbb{F}_{p^m}[x;\theta]$ *satisfy the following properties:*

i) $g_1(x), f_0(x)$ *are monic,*

ii) $\deg(f_1(x)) < \deg(g_1(x)) < \deg(f_0(x)) < n$*,*

iii) $g_1(x)$ *is a right divisor of* $f_0(x)$ *in* $\mathbb{F}_{p^m}[x;\theta]$,

iv) $f_0(x)$ *is a right divisor of* $x^n - \overline{\lambda}$ *in* $\mathbb{F}_{p^m}[x;\theta]$.

Moreover, if $\lambda \in \mathbb{F}_{p^m}$, *then* $g_1(x)$ *is a right divisor of* $\overleftarrow{\left(\frac{x^n-\lambda}{f_0(x)}\right)}^u f_1(x)$ *in* $\mathbb{F}_{p^m}[x;\theta]$.

Proof. Let C be a left ideal of type LI-3. We prove that the generator set $\{g(x) = ug_1(x), f(x) = f_0(x) + uf_1(x)\}$ in Theorem 4.1.1 *iii)* satisfies the desired properties. Recall that $g(x) = ug_1(x)$ is the unique skew polynomial with the leading coefficient u in A, the set of all non-zero skew polynomials of minimal degree in C and $f_0(x) + uf_1(x)$ is the unique monic skew polynomial of minimal degree in C such that $\deg(f_1(x)) < \deg(g_1(x))$.

Properties *i)* and *ii)* are clear. Using the right division algorithm, we have

$$f_0(x) = q(x)g_1(x) + r(x),$$

for unique $q(x), r(x) \in \mathbb{F}_{p^m}[x;\theta]$ such that $r(x) = 0$ or $\deg(r(x)) < \deg(g_1(x))$. Then

$$\begin{aligned} ur(x) &= uf_0(x) - uq(x)g_1(x) \\ &= uf_0(x) - \overrightarrow{q(x)}^u ug_1(x) \\ &= uf(x) - \overrightarrow{q(x)}^u g(x) \in C. \end{aligned}$$

By the minimality of $\deg(g(x))$, $ur(x) = 0$. As $r(x) \in \mathbb{F}_{p^m}[x;\theta]$, $r(x) = 0$. Thus, *iii)* follows.

Note that $uf_0(x)$ is a skew polynomial of minimal degree in $\langle uf_0(x)\rangle$. Using arguments similar to the proof of Proposition 4.1.3, $f_0(x)$ is a right divisor of $x^n - \overline{\lambda}$ in $\mathbb{F}_{p^m}[x;\theta]$. Hence, property *iv)* is proved.

Finally, it is straightforward to see that if $\lambda \in \mathbb{F}_{p^m}$, then $\bar{\lambda} = \lambda$. Thus,

$$\begin{aligned}\frac{x^n-\lambda}{f_0(x)}(f_0(x)+uf_1(x)) &= \frac{x^n-\lambda}{f_0(x)}uf_1(x)\\ &= u\overleftarrow{\left(\frac{x^n-\lambda}{f_0(x)}\right)^u} f_1(x)\\ &\in C \cap u((\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle).\end{aligned}$$

Note that $C \cap u((\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle)$ is a left ideal in $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle$ containing $g(x) = ug_1(x)$ as a skew polynomial of minimal degree. Since $C \cap u((\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle)$ does not contain any monic element, by Proposition 4.1.3, it is generated by $g(x) = ug_1(x)$. Hence, $g_1(x)$ is a right divisor of $\overleftarrow{\left(\frac{x^n-\lambda}{f_0(x)}\right)^u} f_1(x)$. □

Example 4.1.5. Figures 4.1 and 4.2, respectively, show the ideal lattices of $(\mathbb{F}_3+u\mathbb{F}_3)[x]/\langle x^2-1\rangle$ and $(\mathbb{F}_3+u\mathbb{F}_3)[x;\Theta_{\mathrm{id},2}]/\langle x^2-1\rangle$, where $\Theta_{\mathrm{id},2}(a+bu) = a+2bu$ for all $a, b \in \mathbb{F}_3$. The subscripts 1, 2 and 3 indicate types LI-1, LI-2 and LI-3, respectively.

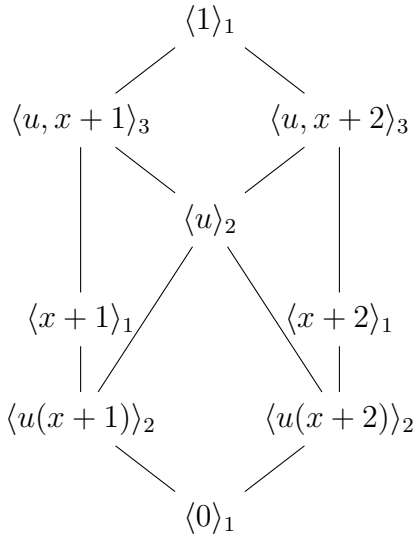

Figure 4.1: The ideal lattice of $(\mathbb{F}_3+u\mathbb{F}_3)[x]/\langle x^2-1\rangle$

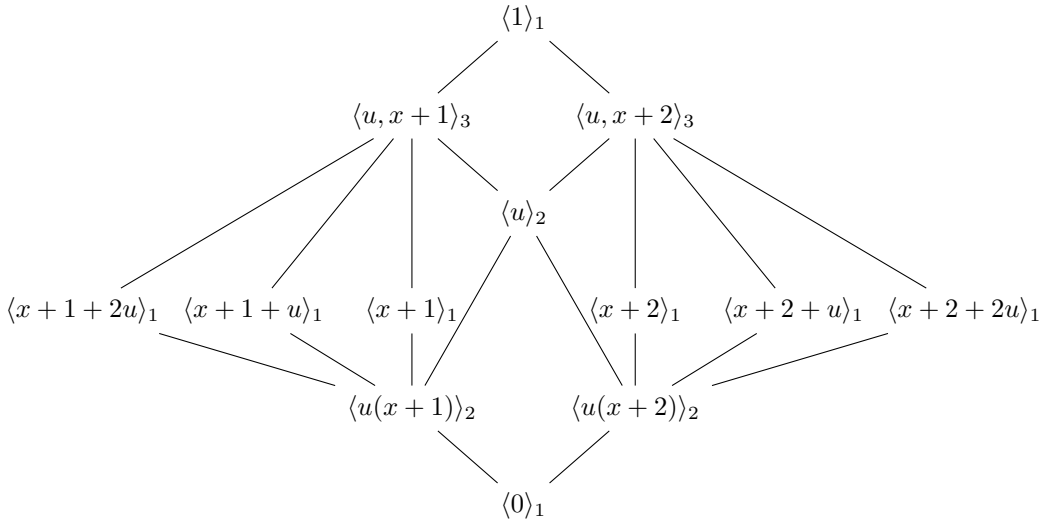

Figure 4.2: The ideal lattice of $(\mathbb{F}_3 + u\mathbb{F}_3)[x;\Theta_{\mathrm{id},2}]/\langle x^2-1\rangle$

Note that Figure 4.1 is embedded in Figure 4.2.

4.2 Euclidean Dual Codes of Skew-Cyclic and Skew-Negacyclic Codes

We study the structures of the Euclidean dual codes of skew-cyclic and skew-negacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. For this purpose, we assume that $\lambda = \pm 1$. Since $\bar{\lambda} = \lambda \in \mathbb{F}_{p^m}$ is always fixed by any automorphism, Θ can be arbitrary. However, the length n of codes is assumed to be a multiple of the order of Θ.

From $\lambda^2 = 1$, by Lemma 3.2.1, the Euclidean dual codes of skew-cyclic and skew-negacyclic codes are again skew-cyclic and skew-negacyclic, respectively. Their generators are given through the unique representation of the original codes and the ring anti-monomorphism φ defined in Proposition 2.2.7, where $\varphi(\sum_{i=0}^{t} a_i x^i) = \sum_{i=0}^{t} x^{-i} a_i$.

Theorem 4.2.1. *Let $\lambda \in \{-1, 1\}$. Then the Euclidean dual code of a left ideal in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$ is also a left ideal in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$*

determined as follows:

LI-1$^\perp$. *If* $C = \langle g_0(x) + ug_1(x) \rangle$, *then* $C^\perp = \langle x^{n-\deg(g_0(x))} \varphi \left(\dfrac{x^n - \lambda}{g_0(x) + ug_1(x)} \right) \rangle$.

LI-2$^\perp$. *If* $C = \langle ug_1(x) \rangle$, *then* $C^\perp = \langle u, x^{n-\deg(g_1(x))} \varphi \left(\dfrac{x^n - \lambda}{g_1(x)} \right) \rangle$.

LI-3$^\perp$. *If* $C = \langle ug_1(x), \overbrace{f_0(x) + uf_1(x)}^{u} \rangle$, *then there exists* $m(x) \in \mathbb{F}_{p^m}[x;\theta]$ *such that* $m(x)g_1(x) = \left(\dfrac{x^n - \lambda}{f_0(x)} \right) f_1(x)$ *and*

$$C^\perp = \langle x^{n-\deg(f_0(x))} \varphi \left(\frac{x^n - \lambda}{f_0(x)} u \right), x^{n-\deg(g_1(x))} \varphi \left(\frac{x^n - \lambda}{g_1(x)} - um(x) \right) \rangle.$$

For LI-1$^\perp$, the Euclidean dual code of type LI-1 code is determined in Theorem 3.2.3 and it is shown to be type LI-1. Moreover, $(C^\perp)^\perp = C$ implies that C is type LI-1 if and only if $C^\perp$ is type LI-1. However, this is not the case for types LI-2 and LI-3 (see Example 4.3.2).

In LI-2$^\perp$ and LI-3$^\perp$, $f_0(x)$, $g_1(x)$ are right divisors of $x^n - \lambda$ in $\mathbb{F}_{p^m}[x;\theta]$. Since $x^n - \lambda$ is central, it follows from (2.2.2) that

$$f_0(x)\frac{x^n - \lambda}{f_0(x)} = x^n - \lambda = \frac{x^n - \lambda}{f_0(x)} f_0(x), \tag{4.2.1}$$

$$g_1(x)\frac{x^n - \lambda}{g_1(x)} = x^n - \lambda = \frac{x^n - \lambda}{g_1(x)} g_1(x). \tag{4.2.2}$$

These two facts and the centrality of $x^n - \lambda$ will be frequently used in the following proofs.

Proof of LI-2$^\perp$. Let $D := \langle u, x^{n-\deg(g_1(x))} \varphi \left(\dfrac{x^n - \lambda}{g_1(x)} \right) \rangle$. Clearly, $u \in C^\perp$. It follows from (4.2.2) that $(ug_1(x))\dfrac{x^n - \lambda}{g_1(x)} = u(x^n - \lambda) = 0$ in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda \rangle$. Hence, $D \subseteq C^\perp$ is concluded via Lemma 3.2.2.

For the other direction, we note that $C^\perp$ is of either type LI-2 or LI-3. If $C^\perp = \langle us_1(x) \rangle$ is of type LI-2, then $C^\perp \subseteq \langle u \rangle \subseteq D$. Suppose that $C^\perp := \langle us_1(x), t_0(x) + ut_1(x) \rangle$ is of type LI-3. Clearly, $us_1(x), ut_1(x) \in \langle u \rangle \subseteq D$.

Since $ug_1(x) \in C$ and $t_0(x) + ut_1(x) \in C^\perp$, it follows from Lemma 3.2.2 that

$$\begin{aligned} 0 &= (ug_1(x))\varphi^{-1}(x^{-\deg(t_0(x))}(t_0(x) + ut_1(x))) \\ &= ug_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)) \end{aligned}$$

in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$. Thus, $g_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)) = 0$. Hence, in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$,

$$g_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)) = l_1(x)(x^n - \lambda) = (x^n - \lambda)l_1(x), \tag{4.2.3}$$

for some $l_1(x) \in \mathbb{F}_{p^m}[x;\theta]$. Note that

$$\deg(t_0(x)) = \deg(l_1(x)) + n - \deg(g_1(x)). \tag{4.2.4}$$

With the notation in (4.2.2), left cancellation of (4.2.3) by $g_1(x)$ gives

$$\frac{x^n - \lambda}{g_1(x)}l_1(x) = \varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)),$$

and hence, by (4.2.4),

$$\begin{aligned} t_0(x) &= x^{\deg(t_0(x))}\varphi\left(\frac{x^n - \lambda}{g_1(x)}l_1(x)\right) \\ &= x^{\deg(l_1(x))+n-\deg(g_1(x))}\varphi(l_1(x))\varphi\left(\frac{x^n - \lambda}{g_1(x)}\right) \\ &= x^{\deg(l_1(x))}\overrightarrow{\varphi(l_1(x))}^{x^{n-\deg(g_1(x))}}x^{n-\deg(g_1(x))}\varphi\left(\frac{x^n - \lambda}{g_1(x)}\right) \in D. \end{aligned}$$

Consequently, $t_0(x) + ut_1(x) \in D$ and $C^\perp \subseteq D$, as desired. □

Proof of LI-3$^\perp$. Since $\lambda \in \mathbb{F}_{p^m}$, it follows from Proposition 4.1.4 that $g_1(x)$ is a right divisor of $\overleftarrow{\left(\frac{x^n - \lambda}{f_0(x)}\right)}^u f_1(x)$. Then there exists $m(x) \in \mathbb{F}_{p^m}[x;\theta]$ such that

$$m(x)g_1(x) = \overleftarrow{\left(\frac{x^n - \lambda}{f_0(x)}\right)}^u f_1(x). \tag{4.2.5}$$

Let $D := \langle x^{n-\deg(f_0(x))}\varphi\left(\frac{x^n - \lambda}{f_0(x)}u\right), x^{n-\deg(g_1(x))}\varphi\left(\frac{x^n - \lambda}{g_1(x)} - um(x)\right)\rangle$. It follows from (4.2.5) that

$$um(x)g_1(x) = u\overleftarrow{\left(\frac{x^n - \lambda}{f_0(x)}\right)}^u f_1(x) = \frac{x^n - \lambda}{f_0(x)}uf_1(x). \tag{4.2.6}$$

Multiplying on the left of (4.2.6) by $f_0(x)$, we have

$$\begin{aligned} f_0(x)um(x)g_1(x) &= f_0(x)\frac{x^n-\lambda}{f_0(x)}uf_1(x) \\ &= (x^n-\lambda)uf_1(x) \qquad \text{(using (4.2.1))} \\ &= uf_1(x)(x^n-\lambda) \\ &= uf_1(x)\frac{x^n-\lambda}{g_1(x)}g_1(x) \quad \text{(using (4.2.2)).} \end{aligned}$$

Hence,

$$f_0(x)um(x) = uf_1(x)\frac{x^n-\lambda}{g_1(x)}, \tag{4.2.7}$$

and

$$\deg(m(x)) = n + \deg(f_1(x)) - \deg(f_0(x)) - \deg(g_1(x)). \tag{4.2.8}$$

Now, we observe the followings:

a) Since $u^2 = 0$, we have

$$ug_1(x)\frac{x^n-\lambda}{f_0(x)}u = 0. \tag{4.2.9}$$

b) Using $u^2 = 0$ and (4.2.2), we conclude that

$$ug_1(x)\left(\frac{x^n-\lambda}{g_1(x)} - um(x)\right) = ug_1(x)\frac{x^n-\lambda}{g_1(x)} = u(x^n-\lambda). \tag{4.2.10}$$

c) It follows from $u^2 = 0$ and (4.2.1) that

$$(f_0(x) + uf_1(x))(\frac{x^n-\lambda}{f_0(x)}u) = f_0(x)\frac{x^n-\lambda}{f_0(x)}u = (x^n-\lambda)u = u(x^n-\lambda). \tag{4.2.11}$$

d) Since $g_1(x)$ is a right divisor of $f_0(x)$, by (2.2.1) and (4.2.2), we have

$$\begin{aligned} f_0(x)\frac{x^n-\lambda}{g_1(x)} = \left(\frac{f_0(x)}{g_1(x)}g_1(x)\right)\frac{x^n-\lambda}{g_1(x)} &= \frac{f_0(x)}{g_1(x)}\left(g_1(x)\frac{x^n-\lambda}{g_1(x)}\right) \\ &= \frac{f_0(x)}{g_1(x)}(x^n-\lambda). \end{aligned} \tag{4.2.12}$$

The next equation follows from $u^2 = 0$, (4.2.7) and (4.2.12)

$$\begin{aligned}(f_0(x) + uf_1(x))\left(\frac{x^n - \lambda}{g_1(x)} - um(x)\right) &= f_0(x)\frac{x^n - \lambda}{g_1(x)} + uf_1(x)\frac{x^n - \lambda}{g_1(x)} \\ &\quad - f_0(x)um(x) \\ &= \frac{f_0(x)}{g_1(x)}(x^n - \lambda). \qquad (4.2.13)\end{aligned}$$

Equations (4.2.9)-(4.2.11) and (4.2.13) equal 0 in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$. Thus, $D \subseteq C^\perp$ by Lemma 3.2.2.

For the reverse inclusion, we note that $C^\perp$ is of type LI-2 or LI-3. First, suppose that $C^\perp := \langle us_1(x)\rangle$ is of type LI-2. Since $f_0(x) + uf_1(x) \in C$ and $us_1(x) \in C^\perp$, the Euclidean orthogonality and Lemma 3.2.2 imply that

$$(f_0(x) + uf_1(x))\varphi^{-1}(x^{-\deg(s_1)}us_1(x)) = 0$$

in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$. Hence, in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$,

$$f_0(x)\varphi^{-1}(x^{-\deg(s_1(x))}us_1(x)) = ul(x)(x^n - \lambda) = (x^n - \lambda)ul(x), \qquad (4.2.14)$$

for some $l(x) \in \mathbb{F}_{p^m}[x;\theta]$. Moreover, $\deg(s_1(x)) = n + \deg(l(x)) - \deg(f_0(x))$. It follows from (4.2.1) and (4.2.14) that

$$\varphi^{-1}(x^{-(n+\deg(l(x))-\deg(f_0(x)))}us_1(x)) = \varphi^{-1}(x^{-\deg(s_1(x))}us_1(x)) = \frac{x^n - \lambda}{f_0(x)}ul(x).$$

Since φ is a ring anti-monomorphism, we conclude that

$$x^{-(n+\deg(l(x))-\deg(f_0(x)))}us_1(x) = \varphi\left(\frac{x^n - \lambda}{f_0(x)}ul(x)\right) = \varphi(l(x))\varphi\left(\frac{x^n - \lambda}{f_0(x)}u\right).$$

Consequently,

$$\begin{aligned}us_1(x) &= x^{n+\deg(l(x))-\deg(f_0(x))}\varphi(l(x))\varphi\left(\frac{x^n - \lambda}{f_0(x)}u\right) \\ &= x^{\deg(l(x))}\overrightarrow{\varphi(l(x))}^{x^{n-\deg(f_0(x))}}x^{n-\deg(f_0(x))}\varphi\left(\frac{x^n - \lambda}{f_0(x)}u\right) \in D.\end{aligned}$$

Next, suppose that $C^{\perp} := \langle us_1(x), t_0(x) + ut_1(x)\rangle$ is of type LI-3. Using arguments similar to those above, $f_0(x) + uf_1(x) \in C$ and $us_1(x) \in C^{\perp}$ imply $us_1(x) \in D$.

Since $ug_1(x) \in C$ and $t_0(x) + ut_1(x) \in C^{\perp}$, it follows from Lemma 3.2.2 that

$$0 = ug_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}(t_0(x) + ut_1(x))) = ug_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)),$$

in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$. Thus, $g_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)) = 0$, and hence, in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]$,

$$g_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)) = l_1(x)(x^n - \lambda) = (x^n - \lambda)l_1(x), \tag{4.2.15}$$

for some $l_1(x) \in \mathbb{F}_{p^m}[x;\theta]$. Note that

$$\deg(t_0(x)) = n + \deg(l_1(x)) - \deg(g_1(x)). \tag{4.2.16}$$

In the notation of (4.2.2), the left cancellation of (4.2.15) by $g_1(x)$ implies

$$\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)) = \frac{x^n - \lambda}{g_1(x)}l_1(x), \tag{4.2.17}$$

and hence

$$t_0(x) = x^{\deg(t_0(x))}\varphi\left(\frac{x^n - \lambda}{g_1(x)}l_1(x)\right) = x^{\deg(t_0(x))}\varphi(l_1(x))\varphi\left(\frac{x^n - \lambda}{g_1(x)}\right). \tag{4.2.18}$$

By Lemma 3.2.2, in $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle$,

$$\begin{aligned}
0 &= (f_0(x)+uf_1(x))\varphi^{-1}(x^{-\deg(t_0(x))}(t_0(x)+ut_1(x)))\\
&= f_0(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x)) + f_0(x)\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x))\\
&\qquad + uf_1(x)\varphi^{-1}(x^{-\deg(t_0(x))}t_0(x))\\
&= f_0(x)\frac{x^n-\lambda}{g_1(x)}l_1(x) + f_0(x)\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x)) + uf_1(x)\frac{x^n-\lambda}{g_1(x)}l_1(x)\\
&\qquad \text{(using (4.2.17))}\\
&= \frac{f_0(x)}{g_1(x)}(x^n-\lambda)l_1(x) + f_0(x)\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x)) + f_0(x)um(x)l_1(x)\\
&\qquad \text{(using (2.2.1), (4.2.2) and (4.2.7))}\\
&= \frac{f_0(x)}{g_1(x)}l_1(x)(x^n-\lambda) + f_0(x)\left(\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x)) + um(x)l_1(x)\right)\\
&= f_0(x)(\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x)) + um(x)l_1(x)).
\end{aligned}$$

Then there exists $l_2(x)\in\mathbb{F}_{p^m}[x;\theta]$ such that, in $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]$,

$$\begin{aligned}
f_0(x)(\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x)) + um(x)l_1(x)) &= ul_2(x)(x^n-\lambda)\\
&= (x^n-\lambda)ul_2(x). \qquad (4.2.19)
\end{aligned}$$

Using (4.2.8), (4.2.16) and the fact $\deg(f_0(x)) > \deg(f_1(x))$, we conclude that

$$\deg(m(x)l_1(x)) \le \deg(m(x)) + \deg(l_1(x)) < \deg(t_0(x)). \qquad (4.2.20)$$

Thus, from (4.2.19) and (4.2.20),

$$\deg(t_0(x)) = n + \deg(l_2(x)) - \deg(f_0(x)). \qquad (4.2.21)$$

The left cancellation of (4.2.19) by $f_0(x)$ implies

$$\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x)) + um(x)l_1(x) = \frac{x^n-\lambda}{f_0(x)}ul_2(x).$$

Hence, $\varphi^{-1}(x^{-\deg(t_0(x))}ut_1(x)) = \dfrac{x^n-\lambda}{f_0(x)}ul_2(x) - um(x)l_1(x)$, i.e.,

$$ut_1(x) = x^{\deg(t_0(x))}\varphi\left(\frac{x^n-\lambda}{f_0(x)}ul_2(x) - um(x)l_1(x)\right). \qquad (4.2.22)$$

Therefore,

$$\begin{aligned}
t_0(x)+ut_1(x) &= x^{\deg(t_0(x))}\varphi(l_1(x))\varphi\left(\frac{x^n-\lambda}{g_1(x)}\right)\\
&\quad + x^{\deg(t_0(x))}\varphi\left(\frac{x^n-\lambda}{f_0(x)}ul_2(x)-um(x)l_1(x)\right)\\
&\quad \text{(using (4.2.18) and (4.2.22))}\\
&= x^{\deg(t_0(x))}\varphi(l_1(x))\varphi\left(\frac{x^n-\lambda}{g_1(x)}\right)-x^{\deg(t_0(x))}\varphi(l_1(x))\varphi(um(x))\\
&\quad + x^{\deg(t_0(x))}\varphi\left(\frac{x^n-\lambda}{f_0(x)}ul_2(x)\right)\\
&= x^{n+\deg(l_1(x))-\deg(g_1(x))}\varphi(l_1(x))\varphi\left(\frac{x^n-\lambda}{g_1(x)}-um(x)\right)\\
&\quad + x^{n+\deg(l_2(x))-\deg(f_0(x))}\varphi(l_2(x))\varphi(\frac{x^n-\lambda}{f_0(x)}u)\\
&\quad \text{(using (4.2.16) and (4.2.21))}\\
&= x^{\deg(l_1(x))}\overrightarrow{\varphi(l_1(x))}^{x^{n-\deg(g_1(x))}}x^{n-\deg(g_1(x))}\varphi\left(\frac{x^n-\lambda}{g_1(x)}-um(x)\right)\\
&\quad + x^{\deg(l_2(x))}\overrightarrow{\varphi(l_2(x))}^{x^{n-\deg(f_0(x))}}x^{n-\deg(f_0(x))}\varphi(\frac{x^n-\lambda}{f_0(x)}u)\in D,
\end{aligned}$$

and we have $C^{\perp}\subseteq D$ as desired. □

4.3 Hermitian Dual Codes of Skew-Cyclic and Skew-Negacyclic Codes

We assume that the order of Θ is 2 and determine the structure of the Hermitian dual codes of skew-cyclic and skew-negacyclic codes in terms of their unique representative generators, the ring anti-monomorphism φ defined in Proposition 2.2.7 and the ring automorphism Φ defined in (3.3.1). Using Lemma 3.3.2 and arguments similar to those in the previous subsection, the next theorem follows.

Theorem 4.3.1. *Let $\lambda\in\{1,-1\}$ and let Θ be an automorphism of order 2. Then the Hermitian dual code of a left ideal in $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle$ is again a left ideal in $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle$ determined as follows:*

LI-1$^{\perp_H}$. *If* $C = \langle g_0(x)+ug_1(x)\rangle$, *then* $C^{\perp_H} = \langle \Phi(x^{n-\deg(g_0(x))}\varphi\left(\frac{x^n-\lambda}{g_0(x)+ug_1(x)}\right))\rangle$.

LI-2$^{\perp_H}$. *If* $C = \langle ug_1(x)\rangle$, *then* $C^{\perp_H} = \langle u, \Phi(x^{n-\deg(g_1(x))}\varphi\left(\frac{x^n-\lambda}{g_1(x)}\right))\rangle$.

LI-3$^{\perp_H}$. *If* $C = \langle ug_1(x), \overleftarrow{f_0(x)+uf_1(x)}^{u}\rangle$, *then there exists* $m(x) \in \mathbb{F}_{p^m}[x;\theta]$ *such that* $m(x)g_1(x) = \left(\frac{x^n-\lambda}{f_0(x)}\right) f_1(x)$ *and*

$$C^{\perp_H} = \langle \Phi(x^{n-\deg(f_0(x))}\varphi\left(\frac{x^n-\lambda}{f_0(x)}u\right)), \Phi(x^{n-\deg(g_1(x))}\varphi\left(\frac{x^n-\lambda}{g_1(x)} - um(x)\right))\rangle.$$

Example 4.3.2. Table 4.1 shows the Euclidean and Hermitian dual codes of the left ideals in $(\mathbb{F}_3 + u\mathbb{F}_3)[x;\Theta_{\mathrm{id},2}]/\langle x^2-1\rangle$ classified in Example 4.1.5. The dual codes are obtained via Theorems 4.2.1 and 4.3.1 and rewritten to satisfy the representation in Proposition 4.1.1. The subscripts 1, 2 and 3 indicate types LI-1, LI-2 and LI-3, respectively.

C	$C^{\perp}$	$C^{\perp_H}$
$\langle 0\rangle_1$	$\langle 1\rangle_1$	$\langle 1\rangle_1$
$\langle u(x+1)\rangle_2$	$\langle u, x+2\rangle_3$	$\langle u, x+2\rangle_3$
$\langle u(x+2)\rangle_2$	$\langle u, x+1\rangle_3$	$\langle u, x+1\rangle_3$
$\langle u\rangle_2$	$\langle u\rangle_2$	$\langle u\rangle_2$
$\langle x+1+2u\rangle_1$	$\langle x+2+2u\rangle_1$	$\langle x+2+u\rangle_1$
$\langle x+1+u\rangle_1$	$\langle x+2+u\rangle_1$	$\langle x+2+2u\rangle_1$
$\langle x+1\rangle_1$	$\langle x+2\rangle_1$	$\langle x+2\rangle_1$
$\langle x+2\rangle_1$	$\langle x+1\rangle_1$	$\langle x+1\rangle_1$
$\langle x+2+u\rangle_1$	$\langle x+1+u\rangle_1$	$\langle x+1+2u\rangle_1$
$\langle x+2+2u\rangle_1$	$\langle x+1+2u\rangle_1$	$\langle x+1+u\rangle_1$
$\langle u, x+1\rangle_3$	$\langle u(x+2)\rangle_2$	$\langle u(x+2)\rangle_2$
$\langle u, x+2\rangle_3$	$\langle u(x+1)\rangle_2$	$\langle u(x+1)\rangle_2$
$\langle 1\rangle_1$	$\langle 0\rangle_1$	$\langle 0\rangle_1$

Table 4.1: The left ideals in $(\mathbb{F}_3 + u\mathbb{F}_3)[x;\Theta_{\mathrm{id},2}]/\langle x^2-1\rangle$ and their Euclidean and Hermitian dual codes

CHAPTER V

GRAY IMAGES OF CODES OVER $\mathcal{R}_{(p^m,e)}$

The discovery of good nonlinear codes from linear codes over $\mathbb{Z}_4$, via the Gray map [21], motivated the study of the Gray images of codes over rings in general. Analogs of the Gray map have also been defined for codes over other finite chain rings [19] linked these codes to codes over finite fields. Qian, Zhang and Zhu characterized the Gray images of $(1+u)$-constacyclic and cyclic codes over the ring $\mathcal{R}_{(2,2)} = \mathbb{F}_2 + u\mathbb{F}_2$ in [30] and investigated some constacyclic codes over $\mathcal{R}_{(2,3)} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ in [31]. Congellenmis [11] have introduced $(1-u^{e-1})$-constacyclic codes over $\mathcal{R}_{(2,e)} = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{e-1}\mathbb{F}_2$ and generalized the results of [30] and [31].

Motivated by these works, we generalize these concepts to the finite chain ring $\mathcal{R}_{(p^m,e)} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$. We study $(1-u^{e-1})$-constacyclic, cyclic and $(1+u^{e-1})$-constacyclic codes over this ring and characterize the structures of the Gray images of such codes. Moreover, we give descriptions concerning the Gray images of some skew-constacyclic codes over $\mathcal{R}_{(p^m,e)}$.

First, we recall some necessary definitions and introduce some useful notations. In (2.1.1), an element $r \in \mathcal{R}_{(p^m,e)}$ is uniquely written as

$$r = a_0 + ua_1 + \cdots + u^{e-1}a_{e-1},$$

where $a_i \in \mathbb{F}_{p^m}$. Hence, an element $\boldsymbol{r} \in {\mathcal{R}_{(p^m,e)}}^n$ can be viewed as

$$\boldsymbol{r} = a_0(\boldsymbol{r}) + ua_1(\boldsymbol{r}) + \cdots + u^{e-1}a_{e-1}(\boldsymbol{r}),$$

where $a_i(\boldsymbol{r}) = (r_{i,0}, r_{i,1}, \ldots, r_{i,n-1})$ is a vector in $\mathbb{F}_{p^m}^n$, for every $0 \leq i \leq e-1$, or

$$\boldsymbol{r} = (r_0, r_1, \ldots, r_{n-1}), \tag{5.1}$$

where $r_i = r_{0,i} + ur_{1,i} + \cdots + u^{e-1}r_{e-1,i} \in \mathcal{R}_{(p^m,e)}$, for every $0 \leq i \leq n-1$.

Let $\rho, \rho_{1-u^{e-1}}, \rho_{1+u^{e-1}} : {\mathcal{R}_{(p^m,e)}}^n \to {\mathcal{R}_{(p^m,e)}}^n$ be defined by

$$\rho((r_0, r_1, \ldots, r_{n-1})) = (r_{n-1}, r_0, \ldots, r_{n-2}),$$

$$\rho_{1-u^{e-1}}((r_0, r_1, \ldots, r_{n-1})) = ((1-u^{e-1})r_{n-1}, r_0, \ldots, r_{n-2})$$

and

$$\rho_{1+u^{e-1}}((r_0, r_1, \ldots, r_{n-1})) = ((1+u^{e-1})r_{n-1}, r_0, \ldots, r_{n-2}).$$

In the light of (2.3.1), a code C of length n over $\mathcal{R}_{(p^m,e)}$ satisfying $\rho(C) = C$ is a *cyclic code*, while C satisfying $\rho_{1-u^{e-1}}(C) = C$ and $\rho_{1+u^{e-1}}(C) = C$ are called $(1-u^{e-1})$-*constacyclic* and $(1+u^{e-1})$-constacyclic codes, respectively.

Let $\sigma^{\otimes p^{m(e-1)-1}} : \mathbb{F}_{p^m}^{p^{m(e-1)}n} \to \mathbb{F}_{p^m}^{p^{m(e-1)}n}$ be defined by

$$(a^{(0)} \mid a^{(1)} \mid \cdots \mid a^{(p^{m(e-1)-1}-1)}) \mapsto (\varphi(a^{(0)}) \mid \varphi(a^{(1)}) \mid \cdots \mid \varphi(a^{(p^{m(e-1)-1}-1)})),$$

where $a^{(i)} \in \mathbb{F}_{p^m}^{pn}$, $\mid$ a vector concatenation and $\varphi : \mathbb{F}_{p^m}^{pn} \to \mathbb{F}_{p^m}^{pn}$ denotes the cyclic shift on $\mathbb{F}_{p^m}^{pn}$:

$$\varphi((c_0, c_1, \ldots, c_{pn-1})) = (c_{pn-1}, c_0, \ldots, c_{pn-2}).$$

A code $\widetilde{C}$ of length $p^{m(e-1)}n$ over $\mathbb{F}_{p^m}$ satisfying $\sigma^{\otimes p^{m(e-1)-1}}(\widetilde{C}) = \widetilde{C}$ is called a *quasi-cyclic code of index* $p^{m(e-1)-1}$. In general, for an automorphism $\theta \in \mathrm{Aut}(\mathbb{F}_{p^m})$ and a permutation δ on $\{0, 1, \ldots, p^{m(e-1)}n-1\}$, $\widetilde{C}$ is called a θ-δ-*invariant code*, a generalization of a permutation invariant code [24], if it is invariant under a composition of the permutation δ on the coordinates and the map defined by taking θ coordinatewise.

Codes $\widetilde{C}_1$ and $\widetilde{C}_2$ are said to be *permutatively equivalent* if $\widetilde{C}_2$ can be obtained from permuting the coordinates of $\widetilde{C}_1$.

5.1 Homogeneous Weights and Gray Maps

A homogeneous distance has firstly been introduced for arbitrary finite chain ring in [19]. In light of this, the homogeneous distance on ${\mathcal{R}_{(p^m,e)}}^n$ can be defined in terms of the weight function $w_{hom}(\boldsymbol{r})$ as follows:

$$w_{hom}(\boldsymbol{r}) = \sum_{i=0}^{n-1} w_{hom}(r_i)$$

for all $\boldsymbol{r} = (r_0, r_1, \ldots, r_{n-1}) \in {\mathcal{R}_{(p^m,e)}}^n$, where

$$w_{hom}(r) = \begin{cases} p^{m(e-2)}(p^m - 1) & \text{if } r \in \mathcal{R}_{(p^m,e)} \setminus u^{e-1}\mathcal{R}_{(p^m,e)}, \\ p^{m(e-1)} & \text{if } r \in u^{e-1}\mathcal{R}_{(p^m,e)} \setminus \{0\}, \\ 0 & \text{otherwise.} \end{cases}$$

The *homogeneous distance* $d_{hom}(\boldsymbol{r}, \boldsymbol{s})$ between vectors $\boldsymbol{r}, \boldsymbol{s}$ in ${\mathcal{R}_{(p^m,e)}}^n$ is defined to be $w_{hom}(\boldsymbol{r} - \boldsymbol{s})$. The minimum homogeneous distance $d_{hom}(C)$ of a code C over $\mathcal{R}_{(p^m,e)}$ is defined by

$$d_{hom}(C) := \min\{d_{hom}(\boldsymbol{r}, \boldsymbol{s}) \mid \boldsymbol{r} \neq \boldsymbol{s} \in C\}.$$

When the code C is linear, $d_{hom}(C)$ is the minimum homogeneous weight of non-zero elements in C.

Example 5.1.1. In $\mathcal{R}_{(3,2)} = \mathbb{F}_3 + u\mathbb{F}_3$,

$$w_{hom}(r) = \begin{cases} 2 & \text{if } r \in \{1, 1+u, 1+2u, 2, 2+u, 2+2u\}, \\ 3 & \text{if } r \in \{u, 2u\}, \\ 0 & \text{if } r = 0. \end{cases}$$

Let

$$\begin{aligned} C = \{&(0,0,0,0), (2,1+u,2+u,1), (1+2u,2,1+u,2+u), \\ &(2+2u,1+2u,2,1+u), (1,2+2u,1+2u,2), (2+u,1,2+2u,1+2u), \\ &(1+u,2+u,1,2+2u), (2u,u,2u,u), (u,2u,u,2u)\}. \end{aligned}$$

Then C is a linear $(1-u)$-constacyclic code of length 4 over $\mathcal{R}_{(3,2)}$. Every non-zero element in C has Hamming weight 4, and hence $d_{Ham}(C) = 4$. The elements $(2, 1+u, 2+u, 1), (1+2u, 2, 1+u, 2+u), (2+2u, 1+2u, 2, 1+u), (1, 2+2u, 1+2u, 2), (2+u, 1, 2+2u, 1+2u)$ and $(1+u, 2+u, 1, 2+2u)$ have homogeneous weight 8 and $(2u, u, 2u, u)$ and $(u, 2u, u, 2u)$ have homogeneous weight 12. Therefore, $d_{hom}(C) = 8$.

In order to define the Gray map for $\mathcal{R}_{(p^m,e)}$, an element $\epsilon \in \mathbb{Z}_{p^m}$ is viewed uniquely as the p-adic representation

$$\epsilon = \xi_0(\epsilon) + \xi_1(\epsilon)p + \cdots + \xi_{m-1}(\epsilon)p^{m-1},$$

where $\xi_i(\epsilon) \in \{0, 1, \ldots, p-1\}$, for every $0 \leq i \leq m-1$. Let α be a primitive element of $\mathbb{F}_{p^m}$. For each $\epsilon \in \mathbb{Z}_{p^m}$, the element $\alpha_\epsilon \in \mathbb{F}_{p^m}$ corresponding to ϵ is given by

$$\alpha_\epsilon := \xi_0(\epsilon) + \xi_1(\epsilon)\alpha + \cdots + \xi_{m-1}(\epsilon)\alpha^{m-1}.$$

Similarly, an element $\omega \in \mathbb{Z}_{p^{m(e-1)}}$ is viewed uniquely as the p^m-adic representation

$$\omega = \overline{\xi}_0(\omega) + \overline{\xi}_1(\omega)p^m + \cdots + \overline{\xi}_{e-2}(\omega)p^{m(e-2)},$$

where $\overline{\xi}_i(\omega) \in \{0, 1, \ldots, p^m - 1\}$, for every $0 \leq i \leq e-2$.

We define the Gray map $\Phi : {\mathcal{R}_{(p^m,e)}}^n \to \mathbb{F}_{p^m}^{p^{m(e-1)}n}$ by

$$\Phi(\boldsymbol{r}) = (\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{p^{m(e-1)}-1}),$$

for all $\boldsymbol{r} = a_0(\boldsymbol{r}) + ua_1(\boldsymbol{r}) + \cdots + u^{e-1}a_{e-1}(\boldsymbol{r}) \in {\mathcal{R}_{(p^m,e)}}^n$, where

$$\boldsymbol{b}_{\omega p^m+\epsilon} = \alpha_\epsilon a_0(\boldsymbol{r}) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} a_l(\boldsymbol{r}) + a_{e-1}(\boldsymbol{r}), \tag{5.1.1}$$

for all $0 \leq \omega \leq p^{m(e-2)} - 1$ and $0 \leq \epsilon \leq p^m - 1$.

Theorem 5.1.2. *The Gray map Φ is an $\mathbb{F}_{p^m}$-linear isometry from $(\mathcal{R}_{(p^m,e)}{}^n, d_{hom})$ to $(\mathbb{F}_{p^m}^{p^{m(e-1)}n}, d_{Ham})$, where d_{Ham} denotes the Hamming distance on $\mathbb{F}_{p^m}^{p^{m(e-1)}n}$.*

Proof. The linearity is clear. It suffices to show that, for all $r \neq s \in \mathcal{R}_{(p^m,e)}$,

$$w_{hom}(r-s) = w_{Ham}(\Phi(r) - \Phi(s)),$$

where w_{Ham} denotes the Hamming weight. We observe that

$$\Phi(u^{e-1}r) = (a_0(r), a_0(r), \ldots, a_0(r)) \tag{5.1.2}$$

$$\Phi(r + u^{e-1}s) = \Phi(r) + \Phi(u^{e-1}s). \tag{5.1.3}$$

For the case $r - s \in u^{e-1}R_{(p^m,e)} \setminus \{0\}$. That is $r - s = u^{e-1}t$ for some $t \in \mathcal{R}_{(p^m,e)}$. It follows from (5.1.3) that $\Phi(r) - \Phi(s) = \Phi(r-s) = \Phi(u^{e-1}t)$. Hence, by (5.1.2), $w_{Ham}(\Phi(r)-\Phi(s)) = w_{Ham}(\Phi(u^{e-1}t)) = p^{m(e-1)} = w_{hom}(r-s)$.

Next, assume that $r - s \in \mathcal{R}_{(p^m,e)} \setminus u^{e-1}\mathcal{R}_{(p^m,e)}$. Write $r = s + u^j t$, where $0 \leq j \leq e-2$ and $t \in \mathcal{R}_{(p^m,e)} \setminus u\mathcal{R}_{(p^m,e)}$. To compute $w_{Ham}(\Phi(r) - \Phi(s))$, we count the number of $0 \leq \omega \leq p^{m(e-1)} - 1$ and $0 \leq \epsilon \leq p^m - 1$ such that

$$\begin{aligned} 0 &= \alpha_\epsilon (a_0(r) - a_0(s)) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} (a_l(r) - a_l(s)) + (a_{e-1}(r) - a_{e-1}(s)) \\ &= \alpha_\epsilon a_0(u^j t) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} a_l(u^j t) + a_{e-1}(u^j t). \end{aligned} \tag{5.1.4}$$

It follows from $a_j(u^j t) \neq 0$ that $a_j(r) - a_j(s) \neq 0$. Consequently, equation (5.1.4) is a linear equation in the $e-1$ variables α_ϵ and $\alpha_{\overline{\xi}_l(\omega)}$ $(0 \leq l \leq e-3)$. So, the number of distinct pairs (ω, ϵ) corresponding to solutions is $p^{m(e-2)}$. Hence, we have $w_{Ham}(\Phi(r) - \Phi(s)) = p^{m(e-1)} - p^{m(e-2)} = p^{m(e-2)}(p^m - 1) = w_{hom}(r-s)$. □

Example 5.1.3. Let

$$\begin{aligned} C = \{&(0,0,0,0), (2,1+u,2+u,1), (1+2u,2,1+u,2+u), \\ &(2+2u,1+2u,2,1+u), (1,2+2u,1+2u,2), (2+u,1,2+2u,1+2u), \\ &(1+u,2+u,1,2+2u), (2u,u,2u,u), (u,2u,u,2u)\} \end{aligned}$$

be a code as in Example 5.1.1. Then

$$\begin{aligned}\Phi(C) = \{&(0,0,0,0,0,0,0,0,0,0,0,0),(0,1,1,0,2,2,0,1,1,0,2,2),\\ &(2,0,1,1,0,2,2,0,1,1,0,2),(2,2,0,1,1,0,2,2,0,1,1,0),\\ &(0,2,2,0,1,1,0,2,2,0,1,1),(1,0,2,2,0,1,1,0,2,2,0,1),\\ &(1,1,0,2,2,0,1,1,0,2,2,0),(2,1,2,1,2,1,2,1,2,1,2,1),\\ &(1,2,1,2,1,2,1,2,1,2,1,2)\}.\end{aligned}$$

Hence, $d_{hom}(C) = 8 = d_{Ham}(\Phi(C))$.

In order to establish the onward results, an element $\boldsymbol{r} \in {\mathcal{R}_{(p^m,e)}}^n$ is viewed as in (5.1), i.e., $\boldsymbol{r} = (r_0, r_1, \ldots, r_{n-1})$, where $r_i = r_{0,i} + ur_{1,i} + \cdots + u^{e-1}r_{e-1,i} \in \mathcal{R}_{(p^m,e)}$ for every $0 \leq i \leq n-1$. Corresponding to this representation of $\boldsymbol{r}$, $\Phi(\boldsymbol{r})$ is written as

$$\Phi(\boldsymbol{r}) = (b_0, b_1, \ldots, b_{p^{m(e-1)}n-1}),$$

where

$$b_{(\omega p^m+\epsilon)n+j} = \alpha_\epsilon r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j}, \tag{5.1.5}$$

for all $0 \leq \omega \leq p^{m(e-2)} - 1$, $0 \leq \epsilon \leq p^m - 1$ and $0 \leq j \leq n-1$.

It follows from equations (5.1.1) and (5.1.5) that for each $0 \leq \omega \leq p^{m(e-2)} - 1$ and $0 \leq \epsilon \leq p^m - 1$, $\boldsymbol{b}_{\omega p^m+\epsilon} = (b_{(\omega p^m+\epsilon)n}, b_{(\omega p^m+\epsilon)n+1}, \ldots, b_{(\omega p^m+\epsilon)n+n-1})$.

5.2 Gray Images of $(1-u^{e-1})$-Constacyclic Codes

A characterization of the Gray images of $(1-u^{e-1})$-constacyclic codes over $\mathcal{R}_{(p^m,e)}$ is given through the next theorem.

Theorem 5.2.1. $\Phi \circ \rho_{1-u^{e-1}} = \sigma^{\otimes p^{m(e-1)-1}} \circ \Phi$.

Proof. Observe that

$$\begin{aligned}\rho_{1-u^{e-1}}(\boldsymbol{r}) \;\; = (\;\; & r_{0,n-1} + ua_{1,n-1} + \cdots + u^{e-1}(r_{e-1,n-1} - r_{0,n-1}),\\ & r_{0,0} + ua_{1,0} + \cdots + u^{e-1}r_{e-1,0}, \ldots,\\ & r_{0,n-2} + ur_{1,n-2} + \cdots + u^{e-1}r_{e-1,n-2}).\end{aligned}$$

Let $(d_0, d_1, \ldots, d_{p^{m(e-1)}n-1}) = \Phi \circ \rho_{1-u^{e-1}}(\boldsymbol{r})$. Then for each $0 \le \omega \le p^{m(e-2)} - 1$, $0 \le \epsilon \le p^m - 1$ and $0 \le j \le n-1$,

$$d_{(\omega p^m+\epsilon)n+j} = \begin{cases} \alpha_\epsilon r_{0,j-1} + \sum_{l=1}^{e-2} \alpha_{\bar{\xi}_{l-1}(\omega)} r_{l,j-1} + r_{e-1,j-1} & \text{if } j \neq 0,\\ (\alpha_\epsilon - 1) r_{0,n-1} + \sum_{l=1}^{e-2} \alpha_{\bar{\xi}_{l-1}(\omega)} r_{l,n-1} + r_{e-1,n-1} & \text{if } j = 0, \end{cases}$$

$$= \begin{cases} \alpha_\epsilon r_{0,j-1} + \sum_{l=1}^{e-2} \alpha_{\bar{\xi}_{l-1}(\omega)} r_{l,j-1} + r_{e-1,j-1} & \text{if } j \neq 0,\\ (\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i - 1) r_{0,n-1} + \sum_{l=1}^{e-2} \alpha_{\bar{\xi}_{l-1}(\omega)} r_{l,n-1} & \\ \qquad + r_{e-1,n-1} & \text{if } j = 0 \text{ and } \xi_0(\epsilon) \neq 0,\\ (\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i + p - 1) r_{0,n-1} + \sum_{l=1}^{e-2} \alpha_{\bar{\xi}_{l-1}(\omega)} r_{l,n-1} & \\ \qquad + r_{e-1,n-1} & \text{if } j = 0 \text{ and } \xi_0(\epsilon) = 0. \end{cases}$$

For the other direction, by equation (5.1.5), we have

$$\Phi(\boldsymbol{r}) = (b_0, b_1, \ldots, b_{p^{m(e-1)}n-1}),$$

where $b_{(\omega p^m+\epsilon)n+j} = \alpha_\epsilon r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\bar{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j}$, for all $0 \le \omega \le p^{m(e-2)} - 1$, $0 \le \epsilon \le p^m - 1$ and $0 \le j \le n-1$.

Let $(c_0, c_1, \ldots, c_{p^{m(e-1)}n-1}) = \sigma^{\otimes p^{m(e-1)-1}} \circ \Phi(\boldsymbol{r})$. Then for each $0 \le \omega \le$

$p^{m(e-2)}-1,\ 0\le\epsilon\le p^m-1$ and $0\le j\le n-1$,

$$c_{(\omega p^m+\epsilon)n+j}=\begin{cases}\alpha_\epsilon r_{0,j-1}+\sum_{l=1}^{e-2}\alpha_{\overline{\xi}_{l-1}(\omega)}r_{l,j-1}+r_{e-1,j-1} & \text{if } j\neq 0,\\ (\sum_{i=0}^{m-1}\xi_i(\epsilon)\alpha^i-1)r_{0,n-1}+\sum_{l=1}^{e-2}\alpha_{\overline{\xi}_{l-1}(\omega)}r_{l,n-1} & \\ \qquad +r_{e-1,n-1} & \text{if } j=0 \text{ and } \xi_0(\epsilon)\neq 0,\\ (\sum_{i=0}^{m-1}\xi_i(\epsilon)\alpha^i+p-1)r_{0,n-1}+\sum_{l=1}^{e-2}\alpha_{\overline{\xi}_{l-1}(\omega)}r_{l,n-1} & \\ \qquad +r_{e-1,n-1} & \text{if } j=0 \text{ and } \xi_0(\epsilon)=0.\end{cases}$$

Hence, the result follows. □

Theorem 5.2.2. *Let C be a linear code of length n over $\mathcal{R}_{(p^m,e)}$. Then $\mathcal{C}$ is a $(1-u^{e-1})$-constacyclic code if and only if $\Phi(C)$ is a quasi-cyclic code of index $p^{m(e-1)-1}$ and length $p^{m(e-1)}n$ over $\mathbb{F}_{p^m}$. In this case, $\Phi(C)$ is a distance invariant quasi-cyclic code.*

Proof. The necessary part follows from Theorem 5.2.1, that is

$$\sigma^{\otimes p^{m(e-1)-1}}\circ\Phi(C)=\Phi\circ\rho_{1-u^{e-1}}(C)=\Phi(C).$$

For the sufficient part, assume that $\Phi(C)$ is quasi-cyclic. Then

$$\Phi(C)=\sigma^{\otimes p^{m(e-1)-1}}\circ\Phi(C)=\Phi\circ\rho_{1-u^{e-1}}(C).$$

The injectivity of Φ implies $\rho_{1-u^{e-1}}(C)=C$, that is C is $(1-u^{e-1})$-constacyclic.

In addition, $\Phi(C)$ is distant invariant by Theorem 5.1.2. □

Example 5.2.3. From Example 5.1.3, it is easy to see that the code C is a $(1-u)$-constacyclic code over $\mathcal{R}_{(3,2)}$ with $d_{hom}(C)=8$. Hence, its Gray image $\Phi(C)$ is a quasi-cyclic code of index 1, i.e., it is a cyclic code over $\mathbb{F}_3$ with $d_{Ham}(\Phi(C))=8=d_{hom}(C)$.

5.3 Gray Images of Cyclic and $(1+u^{e-1})$-Constacyclic Codes

Throughout this section, we assume that p does not divide the length n of codes. Then $\gcd(n,p)=1$, and hence there exists $n' \in \{0,1,\ldots,p-1\}$ such that $nn' \equiv 1 (\mathrm{mod}\ p)$. Let $\beta = 1+n'u^{e-1}$. Then $\beta^j = (1+n'u^{e-1})^j = 1+jn'u^{e-1} \in R$, for all $j \in \mathbb{Z}$. In particular, $\beta^n = 1+u^{e-1}$ and $\beta^{-n} = 1-u^{e-1}$.

Let $\mu : {\mathcal{R}_{(p^m,e)}}^n \to {\mathcal{R}_{(p^m,e)}}^n$ be defined by

$$(r_0, r_1, \ldots, r_{n-1}) \mapsto (r_0, \beta r_1, \ldots, \beta^{n-1} r_{n-1}). \tag{5.3.1}$$

Then both μ and $\mu^2 = \mu \circ \mu$ are $\mathcal{R}_{(p^m,e)}$-module automorphisms on ${\mathcal{R}_{(p^m,e)}}^n$.

Proposition 5.3.1. *Let C be a non-empty subset of ${\mathcal{R}_{(p^m,e)}}^n$. Then C is a linear cyclic code if and only if $\mu(C)$ is a linear $(1-u^{e-1})$-constacyclic code.*

Proof. Assume that C is a linear cyclic code. Let $(r_0, \beta r_1, \ldots, \beta^{n-1} r_{n-1}) \in \mu(C)$. Since μ is injective, $(r_0, r_1, \ldots, r_{n-1}) \in C$. By the linearity and cyclicity of C, we have $\beta^{-1}(r_{n-1}, r_0, r_1, \ldots, r_{n-1}) \in C$. Thus,

$$\begin{aligned}
&\rho_{1-u^{e-1}}((r_0, \beta r_1, \ldots, \beta^{n-1} r_{n-1})) \\
&\qquad = ((1-u^{e-1})\beta^{n-1} r_{n-1}, r_0, \beta r_1, \ldots, \beta^{n-2} r_{n-2}) \\
&\qquad = (\beta^{-n}\beta^{n-1} r_{n-1}, r_0, \beta r_1, \ldots, \beta^{n-2} r_{n-2}) \\
&\qquad = ((\beta^{-1} r_{n-1}), \beta(\beta^{-1} r_0), \beta^2(\beta^{-1} r_1), \ldots, \beta^{n-1}(\beta^{-1} r_{n-1})) \\
&\qquad = \mu((\beta^{-1} r_{n-1}, \beta^{-1} r_0, \beta^{-1} r_1, \ldots, \beta^{-1} r_{n-1})) \\
&\qquad = \mu(\beta^{-1}(r_{n-1}, r_0, r_1, \ldots, r_{n-1})) \in \mu(C)
\end{aligned}$$

since $\beta^{-1}(r_{n-1}, r_0, r_1, \ldots, r_{n-1}) \in C$. Hence, $\mu(C)$ is $(1-u^{e-1})$-constacyclic as desired.

For the other direction, assume that $\mu(C)$ is a linear $(1-u^{e-1})$-constacyclic code. Let $(r_0, r_1, \ldots, r_{n-1}) \in C$. Then $(r_0, \beta r_1, \ldots, \beta^{n-1} r_{n-1}) \in \mu(C)$. By linear-

ity and $(1-u^{e-1})$-constacyclicity of $\mu(C)$, we have

$$\beta((1-u^{e-1})\beta^{n-1}r_{n-1}, r_0, \beta r_1, \ldots, \beta^{n-2}r_{n-2}) \in \mu(C).$$

Since μ is bijective, we have

$$\begin{aligned}\rho((r_0, r_1, \ldots, r_{n-1})) &= (r_{n-1}, r_0, r_1, \ldots, r_{n-2}) \\ &= \mu^{-1}((r_{n-1}, \beta r_0, \beta^2 r_1, \ldots, \beta^{n-1}r_{n-2})) \\ &= \mu^{-1}((\beta^{-n}\beta^n r_{n-1}, \beta r_0, \beta^2 r_1, \ldots, \beta^{n-1}r_{n-2})) \\ &= \mu^{-1}(\beta((1-u^{e-1})\beta^{n-1}r_{n-1}, r_0, \beta r_1, \ldots, \beta^{n-2}r_{n-2})) \in C\end{aligned}$$

since $\beta((1-u^{e-1})r_{n-1}, r_0, \beta r_1, \ldots, \beta^{n-2}r_{n-2}) \in \mu(C)$. Therefore, C is cyclic. □

Proposition 5.3.2. *Let C be a non-empty subset of $\mathcal{R}_{(p^m,e)}{}^n$. Then C is a linear $(1+u^{e-1})$-constacyclic code if and only if $\mu^2(C)$ is a linear $(1-u^{e-1})$-constacyclic code.*

Proof. Assume that C is a linear $(1+u^{e-1})$-constacyclic code. To prove that $\mu^2(C)$ is $(1-u^{e-1})$-constacyclic, let $(r_0, \beta^2 r_1, \ldots, \beta^{2(n-1)}r_{n-1}) \in \mu^2(C)$. Then $(r_0, r_1, \ldots, r_{n-1}) \in C$. From the linearity and $(1+u^{e-1})$-constacyclicity of C, it follows that $\beta^{-2}((1+u^{e-1})r_{n-1}, r_0, r_1, \ldots, r_{n-1}) \in C$. Thus,

$$\begin{aligned}&\rho_{1-u^{e-1}}((r_0, \beta^2 r_1, \ldots, \beta^{2(n-1)}r_{n-1})) \\ &\quad= ((1-u^{e-1})\beta^{2(n-1)}r_{n-1}, r_0, \beta^2 r_1, \ldots, \beta^{2(n-2)}r_{n-2}) \\ &\quad= (\beta^{-n}\beta^{2(n-1)}r_{n-1}, r_0, \beta^2 r_1, \ldots, \beta^{2(n-2)}r_{n-2}) \\ &\quad= (\beta^n(\beta^{-2}r_{n-1}), \beta^2(\beta^{-2}r_0), \beta^4(\beta^{-2}r_1), \ldots, \beta^{2(n-1)}(\beta^{-2}r_{n-1})) \\ &\quad= \mu^2((\beta^{-2}\beta^n r_{n-1}, \beta^{-2}r_0, \beta^{-2}r_1, \ldots, \beta^{-2}r_{n-1})) \\ &\quad= \mu^2(\beta^{-2}((1+u^{e-1})r_{n-1}, r_0, r_1, \ldots, r_{n-1})) \in \mu^2(C)\end{aligned}$$

since $\beta^{-2}((1+u^{e-1})r_{n-1}, r_0, r_1, \ldots, r_{n-1}) \in C$. Therefore, $\mu^2(C)$ is a $(1-u^{e-1})$-constacyclic code.

Conversely, assume that $\mu^2(C)$ is a linear $(1-u^{e-1})$-constacyclic code. Let $(r_0, r_1, \ldots, r_{n-1}) \in C$. Then $(r_0, \beta^2 r_1, \ldots, \beta^{2(n-1)} r_{n-1}) \in \mu^2(C)$. By linearity and $(1-u^{e-1})$-constacyclicity of $\mu^2(C)$, we have

$$\beta^2((1-u^{e-1})r_{n-1}, r_0, \beta^2 r_1, \ldots, \beta^{2(n-2)} r_{n-2}) \in \mu^2(C).$$

Since μ^2 is bijective, we have

$$\begin{aligned}
&\rho_{1+u^{e-1}}((r_0, r_1, \ldots, r_{n-1})) \\
&\qquad = ((1+u^{e-1})r_{n-1}, r_0, r_1, \ldots, r_{n-2}) \\
&\qquad = \mu^{-2}(((1+u^{e-1})r_{n-1}, \beta^2 r_0, \beta^4 r_1, \ldots, \beta^{2(n-1)} r_{n-2})) \\
&\qquad = \mu^{-2}((\beta^{-n}\beta^{2n} r_{n-1}, \beta^2 r_0, \beta^4 r_1, \ldots, \beta^{2(n-1)} r_{n-2})) \\
&\qquad = \mu^{-2}(\beta^2((1-u^{e-1})\beta^{2(n-1)} r_{n-1}, r_0, \beta^2 r_1, \ldots, \beta^{2(n-2)} r_{n-2})) \in C
\end{aligned}$$

since $\beta^2((1-u^{e-1})\beta^{2(n-1)} r_{n-1}, r_0, \beta^2 r_1, \ldots, \beta^{2(n-2)} r_{n-2}) \in \mu^2(C)$. Therefore, C is a $(1+u^{e-1})$-constacyclic code. □

The Nechaev permutation in [32] is extended to be the permutation τ on $\{0, 1, \ldots, pn-1\}$ defined by

$$\tau(sn+j) = (s+jn')_p n + j,$$

where $0 \le s \le p-1$, $0 \le j \le n-1$, and $(s+jn')_p$ is the least residue of $s+jn'$ modulo p. The permutation τ induces $\pi : \mathbb{F}_{p^m}^{pn} \to \mathbb{F}_{p^m}^{pn}$ as follows:

$$\pi((c_0, c_1, \ldots, c_{pn-1})) = (c_{\tau(0)}, c_{\tau(1)}, \ldots, c_{\tau(pn-1)}).$$

The map π is then extended to $\pi^{\otimes p^{m(e-1)-1}} : \mathbb{F}_{p^m}^{p^{m(e-1)}n} \to \mathbb{F}_{p^m}^{p^{m(e-1)}n}$ by

$$(a^{(0)} \mid a^{(1)} \mid \cdots \mid a^{(p^{m(e-1)-1}-1)}) \mapsto (\pi(a^{(0)}) \mid \pi(a^{(1)}) \mid \cdots \mid \pi(a^{(p^{m(e-1)-1}-1)})),$$

where $a^{(i)} \in \mathbb{F}_{p^m}^{pn}$, $\mid$ is a vector concatenation.

Proposition 5.3.3. $\Phi \circ \mu = \pi^{\otimes p^{m(e-1)-1}} \circ \Phi$.

Proof. First, we have $\mu(\boldsymbol{r}) = (r_0, \beta r_1, \ldots, \beta^{n-1} r_{n-1})$. Since $\beta^j = 1 + jn'u^{e-1} \in \mathcal{R}_{(p^m,e)}$,

$$\beta^j r_j = (r_{0,j} + ur_{1,j} + \cdots + u^{e-1}(jn'r_{0,j} + r_{e,j})).$$

Let $(d_0, d_1, \ldots, d_{p^{m(e-1)}-1}) = \Phi(\mu(\boldsymbol{r}))$. Then

$$\begin{aligned}
d_{(\omega p^m+\epsilon)n+j} &= \alpha_\epsilon r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + (jn'r_{0,j} + r_{e-1,j}) \\
&= (\alpha_\epsilon + jn')r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j} \\
&= \left((\xi_0(\epsilon) + \xi_1(\epsilon)\alpha + \cdots + \xi_{m-1}(\epsilon)\alpha^{m-1}) + jn'\right) r_{0,j} \\
&\qquad + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j} \\
&= \alpha_{(\xi_0(\epsilon)+jn')_p+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}} r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j} \\
&= b_{(\omega p^m+((\xi_0(\epsilon)+jn')_p+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+j}.
\end{aligned}$$

On the other hand, we have $\Phi(\boldsymbol{r}) = (b_0, b_1, \ldots, b_{p^{m(e-1)}n-1})$, where

$$b_{(\omega p^m+\epsilon)n+j} = \alpha_\epsilon r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j},$$

for all $0 \le \omega \le p^{m(e-2)} - 1$, $0 \le \epsilon \le p^m - 1$ and $0 \le j \le n-1$. Let $(c_0, c_1, \ldots, c_{p^{m(e-1)}n-1}) = \pi^{\otimes p^{m(e-1)-1}}(\Phi(\boldsymbol{r}))$. Then

$$\begin{aligned}
c_{(\omega p^m+\epsilon)n+j} &= c_{(\omega p^m+(\xi_0(\epsilon)+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+j} \\
&= c_{(\omega p^m+(\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+\xi_0(\epsilon)n+j} \\
&= b_{(\omega p^m+(\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+(\xi_0(\epsilon)+jn')_p n+j} \\
&= b_{(\omega p^m+((\xi_0(\epsilon)+jn')_p+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+j}.
\end{aligned}$$

This completes the proof. □

Next corollary follows immediately from Propositions 5.3.1, 5.3.3 and Theorem 5.2.1.

Corollary 5.3.4. *The Gray image of a linear cyclic code of length n over $\mathcal{R}_{(p^m,e)}$ is permutatively equivalent to a quasi-cyclic code of index $p^{m(e-1)-1}$ and length $p^{m(e-1)}n$ over $\mathbb{F}_{p^m}$.*

Finally, we establish the structure of the Gray image of a linear $(1+u^{e-1})$-constacyclic code.

Proposition 5.3.5. $\Phi \circ \mu^2 = \pi^{\otimes p^{m(e-1)-1}} \circ \pi^{\otimes p^{m(e-1)-1}} \circ \Phi$.

Proof. Observe that $\mu^2(\boldsymbol{r}) = (r_0, \beta^2 r_1, \ldots, \beta^{2(n-1)} r_{n-1})$. Since $\beta^{2j} = 1+2jn'u^{e-1}$,

$$\beta^{2j} r_j = (r_{0,j} + u r_{1,j} + \cdots + u^{e-1}(2jn' r_{0,j} + r_{e,j})).$$

Let $(s_0, s_1, \ldots, s_{p^{m(e-1)}-1}) = \Phi(\mu^2(\boldsymbol{r}))$. Then

$$\begin{aligned}
s_{(\omega p^m+\epsilon)n+j} &= \alpha_\epsilon r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + (2jn' r_{0,j} + r_{e-1,j}) \\
&= (\alpha_\epsilon + 2jn') r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j} \\
&= \left((\xi_0(\epsilon) + \xi_1(\epsilon)\alpha + \cdots + \xi_{m-1}(\epsilon)\alpha^{m-1}) + 2jn'\right) r_{0,j} \\
&\quad + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j} \\
&= \alpha_{(\xi_0(\epsilon)+2jn')_p + \xi_1(\epsilon)p + \cdots + \xi_{m-1}(\epsilon)p^{m-1}} r_{0,j} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j} + r_{e-1,j} \\
&= b_{(\omega p^m + ((\xi_0(\epsilon)+2jn')_p + \xi_1(\epsilon)p + \cdots + \xi_{m-1}(\epsilon)p^{m-1}))n+j}.
\end{aligned}$$

For the other direction, let $\Phi(\boldsymbol{r}) = (b_0, b_1, \ldots, b_{p^{m(e-1)}n-1})$. Then we conclude from the proof of Proposition 5.3.3 that

$$\pi^{\otimes p^{m(e-1)-1}}(\Phi(\boldsymbol{r})) = (c_0, c_1, \ldots, c_{p^{m(e-1)}n-1}),$$

where

$$c_{(\omega p^m+\epsilon)n+j} = b_{(\omega p^m+((\xi_0(\epsilon)+jn')_p+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+j}.$$

Hence,

$$\pi^{\otimes p^{m(e-1)-1}}(\pi^{\otimes p^{m(e-1)-1}}(\Phi(\boldsymbol{r}))) = (d_0, d_1, \ldots, d_{p^{m(e-1)}n-1}),$$

where

$$\begin{aligned}
d_{(\omega p^m+\epsilon)n+j} &= d_{(\omega p^m+(\xi_0(\epsilon)+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+j} \\
&= d_{(\omega p^m+(\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+\xi_0(\epsilon)n+j} \\
&= c_{(\omega p^m+(\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+(\xi_0(\epsilon)+jn')_p n+j} \\
&= c_{(\omega p^m+((\xi_0(\epsilon)+jn')_p+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+j} \\
&= b_{(\omega p^m+(\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+(\xi_0(\epsilon)+2jn')_p n+j} \\
&= b_{(\omega p^m+((\xi_0(\epsilon)+2jn')_p+\xi_1(\epsilon)p+\cdots+\xi_{m-1}(\epsilon)p^{m-1}))n+j}.
\end{aligned}$$

The desired result follows. □

A delineation of the Gray image of a linear $(1+u^{e-1})$-constacyclic code is given as a consequence of Propositions 5.3.2 and 5.3.5 and Theorem 5.2.1.

Corollary 5.3.6. *The Gray image of a linear $(1+u^{e-1})$-constacyclic code of length n over $\mathcal{R}_{(p^m,e)}$ is permutatively equivalent to a quasicyclic code of index $p^{m(e-1)-1}$ and length $p^{m(e-1)}n$ over $\mathbb{F}_{p^m}$.*

Remark 5.3.7. Form the previous classification of $(1-u^{e-1})$-constacyclic, cyclic and $(1+u^{e-1})$-constacyclic codes, we conclude some algebraic relations among those spaces:

$$\begin{array}{ccccccc}
\mathcal{R}_{(p^m,e)}{}^n & \xrightarrow{\mu} & \mathcal{R}_{(p^m,e)}{}^n & \xrightarrow{\mu} & \mathcal{R}_{(p^m,e)}{}^n & \xrightarrow{\rho_{1-u^{e-1}}} & \mathcal{R}_{(p^m,e)}{}^n \\
\downarrow\Phi & \circlearrowright & \downarrow\Phi & \circlearrowright & \downarrow\Phi & \circlearrowright & \downarrow\Phi \\
\mathbb{F}_{p^m}^{p^{m(e-1)}n} & \xrightarrow{\pi^{\otimes p^{m(e-1)-1}}} & \mathbb{F}_{p^m}^{p^{m(e-1)}n} & \xrightarrow{\pi^{\otimes p^{m(e-1)-1}}} & \mathbb{F}_{p^m}^{p^{m(e-1)}n} & \xrightarrow{\sigma^{\otimes p^{m(e-1)-1}}} & \mathbb{F}_{p^m}^{p^{m(e-1)}n}
\end{array}.$$

For an arbitrary n, it follows from Theorem 5.2.1 that the third diagram commutes. As a consequence of Theorem 5.2.1 and Propositions 5.3.3 and 5.3.5, all diagrams commute whenever $\gcd(n, p) = 1$.

5.4 Gray Images of Some Skew-Constacyclic Codes

In this section, we give general descriptions of results in Sections 5.2 and 5.3 using the prefix "skew"in a particular case where an automorphism Θ of $\mathcal{R}_{(p^m,e)}$ is defined by

$$\Theta((a_0 + ua_1 + \cdots + u^{e-1}a_{e-1})) = (\theta(a_0) + u\theta(a_1) + \cdots + u^{e-1}\theta(a_{e-1})),$$

where θ is an automorphism of $\mathbb{F}_{p^m}$, i.e., Θ is $\Theta_{\theta,1,1}$ in Proposition 2.1.3. It is clear that $\mathrm{ord}(\Theta) = \mathrm{ord}(\theta)$ and Θ fixes 1, $1 - u^{e-1}$ and $1 + u^{e-1}$.

Let n be a multiple of the order of Θ. We aim to determine the Gray image of Θ-$(1-u^{e-1})$-constacyclic, Θ-$(1+u^{e-1})$-constacyclic and Θ-cyclic codes of length n over $\mathcal{R}_{(p^m,e)}$. First, we observe that

$$\begin{aligned}\rho_{\Theta,1-u^{e-1}}(\boldsymbol{r}) = (&\theta(r_{0,n-1}) + u\theta(r_{1,n-1}) + \cdots + u^{e-1}(\theta(r_{e-1,n-1}) - \theta(r_{0,n-1})),\\ &\theta(r_{0,0}) + u\theta(r_{1,0}) + \cdots + u^{e-1}\theta(r_{e-1,0}), \ldots,\\ &\theta(r_{0,n-2}) + u\theta(r_{1,n-2}) + \cdots + u^{e-1}\theta(r_{e-1,n-2})).\end{aligned}$$

Hence, $\Phi \circ \rho_{\Theta,1-u^{e-1}}(\boldsymbol{r}) = (d_0, d_1, \ldots, d_{p^{m(e-1)}n-1})$, where

$$d_{(\omega p^m+\epsilon)n+j} = \begin{cases} \alpha_\epsilon \theta(r_{0,j-1}) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} \theta(r_{l,j-1}) + \theta(r_{e-1,j-1}) & \text{if } j \neq 0, \\ (\alpha_\epsilon - 1)\theta(r_{0,n-1}) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} \theta(r_{l,n-1}) + \theta(r_{e-1,n-1}) & \text{if } j = 0, \end{cases}$$

$$= \begin{cases} \alpha_\epsilon \theta(r_{0,j-1}) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} \theta(r_{l,j-1}) + \theta(r_{e-1,j-1}) & \text{if } j \neq 0, \\ (\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i - 1)\theta(r_{0,n-1}) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} \theta(r_{l,n-1}) & \\ \qquad + \theta(r_{e-1,n-1}) & \text{if } j = 0 \text{ and } \xi_0(\epsilon) \neq 0, \\ (\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i + p - 1)\theta(r_{0,n-1}) + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} \theta(r_{l,n-1}) & \\ \qquad + \theta(r_{e-1,n-1}) & \text{if } j = 0 \text{ and } \xi_0(\epsilon) = 0, \end{cases} \tag{5.4.1}$$

for all $0 \leq \omega \leq p^{m(e-2)} - 1$, $0 \leq \epsilon \leq p^m - 1$ and $0 \leq j \leq n-1$.

From the proof of Theorem 5.2.1, we have

$\sigma^{\otimes p^{m(e-1)-1}} \circ \Phi(\boldsymbol{r}) = (c_0, c_1, \ldots, c_{p^{m(e-1)}n-1})$, where

$$c_{(\omega p^m+\epsilon)n+j} = \begin{cases} \alpha_\epsilon r_{0,j-1} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,j-1} + r_{e-1,j-1} & \text{if } j \neq 0, \\ (\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i - 1) r_{0,n-1} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,n-1} & \\ \qquad + r_{e-1,n-1} & \text{if } j = 0 \text{ and } \xi_0(\epsilon) \neq 0, \\ (\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i + p - 1) r_{0,n-1} + \sum_{l=1}^{e-2} \alpha_{\overline{\xi}_{l-1}(\omega)} r_{l,n-1} & \\ \qquad + r_{e-1,n-1} & \text{if } j = 0 \text{ and } \xi_0(\epsilon) = 0, \end{cases}$$

for all $0 \leq \omega \leq p^{m(e-2)} - 1$, $0 \leq \epsilon \leq p^m - 1$ and $0 \leq j \leq n-1$.

Let ν be a permutation on $\{0, 1, \ldots, p^{m(e-1)}n - 1\}$ defined by

$$\nu((\omega p^m + \epsilon)n + j) = (\varpi p^m + \varepsilon)n + j$$

if $\theta(\alpha_\varepsilon) = \alpha_\epsilon$ and $\theta(\alpha_{\overline{\xi}_l(\varpi)}) = \alpha_{\overline{\xi}_l(\omega)}$, for all $1 \leq l \leq e-2$. The linear transformation $T_\nu : \mathbb{F}_{p^m}^{p^{m(e-1)}n} \to \mathbb{F}_{p^m}^{p^{m(e-1)}n}$ induced by ν is given by

$$T_\nu((a_0, a_1, \ldots, a_{p^{m(e-1)}n-1})) = (a_{\nu(0)}, a_{\nu(1)}, \ldots, a_{\nu(p^{m(e-1)}n-1)}).$$

Then $T_\nu \circ \sigma^{\otimes p^{m(e-1)-1}} \circ \Phi(\boldsymbol{r}) = (f_0, f_1, \ldots, f_{p^{m(e-1)}n-1})$, where

$$f_{(\omega p^m+\epsilon)n+j} = \begin{cases} \theta^{-1}(\alpha_\epsilon) r_{0,j-1} + \sum_{l=1}^{e-2} \theta^{-1}(\alpha_{\overline{\xi}_{l-1}(\omega)}) r_{l,j-1} + r_{e-1,j-1} & \text{if } j \neq 0, \\ \theta^{-1}(\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i - 1) r_{0,n-1} + \sum_{l=1}^{e-2} \theta^{-1}(\alpha_{\overline{\xi}_{l-1}(\omega)}) r_{l,n-1} & \\ \qquad + r_{e-1,n-1} & \text{if } j = 0 \text{ and } \xi_0(\epsilon) \neq 0, \\ \theta^{-1}(\sum_{i=0}^{m-1} \xi_i(\epsilon)\alpha^i + p - 1) r_{0,n-1} + \sum_{l=1}^{e-2} \theta^{-1}(\alpha_{\overline{\xi}_{l-1}(\omega)}) r_{l,n-1} & \\ \qquad + r_{e-1,n-1} & \text{if } j = 0 \text{ and } \xi_0(\epsilon) = 0, \end{cases} \tag{5.4.2}$$

for all $0 \leq \omega \leq p^{m(e-2)} - 1$, $0 \leq \epsilon \leq p^m - 1$ and $0 \leq j \leq n-1$.

It follows from (5.4.1) and the result after applying θ on both sides of (5.4.2) that $T_\nu \circ \sigma^{\otimes p^{m(e-1)-1}} \circ \Phi = \Phi \circ \rho_{\Theta, 1-u^{e-1}}$.

Let ν_σ be the permutation on $\{0, 1, \ldots, p^{m(e-1)}n-1\}$ induced by $T_\nu \circ \sigma^{\otimes p^{m(e-1)-1}}$. Hence, the next theorem follows.

Theorem 5.4.1. *Let C be a linear code of length n over $\mathcal{R}_{(p^m,e)}$. Then C is a Θ-$(1-u^{e-1})$-constacyclic code if and only if $\Phi(C)$ is a θ-ν_σ-invariant code of length $p^{m(e-1)}n$ over $\mathbb{F}_{p^m}$.*

Next, we assume that $\gcd(n, p) = 1$ and $n' \in \{1, 2, \ldots, p-1\}$ such that $nn' \equiv 1 (\mod p)$. Note that $\beta = 1 + n'u^{e-1}$ is fixed by Θ. Using μ defined in (5.3.1) and arguments similar to those in Propositions 5.3.1 and 5.3.2, we conclude the the following results.

Proposition 5.4.2. *Let C be a non-empty subset of ${\mathcal{R}_{(p^m,e)}}^n$. Then C is a linear Θ-cyclic code if and only if $\mu(C)$ is a linear Θ-$(1-u^{e-1})$-constacyclic code.*

Corollary 5.4.3. *The Gray image of a linear Θ-cyclic code of length n over $\mathcal{R}_{(p^m,e)}$ is permutatively equivalent to a θ-ν_σ-invariant code of length $p^{m(e-1)}n$ over $\mathbb{F}_{p^m}$.*

Proposition 5.4.4. *Let C be a non-empty subset of ${\mathcal{R}_{(p^m,e)}}^n$. Then C is a linear Θ-$(1+u^{e-1})$-constacyclic code if and only if $\mu^2(C)$ is a linear Θ-$(1-u^{e-1})$-constacyclic code.*

Corollary 5.4.5. *The Gray image of a linear Θ-$(1+u^{e-1})$-constacyclic code of length n over $\mathcal{R}_{(p^m,e)}$ is permutatively equivalent to a θ-ν_σ-invariant code of length $p^{m(e-1)}n$ over $\mathbb{F}_{p^m}$.*

REFERENCES

[1] Alkhamees, Y.: The group of automorphisms of finite chain rings, *Arab Gulf Journal of Scientific Research* **8**, 17–28(1990).

[2] Alkhamees, Y.: The determination of the group of automorphisms of a finite chain ring of characteristic p, *The Quarterly Journal of Mathematics* **42**, 387–391(1991).

[3] Amarra, M. C. V., Nemenzo, F. R.: On $(1-u)$-cyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, *Applied Mathematics Letters* **21**, 1129–1133(2008).

[4] Bachoc, C.: Application of coding theory to the construction of modular lattices, *Journal of Combinatorial Theory Series A* **78**, 92–119(1997).

[5] Bini, G., Flamini, F.: *Finite Commutative Rings and Their Applications*, Kluwer Academic Publishers, Massachusetts, 2002.

[6] Bonnecaze, A., Udaya, P., Cyclic codes and self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$, *IEEE Transactions on Information Theory* **45**, 1250–1255(1999).

[7] Boucher, D., Geiselmann, W., Ulmer, F.: Skew-cyclic codes, *Applicable Algebra in Engineering, Communication and Computing* **18**, 379–389 (2007).

[8] Boucher, D., Solé, P., Ulmer, F.: Skew constacyclic codes over Galois rings, *Advances in Mathematics of Communications* **2**, 273–292(2008).

[9] Boucher, D., Ulmer, F.: Codes as modules over skew polynomial rings, *Lecture Notes in Computer Science* **5921**, 38–55(2009).

[10] Boucher, D., Ulmer, F.: Coding with skew polynomial rings, *Journal of Symbolic Computation* **44**, 1644–1656(2009).

[11] Cengellenmis, Y. : On $(1-u^m)$-cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2+\ldots +u^m\mathbb{F}_2$, *International Journal of Contempolary Mathematical Sciences* **4**, 987–992(2009).

[12] Clark, W. E., Drake, D. A.: Finite chain rings, *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* **39**, 147–153(1973).

[13] Clark, W. E., Liang, J. J.: Enumeration of finite commutative chain rings, *Journal of Algebra* **27**, 445–453(1973).

[14] Dinh, H. Q.: Negacyclic codes of length 2^s over Galois rings, *IEEE Transactions on Information Theory* **51**, 4252–4262(2005).

[15] Dinh, H. Q.: Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2+u\mathbb{F}_2$, *IEEE Transactions on Information Theory* **55**, 1730–1740 (2009).

[16] Dinh, H. Q.: Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Journal of Algebra* **324**, 940–950(2010).

[17] Dinh, H. Q., López-Permouth, S. R.: Cyclic and negacyclic codes over finite chain rings, *IEEE Transactions on Information Theory* **50**, 1728–1744 (2004).

[18] Dougherty, S. T., Ling, S.: Cyclic codes over $\mathbb{Z}_4$ of even length, *Designs, Codes and Cryptography* **39** 127–153(2006).

[19] Greferath, M., Schmidt, S. E.: Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, *IEEE Transactions on Information Theory* **45**, 2522-2624(1999).

[20] Greferath, M., Schmidt, S. E.: Finite-ring combinatorics and MacWilliams' equivalence Theorem, *Journal of Combinatorial Theory, Series A* **92**, 17–28(2000).

[21] Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Transactions on Information Theory* **40**, 301–319 (1994).

[22] Huffman, W. C., Pless, V.: *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[23] Kai, X., Zhu, S., Li, P.: $(1-\lambda u)$-constacyclic codes over $\mathbb{F}_p[u]/\langle u^m\rangle$, *Journal of the Franklin Institute* **347**, 751–762(2010).

[24] Lacan, E., Delpeyroux, E.: The q-ary images of some q^m-ary cyclic codes: permutation group and soft-decision decoding, *IEEE Transactions on Information Theory* **48**, 2069–2078(2002).

[25] Ling, S., Blackford, J. T.: $\mathbb{Z}_{p^{k+1}}$-linear codes, *IEEE Transactions on Information Theory* **48**, 2592–2605(2002).

[26] Ling, S., Xing, C.: *Coding Theory : A First Course*, Cambridge University Press, 2004.

[27] MacWilliams, F. J., Sloan, N. J. A.: *The Theory of Error-Correcting Codes*, New York : Elsevier/North Halland, 1977.

[28] McDonald, B. R. *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[29] Norton, G. H., Sălăgean, A.: On the structure of linear and cyclic codes over a finite chain ring, *Applicable Algebra in Engineering, Communication and Computing* **10**, 489–506(2000).

[30] Qian, J. F., Zhang, L. N., Zhu, S. X.: $(1 + u)$-cyclic and cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, *Applied Mathematics Letters* **19**, 820–823(2006).

[31] Qian, J. F., Zhang, L. N., Zhu, S. X.: Constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E89-A**, 1863-1865(2006).

[32] Qian, J. F., Ma, W., Wang, X.: On the Gray image of cyclic codes over finite chain rings, *IEICE Transactions on Electronics* **EA91-A**, 2685–2687 (2008).

[33] Ribenboim, P.: Sur la localisation des anneaux non commutatifs (French), *Séminaire Dubreil. Algèbre et théorie des nombres* **24**, 1970/71.

[34] Sobhani, R., Esmaeili, M.: A note on cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k, *Finite Fields and Their Applications* **15**, 387–391(2009).

[35] Sobhani, R., Esmaeili, M.: Cyclic and negacyclic codes over the Galois ring $\mathrm{GR}(p^2, m)$, *Discrete Applied Mathematics* **157**, 2892–2903(2009).

[36] Udaya, P., Siddiqi, M. U.: Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings, *IEEE Transactions on Information Theory* **44**, 1492–1503(1998).

[37] Wan, Z.-X.: *Lectures on Finite Fields and Galois Rings*, World Scientific, New Jersey, 2003.

VITA

Mr. Somphong Jitman was born on May 30, 1982 in Nakhon Si Thammarat, Thailand. He has been in the Development and Promotion of Science and Technology Talents Project (DPST) under the support of the Institute for the Promotion of Teaching Science and Technology (IPST) since 2000. He got a Bachelor of Science in Mathematics with first class honors from Prince of Songkla University in 2005. After that he took his master program in Mathematics at Chulalongkorn University and finished the degree in 2007. Subsequently, he started his Doctoral degree at Chulalongkorn University. In the last two years of his Ph.D. program, he got a special support from the IPST and the great opportunity from School of Physical and Mathematical Sciences, Nanyang Technological University to join the Coding and Cryptography Research Group (CCRG) in this school.