Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 3965789, 17 pages
http://dx.doi.org/10.1155/2016/3965789

Review Article

Skew Constacyclic Codes over Finite Fields and Finite Chain Rings

Hai Q. Dinh,[1] Bac T. Nguyen,[2,3] and Songsak Sriboonchitta[4]

[1]*Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA*
[2]*Department of Mathematics, Faculty of Science, Mahidol University, Bangkok 10400, Thailand*
[3]*Department of Basic Science, University of Economics and Business Administration, Thai Nguyen University, Thai Nguyen Province, Vietnam*
[4]*Faculty of Economics, Chiang Mai University, Chiang Mai, Thailand*

Correspondence should be addressed to Hai Q. Dinh; hdinh@kent.edu

Received 5 August 2015; Revised 13 November 2015; Accepted 2 December 2015

Academic Editor: Haipeng Peng

This paper overviews the study of skew Θ-λ-constacyclic codes over finite fields and finite commutative chain rings. The structure of skew Θ-λ-constacyclic codes and their duals are provided. Among other results, we also consider the Euclidean and Hermitian dual codes of skew Θ-cyclic and skew Θ-negacyclic codes over finite chain rings in general and over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ in particular. Moreover, general decoding procedure for decoding skew BCH codes with designed distance and an algorithm for decoding skew BCH codes are discussed.

1. Introduction

Reliable communication has been an unavoidable problem for a long time. Before 1948, communication was strictly an engineering discipline. However, there was very little scientific to develop a system to understand it. In 1948, Shannon's[1] landmark paper "A Mathematical Theory of Communication" [1] on the mathematical theory of communication, which showed that good codes exist, gave birth to information theory and coding theory. Coding theory is applicable in many situations that involve a common feature that a sender wants to send a message to a receiver through a noisy-channel. When the receiver has a message, it might contain some errors. Therefore, rather than sending it directly, the sender will encode it and send it to a decoder that estimates the message to give the receiver. Figure 1 describes a communication channel that transmits information from a source to a destination through a system.

Shannon's noisy-channel coding theorem ensures that our hopes of getting the correct messages to the users will be fulfilled a certain percentage of the time. Based on the characteristics of the communication channel, it is possible to build the right encoders and decoders so that this percentage, although not 100%, can be made as high as we desire. However, the proof of Shannon's noisy-channel coding theorem is probabilistic and only guarantees the existence of such good codes. No specific codes were constructed in the proof that provides the desired accuracy for a given channel. The main goal of coding theory is to establish good codes that fulfill the assertions of Shannon's noisy-channel coding theorem. During the last 50 years, while many good codes have been constructed, but only from 1993, with the introduction of turbo codes[2], the rediscoveries of LDPC codes[3], and the study of related codes and associated iterative decoding algorithms, researchers started to see codes that approach the expectation of Shannon's noisy-channel coding theorem in practice.

In real life, the noise is unavoidable, so we want to *DETECT* if there is an error and *CORRECT* if there is one. In 1950, a colleague of Shannon, Hamming[4], developed a ground-breaking idea in his famous paper "Error Detecting and Error Correcting Codes" [2]. The ground-breaking idea in Hamming's paper describes a single error correcting code.[5] A simple extension of this code is also discovered by Hamming in [2]. For more details, we refer the readers to [2].

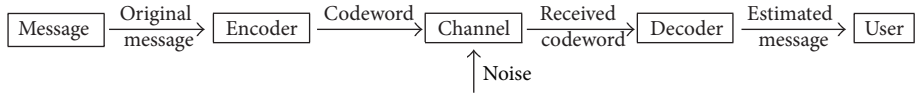

Figure 1

The classes of cyclic and negacyclic codes in particular, and constacyclic codes in general, play a very significant role in the theory of error correcting codes. All λ-constacyclic codes of length n are classified as ideals $\langle f(x)\rangle$ of $\mathbb{F}[x]/\langle x^n - \lambda\rangle$, where $f(x)$ is a divisor of $x^n - \lambda$. Due to their rich algebraic structure, constacyclic codes can be efficiently encoded using shift registers, which explains their preferred role in engineering.

In fact, cyclic codes are the most studied of all codes. Many well-known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes. Cyclic codes over finite fields were first studied in the late 1950s by Prange [4–7], while negacyclic codes over finite fields were initiated by Berlekamp in the late 1960s [8, 9]. The case when the code length n is divisible by the characteristic p of the field yields the so-called repeated-root codes, which were first studied since 1967 by Berman [10] and then in the 1970s and 1980s by several authors such as Massey et al. [11], Falkner et al. [12], Roth and Seroussi [13], Castagnoli et al. [14], and van Lint [15].

In 2007, Boucher et al. initiated [3] the study of skew cyclic codes. They generalized the notion of cyclic codes by using generator polynomials in noncommutative skew polynomial rings. In 2008 and 2011, Boucher and Ulmer [16, 17] continued to study skew Θ-λ-constacyclic codes over Galois rings and codes as modules over skew polynomial rings.

In [16], Boucher et al. generalized the construction of linear codes via skew polynomial rings by using Galois rings instead of finite fields as coefficients. If finite fields are replaced by Galois rings, then the technical difficulty in studying from finite fields alphabet to Galois rings alphabet is that the skew polynomial rings are not Ore rings. They are neither left nor right Euclidean rings. However, left and right divisor can be defined for some suitable elements. Therefore, in [16], self-dual codes over $\mathrm{GR}(4^2)$ are constructed and used for three applications: self-dual Euclidean codes give self-dual $\mathbb{Z}_4$ codes by projection on a trace orthogonal basis, self-dual Hermitian codes build 3-modular lattices, and self-dual Hermitian codes yield self-dual quasi-cyclic codes over $\mathbb{Z}_4$ by the cubic construction. For more details, we refer the readers to [16] and the references therein. Boucher and Ulmer also studied the factorization of skew polynomial in skew polynomial rings [18]. These results allowed them to study the skew self-dual cyclic codes with length 2^s.

The class of finite rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ has been widely used as alphabets of certain constacyclic codes. For example, the structure of $\mathbb{F}_2 + u\mathbb{F}_2$ is interesting; it is lying between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$ and multiplicatively analogous to $\mathbb{Z}_4$. It has been studied by a lot of researchers (see, e.g., [19–24]). The classification of codes plays an important role in studying their structures, but, in general, it is very difficult. Only some codes of certain lengths over certain finite fields or finite chain rings are classified. All constacyclic codes of length 2^s over the Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$ are classified and their detailed structures are also established in [25].

In 2012, Jitman et al. [26] introduced the notion of skew Θ-λ-constacyclic (or skew constacyclic) codes over finite chain rings. They studied the structure of skew Θ-λ-constacyclic, the Euclidean, and Hermitian dual codes of skew Θ-cyclic and negacyclic codes over finite chain rings. The goal of this survey is to study skew Θ-λ-constacyclic codes over finite fields and finite chain rings.

This paper is arranged as follows. Basic concepts are reviewed in Section 2. After presenting preliminary concepts in Section 2, we study skew Θ-negacyclic, cyclic, and Θ-λ-constacyclic codes over finite fields in Section 3. We also introduce some results for Euclidean and Hermitian self-dual codes over finite fields. In Section 4, general decoding procedure for decoding skew BCH codes with designed distance is provided. We also discuss an algorithm for decoding skew BCH codes. Finally, in Section 5, we consider the structure of skew Θ-λ-constacyclic codes over finite chain rings. The Euclidean and Hermitian dual codes over finite chain rings are also exhibited in this section.

2. Preliminaries

2.1. Finite Fields and Their Automorphisms. In this subsection, we will not give entire properties of finite fields and their automorphisms; rather we will only introduce without proofs some properties of finite fields and their automorphisms that are needed in our consideration later.

Definition 1. Let $\mathbb{F}$ be a finite field with multiplicative identity 1. The characteristic of $\mathbb{F}$ is the least positive integer p such that $p \cdot 1 = 0$. Such p always exists for a finite field and it is well known that the characteristic p must be a prime.

Theorem 2. *A finite field $\mathbb{F}$ of characteristic p contains p^n elements for some integer $n \geq 1$. For every element β of a finite field $\mathbb{F}$ with p^m elements, we have $\beta^{p^m} = \beta$.*

Definition 3. An element α in a finite field $\mathbb{F}_{p^m}$ is called a *primitive element* (or generator) of $\mathbb{F}_{p^m}$ if $\mathbb{F}_{p^m} = \{0, \alpha, \alpha^2, \ldots, \alpha^{p^m-1}\}$.

Example 4. $\mathbb{F}_5$ has 2 primitive elements, namely, 2 and 3. $\mathbb{F}_4$ has 2 primitive elements. In fact, expressing $\mathbb{F}_4$ as $\mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$, where $\alpha^2 + \alpha + 1 = 0$, then α and $\alpha + 1$ are primitive elements of $\mathbb{F}_4$.

Note that an automorphism φ of a field $\mathbb{F}$ is a bijection $\varphi : \mathbb{F} \to \mathbb{F}$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in \mathbb{F}$. Suppose that $\mathbb{F}_{p^m}$ is a finite field of characteristic $p > 0$, and then the map $\varphi_p : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is defined by $\varphi_p(x) = x^p$, the Frobenius automorphism of $\mathbb{F}_{p^m}$. Since $\mathbb{F}_{p^m}$ is a field of characteristic p, we have $\varphi_p(a+b) = (a+b)^p = a^p + b^p = \varphi_p(a) + \varphi_p(b)$. From $\varphi_p(ab) = (ab)^p = a^p \cdot b^p = \varphi_p(a)\varphi_p(b)$, we can see that φ_p is a field homomorphism. Similarly, the map $\varphi_{p^t} : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ defined by $\varphi_{p^t}(x) = x^{p^t}$ is also a field homomorphism. The set of automorphisms of $\mathbb{F}_{p^m}$ forms a group under composition which we denote as $\mathrm{Aut}(\mathbb{F}_{p^m})$. Next, we give the following theorem characterizing this group.

Theorem 5 (see [27, Theorem 3.6.1]). *(i) If $\mathbb{F}_{p^m}$ is a finite field, then $\mathrm{Aut}(\mathbb{F}_{p^m})$ is a cyclic group of order m and is generated by Frobenius automorphism φ_p.*

(ii) The prime subfield of $\mathbb{F}_{p^m}$ is precisely the set of elements in $\mathbb{F}_{p^m}$ such that $\varphi_p(\alpha) = \alpha$.

(iii) The subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^t}$ is precisely the set of elements in $\mathbb{F}_{q^t}$ such that $\varphi_p(\alpha) = \alpha$, where $q = p^m$.

Theorem 6 (see [27, Theorem 3.6.2]). *If $\mathbb{F}_1 = \mathbb{F}_{p^k} \subset \mathbb{F}_2 = \mathbb{F}_{p^n}$, then $\mathrm{Aut}(\mathbb{F}_2/\mathbb{F}_1)$ is a cyclic group of order n/k and is generated by φ_{p^k}.*

2.2. Codes, Cyclic Codes, Generator, and Parity-Check Matrices. Let $\mathbb{F}_{p^m}$ be a finite field. A linear (n,k)-code over $\mathbb{F}_{p^m}$ is a k-dimensional vector subspace $\mathscr{C}$ of the vector space

$$V = \mathbb{F}_{p^m}^n = \left\{ (a_0, \ldots, a_{n-1}) \mid a_i \in \mathbb{F}_{p^m} \right\}. \tag{1}$$

In this paper, all codes are assumed to be linear codes unless otherwise stated. We use polynomial representation of the code C, where we identify codewords $(a_0, \ldots, a_{n-1}) \in C$ with coefficient tuples of polynomials:

$$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_{p^m}[x]. \tag{2}$$

Those polynomials can also be seen as elements of a quotient ring $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$, and any code C of length n over $\mathbb{F}_{p^m}$ corresponds to a subset of $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$.

Example 7. The polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ of degree at most $n-1$ over finite field $\mathbb{F}_{p^m}$ may be regarded as the word $v = a_0 a_1 a_2 \cdots a_{n-1}$ of length n in $\mathbb{F}_{p^m}^n$. If $n = 6$, then the polynomial $1 + x + x^2 + x^3 + x^5$ may be regarded as the word $c = 111101$. Similarly, the polynomial $1 + x^3 + x^4 + x^5$ may be regarded as the word $v = 100111$.

Definition 8. Let c be a word of length n, and the cyclic shift $\tau(c)$ the word of length n:

$$\tau(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2}). \tag{3}$$

A code C is said to be cyclic if $\tau(c) \in C$, for all $c \in C$.

Example 9. Let $C = \{000, 111, 121, 222, 012, 120, 201, 021, 102, 210\}$ be a linear code over $\mathbb{Z}_3$. It is easy to see that $\tau(c) \in C$, $\forall c \in C$. This implies that C is a linear cyclic code over $\mathbb{Z}_3$.

Let $C_1 = \{021, 012, 000, 112, 121, 100, 212, 221, 200\}$ be a linear code over $\mathbb{Z}_3$. Since $\tau(112) = 211 \notin C_1$, we can conclude that C_1 is not cyclic code.

Definition 10. A code C is said to be a *λ-constacyclic code* of length n if it is closed under the λ-constacyclic shift $\tau_\lambda : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}^n$ defined by

$$\tau_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2}). \tag{4}$$

In particular, when $\lambda = 1$ or $\lambda = -1$, such codes are called *cyclic* and *negacyclic codes*, respectively.

We now give some properties of cyclic code. The following results are well known (cf. [27]).

Theorem 11 (see [27, Theorem 4.2.1]). *Let C be a nonzero cyclic code in $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$. There exists a polynomial $g(x) \in C$ with the following properties:*

(i) *$g(x)$ is the unique monic polynomial of minimum degree in C, and it is called the generating polynomial for C.*

(ii) *$C = \langle g(x)\rangle$.*

(iii) *The generating polynomial $g(x)$ divides $x^n - 1$.*

(iv) *If $\deg g(x) = r$, then C has dimension $n - r$ and $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ is a basis for C.*

(v) *Every element of C is uniquely expressible as a product $f(x)g(x)$, where $f(x) = 0$ or $\deg f(x) < n - r$, that is, $C = \langle g(x)\rangle = \{f(x)g(x) \mid \deg f(x) < n - r\}$.*

(vi) *If $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, then $g_0 \neq 0$ and C has the following generator matrix:*

$$G := \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_r & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{pmatrix} \tag{5}$$

$$\Longleftrightarrow \begin{pmatrix} g(x) & & & \\ & xg(x) & & \\ & & \ddots & \\ & & & x^{n-r-1}g(x) \end{pmatrix}.$$

From this theorem, we can see that C is a nonzero cyclic code in $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ and $g(x)$ is the monic polynomial of minimum degree in C if and only if $C = \langle g(x)\rangle$, and $x^n - 1$ is divisible by $g(x)$.

Let C be a cyclic code in $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ with generator polynomial $g(x)$, such that $\deg g(x) = r$. Let

$h(x) = (x^n - 1)/g(x) = \sum_{i=0}^{n-r} h_i x^i$. Then a parity-check matrix for C is given by

$$H \coloneqq \begin{pmatrix} h_{n-r} & \cdots & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ \cdots & 0 & h_{n-r} & \cdots & \cdots & \cdots & h_0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \cdots & h_{n-r} & \cdots & \cdots & h_0 \end{pmatrix}. \quad (6)$$

Example 12. Let C be a cyclic code of length $n = 9$ over the binary field $\mathbb{F}_2$. Put $g(x) = x^6 + x^3 + 1$. Then we have $h(x) = x^3 - 1$. We can see that C has dimension 3 and generating matrix is given by

$$G \coloneqq \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \quad (7)$$

Hence, a parity-check matrix for C is given by

$$H \coloneqq \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \quad (8)$$

Definition 13. (i) The Hamming distance $d_H(x, y)$ between two vectors $x, y \in \mathbb{F}_{p^m}^n$ is defined to be the number of coordinates in which x and y differ.

(ii) The Hamming weight $w_H(x)$ of a vector $x \in \mathbb{F}_{p^m}^n$ is the number of nonzero coordinates in x.

(iii) For a code C containing at least two words, the minimum distance of a code C, denoted by $d(C)$, is

$$d(C) = \min\{d(x, y), x, y \in C, x \neq y\}. \quad (9)$$

It is easy to see that the definition of distance satisfies nonnegativity, symmetry, and the triangle inequality, so our code C is living in a metric space.

Example 14. Let $C = \{00000, 00111, 11111\}$ be a binary code. Then we have

$$d_H(00000, 00111) = 3; \quad w_H(00111) = 3. \quad (10)$$

We can see that

$$d(00000, 00111) = 3; \quad d(00111, 11111) = 2; \quad d(00000, 11111) = 5. \quad (11)$$

This shows that $d(C) = 2$.

The following theorem gives a relationship between minimum distance d and the minimum weight of the nonzero codewords of a linear code C.

Theorem 15 (see [27, Theorem 1.4.2]). *If $x, y \in \mathbb{F}_{p^m}^n$, then $d(x, y) = wt(x, y)$. If C is a linear code, the minimum distance d is the same as the minimum weight of the nonzero codewords of C.*

2.3. The Skew Polynomial Ring $\mathbb{F}_{p^m}[x; \Theta]$. Now let Θ be an automorphism of $\mathbb{F}_{p^m}$. We consider the set $\mathbb{F}_{p^m}[x; \Theta] = \{a_0 + a_1 x + \cdots + a_{n-1}x^n \mid a_i \in \mathbb{F}_{p^m}, n \in \mathbb{N}\}$ of formal polynomials where coefficients are written on the left of the variable x. The set $\mathbb{F}_{p^m}[x; \Theta]$ forms a ring under the usual addition of polynomials and the multiplication is defined by the following basic rule: $xa = \Theta(a)x$. The multiplication is extended to all elements in $\mathbb{F}_{p^m}[x; \Theta]$ by associativity and distributivity. The ring $\mathbb{F}_{p^m}[x; \Theta]$ is called a *skew polynomial ring* over $\mathbb{F}_{p^m}$, and each element in $\mathbb{F}_{p^m}[x; \Theta]$ is called a *skew polynomial*. It is easy to see that the ring $\mathbb{F}_{p^m}[x; \Theta]$ is noncommutative unless Θ is the identity automorphism on $\mathbb{F}_{p^m}$. If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$, then we say that $f(x)$ has degree n, denoted by $\deg(f(x))$. The following facts are straightforward for the skew polynomial ring $\mathbb{F}_{p^m}[x; \Theta]$:

(i) It has no nonzero zero-divisors,

(ii) the units of $\mathbb{F}_{p^m}[x; \Theta]$ are the units of $\mathbb{F}_{p^m}$,

(iii) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$,

(iv) $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Recall that a left (right) ideal I of a ring R is called a *left (right) principal ideal* if there exists an element $g \in I$ such that $I = \langle g \rangle$, where $\langle g \rangle = \{r \cdot g \ (g \cdot r) : r \in R\}$. The element g is called a *generator* of I and I is said to be generated by g. A ring R is called a *left (right) principal ideal ring* if every left (right) ideal of R is principal. The skew polynomial ring $\mathbb{F}_{p^m}[x; \Theta]$ is left and right Euclidean ring whose left and right ideals are principal. For $f(x), g(x) \in \mathbb{F}_{p^m}[x; \Theta]$ which are nonzero, there exists unique polynomial $h(x), r(x) \in \mathbb{F}_{p^m}[x; \Theta]$ such that $f(x) = h(x)g(x) + r(x)$. If $r(x) = 0$, then $g(x)$ is a right divisor of $f(x)$ in $\mathbb{F}_{p^m}[x; \Theta]$. The definition of left divisor in $\mathbb{F}_{p^m}[x; \Theta]$ is similar.

The centre $Z(\mathbb{F}_{p^m}[x; \Theta])$ of the skew polynomial ring $\mathbb{F}_{p^m}[x; \Theta]$ is the set of all elements that commute with all other elements of $\mathbb{F}_{p^m}[x; \Theta]$. An element $f \in Z(\mathbb{F}_{p^m}[x; \Theta])$ is called a *central element*. An automorphism $\Theta \in \mathrm{Aut}(\mathbb{F}_{p^m})$ is said to fix an element $\alpha \in \mathbb{F}_{p^m}$ if $\Theta(\alpha) = \alpha$. We denote $\mathbb{F}_{p^m}^{\Theta} \subset \mathbb{F}_{p^m}$ the subfield of elements of $\mathbb{F}_{p^m}$ which are fixed by Θ. Then the ring $\mathbb{F}_{p^m}^{\Theta}[x]$ is a commutative subring of $\mathbb{F}_{p^m}[x; \Theta]$. A polynomial $f \in \mathbb{F}_{p^m}[x; \Theta]$ is central element if and only if f is both in $\mathbb{F}_{p^m}^{\Theta}$ and in $\mathbb{F}_{p^m}[x^m]$, where $\mathbb{F}_{p^m}[x^m] = \{a_0 + a_1 x^m + \cdots + a_d x^{md}, \ d \in \mathbb{N}, \ a_i \in \mathbb{F}_{p^m}\}$. In other words, a polynomial $P \in \mathbb{F}_{p^m}[x; \Theta]$ is central element (i.e., commutes with all elements of $\mathbb{F}_{p^m}[x; \Theta]$) if and only if $P = \sum_{i=0}^{m} c_i X^{i\alpha} \in \mathbb{F}_{p^m}[x; \Theta]$, where $\alpha = |\langle \Theta \rangle|$ is the order of Θ [28, Theorem II.12].

3. Structure and Duals of Skew Constacyclic Codes over Finite Fields

In this section, we study skew Θ-λ-constacyclic codes over finite fields. We extend the work of Boucher et al. (in 2007) [3] on skew cyclic codes. For more details, we refer the readers to [3] and the references therein. We first introduce the definition of skew Θ-λ-constacyclic codes over finite fields.

Definition 16. Given an automorphism Θ of $\mathbb{F}_{p^m}$ and a unit λ in $\mathbb{F}_{p^m}$, a code C is said to be *skew* Θ-λ-*constacyclic* of length n if it is closed under the skew Θ-λ-constacyclic shift $\tau_{\Theta,\lambda} : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}^n$ defined by

$$\begin{aligned}&\tau_{\Theta,\lambda}\left(c_0, c_1, \ldots, c_{n-1}\right)\\ &\quad = \left(\Theta\left(\lambda c_{n-1}\right), \Theta\left(c_0\right), \ldots, \Theta\left(c_{n-2}\right)\right).\end{aligned} \tag{12}$$

In particular, when $\lambda = 1$ or $\lambda = -1$, such codes are called *skew* Θ-*cyclic* and *skew* Θ-*negacyclic codes*, respectively. When Θ is the identity automorphism, they become classical constacyclic cyclic, cyclic, and negacyclic codes. A right factor of degree $n-k$ of $x^n - \lambda$ generates $[n,k]$ linear code. While the ring $\mathbb{F}_{p^m}[x]$ is a commutative ring, so every ideal in $\mathbb{F}_{p^m}[x]$ is two-sided ideal, the skew polynomial ring $\mathbb{F}_{p^m}[x;\Theta]$ is noncommutative. Therefore, we need to have conditions of Θ and λ to ensure that $\langle x^n - \lambda\rangle$ is a two-sided ideal of $\mathbb{F}_{p^m}[x;\Theta]$. If n is divisible by the order of Θ and λ is fixed by Θ, then $\langle x^n - \lambda\rangle$ is a two-sided ideal of $\mathbb{F}_{p^m}[x;\Theta]$. Indeed, for all $h(x) = \sum_{i=0}^{t} h_i x^i$ in $\mathbb{F}_{p^m}[x;\Theta]$, we can see that

$$\begin{aligned}\left(x^n - \lambda\right)\left(\sum_{i=0}^{t} h_i x^i\right) &= \Theta^n\left(h_0\right)x^n + \Theta^n\left(h_1\right)x^{n+1} + \cdots\\ &\quad + \Theta^n\left(h_t\right)x^{n+t} - \lambda\left(\sum_{i=0}^{t} h_i x^i\right).\end{aligned} \tag{13}$$

Since n is divisible by the order of Θ, we have $\Theta^n(h_i) = h_i, \forall i = \{1, \ldots, t\}$. If λ is fixed by Θ, then we have $(x^n - \lambda)(\sum_{i=0}^{t} h_i x^i) = (\sum_{i=0}^{t} h_i x^i)(x^n - \lambda)$, proving that $x^n - \lambda$ is in $Z(\mathbb{F}_{p^m}[x;\Theta])$. This implies that $\langle x^n - \lambda\rangle$ is a two-sided ideal of $\mathbb{F}_{p^m}[x;\Theta]$, which makes the quotient ring $\mathbb{F}_{p^m}[x;\Theta]/\langle x^n - \lambda\rangle$ well defined. If Θ is not the identity, then $\mathbb{F}_{p^m}[x;\Theta]$ is in general not a unique factorization ring. In this case, there are typically many more right factors than in the commutative case, producing many Θ-λ-constacyclic codes.

Example 17. Let α be a generator of the multiplicative group of $\mathbb{F}_4$; that is, α is a zero of $z^2 + z + 1 \in \mathbb{F}_2[z]$. Let Θ be the automorphism $a \mapsto a^2$ of $\mathbb{F}_4$. We consider the polynomial $x^6 + \alpha x^3 \in \mathbb{F}_4[x;\Theta]$. We have

$$\begin{aligned}x^6 + \alpha x^3 &= \left(x^4 + \alpha x\right)x^2 = \left(x^4 + \alpha x^3\right)\left(x^2 + \alpha x + 1\right)\\ &= \left(x^4 + \alpha x^3 + x^2\right)\left(x^2 + \alpha x\right).\end{aligned} \tag{14}$$

This shows that the ring $\mathbb{F}_4[x;\Theta]$ is not a unique factorization ring.

Lemma 1 in [3] can be extended as follows.

Lemma 18 (extending [3, Lemma 1]). *Let Θ be an automorphism of $\mathbb{F}_{p^m}$, n an integer divisible by the order of Θ, and λ a unit in $\mathbb{F}_{p^m}$ which is fixed by Θ. The ring $\mathbb{F}_{p^m}[x;\Theta]/\langle x^n - \lambda\rangle$ is a principal left ideal ring, in which the left ideals are generated by $g(x)$, where $g(x)$ is a right divisor of $x^n - \lambda$ in $\mathbb{F}_{p^m}[x;\Theta]$.*

Consider a codeword $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Then

$$\begin{aligned}xc\left(x\right) &= xc_0 + xc_1 x + \cdots + xc_{n-1}x^{n-1}\\ &= \Theta\left(c_0\right)x + \Theta\left(c_1\right)x^2 + \cdots + \Theta\left(c_{n-1}\right)x^n\\ &= \Theta\left(\lambda c_{n-1}\right) + \Theta\left(c_0\right)x + \Theta\left(c_1\right)x^2 + \cdots\\ &\quad + \Theta\left(c_{n-2}\right)x^{n-1}.\end{aligned} \tag{15}$$

Thus, $xc(x)$ is corresponding to a Θ-λ-constacyclic shift of $c(x)$, proving that the code C is a skew Θ-λ-constacyclic code if and only if C is a left ideal $\langle g(x)\rangle \subseteq \mathbb{F}_{p^m}[x;\Theta]/\langle x^n - \lambda\rangle$, where $g(x)$ is a right divisor of $x^n - \lambda$. We summarize this discussion by the following theorem, which is an extension of [3, Theorem 1].

Theorem 19 (extending [3, Theorem 1]). *Let Θ be an automorphism of $\mathbb{F}_{p^m}$, n an integer divisible by the order of Θ, and λ a unit in $\mathbb{F}_{p^m}$ which is fixed by Θ. Then the code C is a skew Θ-λ-constacyclic code if and only if C is a left ideal $\langle g(x)\rangle \subseteq \mathbb{F}_{p^m}[x;\Theta]/\langle x^n - \lambda\rangle$, where $g(x)$ is a right divisor of $x^n - \lambda$.*

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

$$G \coloneqq \begin{pmatrix} g_0 & \cdots & g_{n-k-1} & 1 & 0 & \cdots & 0\\ 0 & \Theta\left(g_0\right) & \cdots & \Theta\left(g_{n-k-1}\right) & 1 & \cdots & 0\\ 0 & \cdots & \cdots & \cdots & \Theta^2\left(g_{n-k-1}\right) & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & \cdots & 0 & \Theta^{k-1}\left(g_0\right) & \cdots & \Theta^{k-1}\left(g_{n-k-1}\right) & 1 \end{pmatrix}. \tag{16}$$

Lemma 20 (see [29, Lemma 17]). *Let Θ be an automorphism of $\mathbb{F}_{p^m}$, n an integer divisible by the order of Θ, and λ a unit in $\mathbb{F}_{p^m}$ which is fixed by Θ. Let C be the Θ-λ-constacyclic code generated by a monic right divisor $g(x)$ of $\langle x^n - \lambda\rangle$ and $h(x) := (x^n - \lambda)/g(x)$. If $h = h_0 + h_1 x + \cdots + x^{n-r}$, then the following matrix*

$$H := \begin{pmatrix} 1 & \Theta(h_{n-r-1}) & \cdots & \Theta^{n-r}(h_0) & 0 & \cdots & 0 \\ 0 & 1 & \Theta^2(h_{n-r-1}) & \cdots & \Theta^{n-r+1}(h_0) & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \Theta^r(h_{n-r-1}) & \cdots & \Theta^{n-1}(h_0) \end{pmatrix} \tag{17}$$

is a parity-check matrix for C.

Since $\Theta(1) = 1$ for any $\Theta \in \mathrm{Aut}(\mathbb{F}_{p^m})$, we have $\Theta(-1) = -1$. This shows that $-1 \in \mathbb{F}_{p^m}$ is fixed by Θ. The following two corollaries are direct consequences of Theorem 19.

Corollary 21. *Let Θ be an automorphism of $\mathbb{F}_{p^m}$ and n an integer divisible by the order of Θ. Then the code C is a skew Θ-negacyclic code if and only if C is a left ideal $\langle g(x)\rangle \subseteq \mathbb{F}_{p^m}[x;\Theta]/\langle x^n + 1\rangle$, where $g(x)$ is a right divisor of $x^n + 1$.*

Corollary 22 (see [3, Lemma 1]). *Let Θ be an automorphism of $\mathbb{F}_{p^m}$ and n an integer divisible by the order of Θ. Then the code C is a skew Θ-cyclic code if and only if C is a left ideal $\langle g(x)\rangle \subseteq \mathbb{F}_{p^m}[x;\Theta]/\langle x^n - 1\rangle$, where $g(x)$ is a right divisor of $x^n - 1$.*

We give an example to illustrate these results.

Example 23. Let α be a generator of the multiplicative group of $\mathbb{F}_4$; that is, α is a zero of $z^2 + z + 1 \in \mathbb{F}_2[z]$. Let Θ be the automorphism $a \mapsto a^2$ of $\mathbb{F}_4$. To list all $[4, 1]$ skew Θ-cyclic codes over $\mathbb{F}_4$, we find all monic degree 1 right factors of $x^4 - 1 \in \mathbb{F}_4[x;\Theta]$. They are

$$\begin{aligned} f_1 &= x + 1, \\ f_2 &= x + \alpha, \\ f_3 &= x + \alpha^2. \end{aligned} \tag{18}$$

Similarly, to list all $[4, 2]$ skew Θ-cyclic codes over $\mathbb{F}_4$, we find all monic degree 2 right factors of $x^4 - 1 \in \mathbb{F}_4[x;\Theta]$. They are

$$\begin{aligned} g_1 &= x^2 + 1, \\ g_2 &= x^2 + \alpha x + \alpha^2, \\ g_3 &= x^2 + \alpha^2 x + \alpha, \\ g_4 &= x^2 + \alpha^2 x + \alpha^2, \\ g_5 &= x^2 + x + \alpha, \\ g_6 &= x^2 + x + \alpha^2, \\ g_7 &= x^2 + \alpha x + \alpha. \end{aligned} \tag{19}$$

Let g be a right divisor of $x^n - 1$ of degree r. Then the skew Θ-cyclic code is $[n, n - r]$ linear code with generator matrix

$$G := \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & \Theta(g_0) & \cdots & \Theta(g_{r-1}) & \Theta(g_r) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \vdots & \Theta^{n-r-1}(g_0) & \Theta^{n-r-1}(g_1) & \vdots & \Theta^{n-r-1}(g_r) \end{pmatrix}. \tag{20}$$

A right factor of degree $n - k$ of $x^n - 1$ generates a linear code with parameters (n, k). If Θ is not the identity, then the skew polynomial ring $\mathbb{F}_{p^m}[x;\Theta]$ is in general not a unique factorization. In this case, we have more right factors than in the commutative case. For small values of n, all right skew factors of $x^n - 1$ can be found by a computational algebra system such as MAGMA (cf. [30]). Minimum distance of a code can be also calculated by using the MAGMA procedures. However, these procedures must be spent a long time for larger codes to check them. Therefore, the process will only find the smaller codes. The code parameters and the number of codes are introduced with these parameters $(n, k, d_{\min})$ because many different codes with the same minimum distance can be found. A generating polynomial for one code respected the class of parameters $(n, k, d_{\min})$ is also exhibited. Table 1, computed

Table 1: Generating polynomial of skew Θ-cyclic codes over $\mathbb{F}_4$ with their parameters $(n, k, d_{\min})$, where $n \leq 56$. This result is given by Boucher et al. [3].

$(n, k, d_{\min})$	Number	g
$(30, 16, 9)$	422	$x^{14} + x^{13} + \alpha x^{11} + x^{10} + x^9 + x^8 + \alpha x^7 + x^6 + \alpha x^5 + \alpha^2 x^4 + \alpha^2 x^2 + \alpha x + \alpha^2$
$(36, 20, 10)$	13	$x^{16} + \alpha^2 x^{15} + x^{13} + \alpha^2 x^{12} + x^{11} + \alpha x^{10} + x^9 + \alpha^2 x^8 + \alpha x^7 + \alpha x^6 + \alpha x^4 + \alpha^2 x^3 + \alpha^2 x^2 + 1$
$(40, 16, 15)$	6	$x^{24} + \alpha x^{23} + x^{22} + x^{21} + \alpha^2 x^{20} + \alpha x^{19} + \alpha x^{18} + \alpha x^{17} + x^{15} + x^{14} + x^{13} + \alpha x^{11} + \alpha^2 x^{10} + x^9 + x^8 + x^7 + \alpha^2 x^6 + \alpha x^5 + \alpha^2 x^4 + \alpha x^2 + \alpha^2$
$(42, 23, 11)$	92	$x^{19} + x^{17} + \alpha^2 x^{16} + \alpha x^{15} + \alpha^2 x^{14} + \alpha x^{13} + \alpha x^{11} + \alpha^2 x^{10} + \alpha x^9 + x^7 + \alpha x^6 + \alpha^2 x^5 + \alpha x^4 + \alpha x + \alpha^2$
$(42, 17, 16)$	3	$x^{25} + x^{23} + \alpha x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + \alpha^2 x^{17} + \alpha^2 x^{16} + \alpha x^{15} + \alpha x^{14} + x^{13} + x^{11} + x^{10} + x^8 + \alpha^2 x^4 + \alpha^2 x^3 + x^2 + \alpha x + 1$
$(48, 25, 13)$	2	$x^{23} + \alpha^2 x^{22} + x^{21} + \alpha x^{20} + \alpha x^{19} + \alpha^2 x^{18} + \alpha x^{17} + \alpha x^{14} + \alpha^2 x^{13} + \alpha^2 x^{11} + x^9 + \alpha x^7 + x^6 + x^3 + \alpha^2 x^2 + 1$
$(48, 19, 17)$	2	$x^{29} + \alpha^2 x^{28} + x^{26} + \alpha x^{25} + \alpha^2 x^{24} + \alpha x^{23} + \alpha x^{21} + \alpha x^{20} + \alpha^2 x^{19} + \alpha x^{18} + \alpha x^{17} + \alpha x^{16} + x^{15} + x^{14} + \alpha x^{13} + \alpha x^{10} + \alpha x^8 + \alpha^2 x^7 + x^6 + x^5 + x^4 + \alpha^2 x^3 + x^2 + \alpha^2$
$(56, 30, 14)$	1	$x^{26} + x^{23} + \alpha x^{22} + \alpha^2 x^{21} + \alpha x^{20} + \alpha^2 x^{19} + \alpha^2 x^{18} + \alpha x^{17} + x^{16} + x^{14} + x^{13} + \alpha x^{11} + \alpha^2 x^{10} + \alpha^2 x^9 + \alpha^2 x^8 + \alpha x^7 + \alpha^2 x^6 + \alpha x^5 + \alpha x^5 + \alpha^2 x^4 + x^2 + \alpha^2 x + \alpha^2$

by Bosma et al. [30], provides parameters and generating polynomials of skew Θ-cyclic codes over $\mathbb{F}_4$, where Θ is the Frobenius automorphism and α is a generator of the multiplicative group of $\mathbb{F}_4$.

Given n-tuples $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_{p^m}$, their inner product or dot product is defined in the usual way:

$$x \circ y = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1}, \tag{21}$$

evaluated in $\mathbb{F}_{p^m}$. Two codewords x, y are called *orthogonal* if $x \circ y = 0$. For a linear code C over $\mathbb{F}_{p^m}$, its dual code $C^\perp$ is the set of n-tuples over $\mathbb{F}_{p^m}$ that are orthogonal to all codewords of C; that is,

$$C^\perp = \{x \mid x \circ y = 0, \ \forall y \in C\}. \tag{22}$$

A code C is called *self-orthogonal* if $C \subset C^\perp$, and it is called *self-dual* if $C = C^\perp$. The following result is well known (cf. [29]).

Lemma 24 (see [29, Corollary 18]). *Let Θ be an automorphism of $\mathbb{F}_{p^m}$, n an integer divisible by the order of Θ, and λ a unit in $\mathbb{F}_{p^m}$ which is fixed by Θ. Let $g(x) = \sum_{i=0}^{r-1} g_i x^i + x^r$ and $h(x) = \sum_{i=0}^{n-r-1} h_i x^i + x^{n-r}$ such that $h(x)g(x) = x^n - 1$. The dual of the skew Θ-cyclic code generated by $g(x)$ in $\mathbb{F}_{p^m}[x; \Theta]/\langle x^n - 1\rangle$ is the skew Θ-cyclic code generated by*

$$g^\perp = 1 + \Theta(h_{n-r-1})\, x + \cdots + \Theta^{n-r}(h_0)\, x^{n-r}. \tag{23}$$

We give an example to illustrate how we use Lemma 24 to determine Euclidean self-dual Θ-cyclic codes.

Example 25. Let α be a generator of the multiplicative group of $\mathbb{F}_4$; that is, α is a zero of $z^2 + z + 1 \in \mathbb{F}_2[z]$. Let Θ be the automorphism $a \mapsto a^2$ of $\mathbb{F}_4$. We find all Euclidean self-dual Θ-cyclic codes over $\mathbb{F}_4$ in $\mathbb{F}_4[x; \Theta]/(x^4 - 1)$. From Example 23, we can list all monic degree 2 right factors of $x^4 - 1 \in \mathbb{F}_4[x; \Theta]$. Put h_i $(i = \{1, \ldots, 7\})$ to be all monic degree 2 right factors such that $h_i \cdot g_i = x^4 - 1$, $\forall i \in \{1, \ldots, 7\}$. Then we have

$$\begin{aligned}
h_1 &= x^2 + 1,\\
h_2 &= x^2 + \alpha x + \alpha,\\
h_3 &= x^2 + \alpha^2 x + \alpha^2,\\
h_4 &= x^2 + \alpha^2 x + \alpha,\\
h_5 &= x^2 + x + \alpha^2,\\
h_6 &= x^2 + x + \alpha,\\
h_7 &= x^2 + \alpha x + \alpha^2.
\end{aligned} \tag{24}$$

Applying Lemma 24, we have

$$\begin{aligned}
g_1^\perp &= x^2 + 1,\\
g_2^\perp &= \alpha x^2 + \alpha^2 x + 1,\\
g_3^\perp &= \alpha^2 x^2 + \alpha x + 1,\\
g_4^\perp &= \alpha x^2 + \alpha x + 1,\\
g_5^\perp &= \alpha^2 x^2 + x + 1,\\
g_6^\perp &= \alpha x^2 + x + 1,\\
g_7^\perp &= \alpha^2 x^2 + \alpha^2 x + 1,
\end{aligned} \tag{25}$$

where the dual of the skew Θ-cyclic code generated by $g_i(x)$ in $\mathbb{F}_4[x; \Theta]/\langle x^n - 1\rangle$ is the Θ-cyclic code generated by $g_i^\perp$. Suppose that C_i, the skew Θ-cyclic code generated by $g_i(x)$ in $\mathbb{F}_4[x; \Theta]/\langle x^n - 1\rangle$, is an Euclidean self-dual Θ-cyclic code. Then we have $C = C^\perp$. This implies that $g_i^\perp$ is a constant multiple of g_i. From this, the skew Θ-cyclic codes generated by $g_1(x)$, $g_2(x)$, $g_3(x)$ are Euclidean self-dual Θ-cyclic codes.

We now turn our attention to Euclidean self-dual Θ-cyclic codes over $\mathbb{F}_4$ (cf. [29]). Suppose that Θ is the Frobenius

automorphism and α is a generator of $\mathbb{F}_4$. It is easy to see that n must be an even number. In fact, by Lemma 24, if n is odd, then there are no Euclidean self-dual codes. Therefore, $n = 2r$ for some $r \in \mathbb{Z}^+$. Let C be a self-dual code. Applying Lemma 24, the coefficients of the generating polynomial $g^\perp$ of $C^\perp$ is expressed. Since $C = C^\perp$, $g^\perp$ and g must differ by a constant multiple and $\deg(g) = \deg(g^\perp)$. Now assume that $g = \sum_{i=0}^{r-1} g_i x^i + x^r$ with $g_0 \neq 0$ is the generator polynomial of the self-dual Θ-cyclic code C. Assume that $h = x^r + \sum_{i=0}^{r-1} h_i x^i$ such that $gh = x^n - 1$. From Lemma 24, the code $C^\perp$ is generated by $g^\perp = 1 + \sum_{i=1}^{r} \Theta^i(h_{r-i}) x^i$. Since $g^\perp$ is a constant multiple of g, $g^\perp = \Theta^r(h_0) g$. This implies that if the coefficients of both polynomials g and $g^\perp$ are compared, then system (26) is built as follows:

$$\begin{aligned} 1 &= \Theta^r(h_0)\, g_0, \\ \Theta^i(h_{r-i}) &= \Theta^r(h_0)\, g_i, \quad i = 0, 1, \ldots, r-1. \end{aligned} \tag{26}$$

Since $\Theta^2(\alpha) = \alpha$, it is easy to see that $\Theta = \Theta^{-1}$. By assumption, $g_0 \neq 0$. This implies that $g_0^{-1} = g_0^2$. Hence, system (26) becomes

$$\begin{aligned} h_0 &= \Theta^r\left(g_0^2\right), \\ (h_{r-i}) &= \Theta^i\left(g_0^2 \cdot g_i\right), \quad i = 0, 1, \ldots, r-1. \end{aligned} \tag{27}$$

System (27) allows expressing the coefficients of h as follows:

$$h = \Theta^2\left(g_0^2\right) + \sum_{i=1}^{r} \Theta^{r-i}\left(g_0^2\right) \Theta^{r-i}\left(g_{r-i}\right) x^i. \tag{28}$$

From $\Theta^i(a) = a^{(2^i \bmod 3)}$, (28) becomes

$$h = g_0^{(2^{r-1} \bmod 3)} + \sum_{i=1}^{r} g_0^{(2^{r-i+1} \bmod 3)} g_{r-i}^{(2^{r-i} \bmod 3)} x^i, \tag{29}$$

where powers of g_i are of degree less than 4. By using the rule $x^i a = a^{(2^i \bmod 3)} x^i$ and expanding the skew product $(x^n - 1) - (h \cdot g) = 0$, $(2r + 1)$ polynomial equations in the coefficients g_i of degree less than 4 in each variable can be determined. From $g_i \in \mathbb{F}_4$, $g_i^4 - g_i = 0$ for any $i = 1, \ldots, r$. Adding r equations $g_i^4 - g_i = 0$ to $2r+1$ polynomial equations in r variables of degree less than 4 to have a system, then the solutions of this system can be found by using Groebner bases in MAGMA system because the solution set must be finite. This shows that all polynomials g corresponding to a solution will be listed and hence the linear code which it generates and its minimum Hamming distance can be computed. Then all Euclidean self-dual Θ-cyclic codes of length $n \leq 40$ in $\mathbb{F}_4[x; \Theta]$ will be exhibited. In [29], Boucher and Ulmer gave the table of Euclidean self-dual codes over $\mathbb{F}_4$ and $n \leq 40$. We refer the readers to [29] for more details.

Recall that Hermitian inner product is denoted and calculated by $\langle u, v\rangle_H = \sum_{i=0}^{n-1} u_i \Theta(v_i)$, for all $u = (u_0, \ldots, u_{n-1})$ and $v = (v_0, \ldots, v_{n-1})$ in $\mathbb{F}_{p^m}^n$. Then we give the definition of the Hermitian dual code of a code C as follows:

$$C^{\perp_H} = \left\{ v \in \mathbb{F}_{p^m}^n \mid \langle v, c\rangle_H = 0, \ \forall c \in C \right\}. \tag{30}$$

If $C = C^{\perp_H}$, then C is said to be a Hermitian self-dual code. It is easy to check that if n is odd, then there is no Hermitian self-dual of Θ-cyclic codes. Therefore, n must be an even number. Suppose that the order m of Θ divides $n = 2r$. Let $g = \sum_{j=0}^{r} g_j x^j$ and $h = \sum_{i=0}^{r} h_i x^i$ be elements of $\mathbb{F}_{p^m}[x; \Theta]$ such that $h \cdot g = x^{2r} - 1$. The Hermitian dual of a Θ-cyclic code generated by g in $\mathbb{F}_{p^m}[x; \Theta]/\langle x^{2r} - 1\rangle$ is again Θ-cyclic code and is generated by $g^H = \Theta(h_r) + \Theta^2(h_{r-1})x + \cdots + \Theta^{r+1}(h_0)x^r$ [29, Lemma 21]. Similar to the case of Euclidean self-dual codes, all the Hermitian self-dual Θ-cyclic codes of length $n \leq 40$ in $\mathbb{F}_4[x; \Theta]$ can be found. The polynomial h of Hermitian self-dual code in $\mathbb{F}_4[x; \Theta]$ can be expressed as follows:

$$\begin{aligned} h = x^r + \sum_{i=1}^{r-1} \left(\Theta^{r-i+1}\left(g_0^2\right) \Theta^{r-i+1}\left(g_{r-i}\right) x^i\right) \\ + \Theta^{r+1}\left(g_0^2\right). \end{aligned} \tag{31}$$

In this case, the coefficient of (31) is shifted by $\Theta^{m-1} = \Theta$. Expanding the skew product $x^{2r} - 1 - h \cdot g = 0$ which gives again a polynomial system of equations, the solutions of this system can be also computed by using Groebner bases in MAGMA because the solution set must be finite. Similar to the case of Euclidean self-dual codes, in [29], Boucher and Ulmer also gave the table of Hermitian self-dual codes over $\mathbb{F}_4$ and $n \leq 40$. For more details we refer the readers to [29].

4. Decoding Skew Θ-Cyclic Codes over Finite Fields

In coding theory, BCH codes were invented in 1959 by French mathematician Alexis Hocquenghem and independently in 1960 by Raj Bose and D. K. Ray-Chanahuri. General decoding procedure for decoding BCH codes with designed distance is introduced in [31]. In this section, we first give the algorithm for decoding with cyclic codes in $\mathbb{F}_{p^m}[x]$. After that, we will modify the algorithm for decoding skew BCH codes.

Let C be $[n, k, d]$ cyclic code over $\mathbb{F}_{p^m}$ with generator polynomial $g(x)$ of degree $n - k$. Suppose that $c(x) \in C$ is transmitted and $y(x) = c(x) + e(x)$ is received, where $e(x) = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}$ is the error vector with $wt(e(x)) \leq t$ and $t = (d - 1)/2$. Let $R_{g(x)}$ be the unique remainder when $h(x)$ is divided by $g(x)$ according to the Division Algorithm; that is, $R_{g(x)}(h(x)) = r(x)$, where $h(x) = g(x)f(x) + r(x)$, with $r(x) = 0$ or $\deg r(x) < n - k$. Then the function $R_{g(x)}$ satisfies the following properties.

Theorem 26 (see [27, Theorem 4.6.1]). *With the preceding notation the following statements hold:*

(i) $R_{g(x)}(ah(x) + bh'(x)) = aR_{g(x)}(h(x)) + bR_{g(x)}(h'(x))$ *for all* $h(x); h'(x) \in \mathbb{F}_{p^m}[x]$ *and all* $a; b \in \mathbb{F}_{p^m}$,

(ii) $R_{g(x)}(h(x) + a(x)(x^n - 1)) = R_{g(x)}(h(x))$,

(iii) $R_{g(x)}(h(x)) = 0$ *if and only if* $h(x) \pmod{(x^n - 1)} \in C$,

(iv) *If* $c(x) \in C$, *then* $R_{g(x)}(c(x) + e(x)) = R_{g(x)}(e(x))$,

Table 2

$e(x)$	$S(e(x))$	$e(x)$	$S(e(x))$
x^{14}	x^7	$x^6 + x^{14}$	$x^3 + x^5 + x^6$
$x^{13} + x^{14}$	$x^6 + x^7$	$x^5 + x^{14}$	$x^2 + x^4 + x^5 + x^6 + x^7$
$x^{12} + x^{14}$	$x^5 + x^7$	$x^4 + x^{14}$	$x + x^3 + x^4 + x^5 + x^7$
$x^{11} + x^{14}$	$x^4 + x^7$	$x^3 + x^{14}$	$1 + x^2 + x^3 + x^4 + x^7$
$x^{10} + x^{14}$	$x^3 + x^7$	$x^2 + x^{14}$	$x + x^2 + x^3 + x^4 + x^7$
$x^{10} + x^{14}$	$x^3 + x^7$	$x^2 + x^{14}$	$x + x^2 + x^5 + x^6$
$x^9 + x^{14}$	$x^2 + x^7$	$x + x^{14}$	$1 + x + x^4 + x^5 + x^6 + x^7$
$x^8 + x^{14}$	$x + x^7$	$1 + x^{14}$	$1 + x^4 + x^6$
$x^7 + x^{14}$	$1 + x^7$		

(v) *If* $R_{g(x)}(e(x)) = R_{g(x)}(e'(x))$, *where* $e(x)$ *and* $e'(x)$ *each have weight at most* t, *then* $e(x) = e'(x)$,

(vi) $R_{g(x)}(h(x)) = h(x)$ *if* $\deg h(x) < n - k$.

Theorem 27 (see [27, Theorem 4.6.2]). *Let* $g(x)$ *be a monic divisor of* $x^n - 1$ *of degree* $n - k$. *If* $R_{g(x)}(h(x)) = s(x)$, *then* $R_{g(x)}(xh(x)(\mathrm{mod}(x^n - 1)) = R_{g(x)}(xs(x)) = xs(x) - g(x)s_{n-k-1}$, *where* s_{n-k-1} *is the coefficient of* x^{n-k-1} *in* $s(x)$.

Define the syndrome polynomial $S(h(x))$ of any $h(x)$ to be

$$S(h(x)) = R_{g(x)}\left(x^{n-k}h(x)\right). \tag{32}$$

We now describe the first version of the Meggitt Decoding Algorithm and we provide an example to illustrate each step.

Step 1. Find the syndrome polynomial $S(e(x))$ of error patterns $e(x) = \sum_{i=0}^{n-1} e_i x^i$ such that $wt(e(x)) \le t$ and $e_{n-1} \neq 0$.

Example 28 (see [27, Example 4.6.3]). Let C be the $[15, 7, 5]$ binary cyclic code with a generating polynomial $g(x) = 1 + x^4+x^6+x^7+x^8 = (x-\xi)(x-\xi^2)(x-\xi^3)(x-\xi^4)(x-\xi^6)(x-\xi^8)(x-\xi^9)(x-\xi^{12})$, where ξ is a 15th root of unity in $\mathbb{F}_{16}$. Then the syndrome polynomial of $e(x)$ is $S(e(x)) = R_{g(x)}(x^8e(x))$. The syndrome polynomial for polynomial $1+x^{14}$ can be computed as follows. First, it is easy to see that $R_{g(x)}(x^8) = 1+x^4+x^6+x^7$. Then $S(1+x^{14}) = R_{g(x)}(x^8(1+x^{14})) = R_{g(x)}(x^8)+R_{g(x)}(x^7) = 1 + x^4 + x^6$. Applying Theorem 26, $R_{g(x)}(x^9) = R_{g(x)}(xx^8) = R_{g(x)}(x+x^5+x^7)+R_{g(x)}(x^8) = x+x^5+x^7+1+x^4+x^6+x^7 = 1+x+x^4+x^5+x^6$. Similarly, by applying Theorems 26 and 27, all syndrome polynomials will be determined. Table 2 shows all syndrome polynomials.

Step 2. Assume that $y(x)$ is the received polynomial. Then the syndrome polynomial $S(y(x)) = R_{g(x)}(x^{n-k}y(x))$ can be computed. Applying Theorem 26(iv), $S(y(x)) = S(e(x))$, where $y(x) = c(x) + e(x)$ and $c(x) \in C$.

Example 29 (see [27, Example 4.6.4]). We give an example for Step 2. We continue Example 28. Suppose that $y(x) = 1+x^4+x^7+x^9+x^{10}+x^{12}$ is a received polynomial. This implies that $S(y(x)) = x + x^2 + x^6 + x^7$.

Step 3. If $S(y(x))$ is in list computed in Step 1, then the error polynomial $e(x)$ can be computed and it can be subtracted from $y(x)$ to the corrected codeword $c(x) = y(x) - e(x)$. If $S(y(x))$ is not appearing in the list computed in Step 1, then the process will continue to Step 4.

Step 4. It is continuing to compute the syndrome polynomial of $xy(x), x^2y(x), \ldots$ until the syndrome polynomial is in the list from Step 1. If $S(x^iy(x))$ is in this list and it is associated with the error polynomial $e^*(x)$, then the received vector is decoded as $y(x) - x^{n-i}e^*(x)$. By using Theorem 27, $R_{g(x)}(x^{n-k}y(x)) = S(y(x)) = \sum_{i=0}^{n-k-1} s_i x^i$ and $S(xy(x)) = R_{g(x)}(x^{n-k}xy(x)) = R_{g(x)}(x(x^{n-k}y(x))) = R_{g(x)}(xS(y(x))) = xS(y(x)) - s_{n-k-1}g(x)$.

We finish this part by the following example.

Example 30 (see [27, Example 4.6.6]). We can see that $S(y(x)) = x + x^2 + x^6 + x^7$ is not in the list computed in Step 1, then we continue to compute $S(xy(x)) = x(x + x^2 + x^6 + x^7) - 1 \cdot g(x) = 1 + x^2 + x^3 + x^4 + x^6$, which is not also appearing in the list in Step 1. It is easy to check that $S(x^2y(x)) = x(1+x^2+x^3+x^4+x^6)-0\cdot g(x) = x+x^3+x^4+x^5+x^7$ is in the list in Step 1. This implies that $y(x)$ is decoded as $y(x) - (x^2 + x^{12}) = 1 + x^2 + x^4 + x^7 + x^9 + x^{10}$.

Suppose that $\alpha \in \mathbb{F}_q$ is a primitive $(q-1)$th root of unity, n is even, $q = 2^m$, and Θ is an automorphism of $\mathbb{F}_q$ such that $\Theta(\alpha) = \alpha^2$. We give two results in [3] and use them later.

Lemma 31 (see [3, Proposition 1]). *For* $P = \sum_{k=0}^{n-1} a_k x^k \in \mathbb{F}_q[x; \Theta]$, $\beta \in \mathbb{F}_q$ *and* $r \in \mathbb{F}_q$ *the remainder of the right division of* P *by* $x - \beta$, *then* $r = \overline{P}$ *is a (classical) polynomial given by* $\overline{P} = \sum_{k=0}^{n-1} a_k z^{2^k-1} \in \mathbb{F}_q[z]$.

Lemma 32 (see [3, Proposition 2]). *Let* n *be even,* $q = 2^n$, *and* α *a primitive* $(q-1)$*th root of unity. Let* C *be a* Θ*-cyclic code with* $\Theta(\alpha) = \alpha^2$. *Let* $G \in \mathbb{F}_q[x; \Theta]$ *be its generating polynomial such that* G *is a right divisor of* $x^n - 1$ *in* $\mathbb{F}_q[x; \Theta]$ *and* $x - \alpha^k$ *is a right factor of* G *for* $k \in \{1, \ldots, d-1\}$. *The distance of the code* C *is equal to its designed distance* d.

We now introduce the procedure for decoding skew BCH codes. Assume that $e = e_{i_1}x^{i_1} + \cdots + e_{i_r}x^{i_r}$ is the error polynomial with $i_1 < i_2 < \cdots < i_r$, where $r \le (d-1)/2$. The polynomial $S_d(z) = \sum_{k=1}^{d-1} \mathrm{Rem}(e, x - \alpha^k)z^{k-1} \in \mathbb{F}_{p^m}[z]$ is called a *syndrome polynomial* of e. Note that $\mathrm{Rem}(e, x - \alpha^k)$ is to be computed in the skew polynomial $\mathbb{F}_{p^m}[x; \Theta]$. Hence,

$$S_d(z) = \sum_{k=1}^{d-1} \mathrm{Rem}\left(e, x - \alpha^k\right) z^{k-1} = \sum_{k=1}^{d-1} \overline{e}\left(\alpha^k\right) z^{k-1}, \tag{33}$$

where $\overline{e}(z) = \sum_{k=1}^{r} e_{i_k} z^{j_k} \in \mathbb{F}_{p^m}[z]$ and $j_k = 2^{i_k} - 1$. The polynomials $\sigma(z) = \prod_{k=1}^{r}(1 - \alpha^{j_k} z)$ and $w(z) = \sum_{l=1}^{r} e_{i_l} \alpha^{j_l} - \prod_{k \neq l}(1 - \alpha^{j_k} z)$ are called *pseudolocator polynomial* and *evaluator polynomial*, respectively. Let

$$\begin{aligned} S(z) &= \sum_{k=1}^{\infty} \overline{e}\left(\alpha^k\right)\left(z^{k-1}\right) \\ &= S_d(z) + z^{d-1} \sum_{k=0}^{\infty} \overline{e}\left(\alpha^{k+1+d}\right) z^k. \end{aligned} \tag{34}$$

This implies that $\sigma(z)S(z) = w(z)$. This equation can be written to become $\sigma(z) + S_d(z) + v(z)z^{d-1} = w(z)$, where $v(z) = \sigma(z) \sum_{k=1}^{\infty} \overline{e}(\alpha^{k+1+d}) z^k$.

Applying the Euclidean Algorithm to the polynomials $S_d(z)$ and z^{d-1} in $\mathbb{F}_{p^m}[z]$, three sequences $(r_i(z))$, $(u_i(z))$, and $(v_i(z))$ are defined as follows:

$$\begin{aligned} r_{-1}(z) &= z^{d-1}, \\ r_0(z) &= S_d(z), \\ u_{-1}(z) &= 0, \\ u_0(z) &= 1, \\ v_{-1}(z) &= 1, \\ v_0(z) &= 0 \end{aligned} \tag{35}$$

and $r_i(z) = r_{i-2}(z) - q_i(z) r_{i-1}(z)$, $u_i(z) = u_{i-2}(z) - q_i(z) u_{i-1}(z)$, and $v_i(z) = v_{i-2}(z) - q_i(z) v_{i-1}(z)$ with $\deg(r_i(z)) < \deg(r_{i-1})(z)$. The process will stop whenever k can be determined satisfying $\deg(r_{k-1}) \geq (d-1)/2$ and $\deg(r_k) < (d-1)/2$. From this, $r_k(z)$, $\sigma(z)$, and $w(z)$ can be computed by three equations as follows:

$$\begin{aligned} u_k(z) S_d(z) + v_k(z) z^{d-1} &= r_k(z); \\ \sigma(z) &= \frac{u_k(z)}{u_k(0)}; \\ w(z) &= \frac{r_k(z)}{r_k(0)}. \end{aligned} \tag{36}$$

From the roots of the pseudolocator polynomial $\sigma(z)$, all j_l, $l \in \{1, 2, \ldots, r\}$, will be listed. This shows that

$$e_{i_l} = \alpha^{-j_l} w\left(\alpha^{-j_l}\right) \prod_{k \neq l} \left(1 - \alpha^{j_k - j_l}\right), \quad l \in \{1, 2, \ldots, r\}. \tag{37}$$

From the equation above, all coefficients of e are also determined. For each j_l, a finite number of possibilities i_l solutions to the equation $j_l \equiv 2^{i_l} - 1 \pmod{n}$ can be found. Similarly to the procedure for decoding BCH codes, this process will test until the skew polynomial e is determined. Since e is unique, the decoded word can be exhibited, as required.

We conclude this section by an example provided by Boucher et al. in [3] to illustrate this process in detail.

Example 33 (see [3]). Let α be such that $\alpha^{2^{10}-1} = 1$. Suppose that $m = n = 10$. Then the polynomial $g(x) = x^6 + \alpha^{345}x^5 + \alpha^{643}x^4 + \alpha^{878}x^3 + \alpha^{670}x^2 + \alpha^{1020}x + \alpha^{777}$ is a divisor of $x^{10} + 1$ in $\mathbb{F}_{2^{10}}[x; \Theta]$. This implies that $g(x)$ is the generator polynomial of a Θ-cyclic code of length 10 over $\mathbb{F}_{2^{10}}$. We can see that $x - \alpha^k$ is a right factor of $g(x)$ for all $k \in \{1, \ldots, 6\}$. Hence, the designed distance of the code C is $d = 7$. Now we consider $f(x) = \alpha^{654}x^9 + \alpha^{547}x^8 + \alpha^{650}x^7 + \alpha^{16}x^6 + \alpha^{567}x^5 + \alpha^{29}x^4 + \alpha^{87}x^3 + \alpha^{696}x^2 + \alpha^{252}x + \alpha^{555}$ and an error $e = \alpha^{341}x^9 + \alpha^{682}x^8 + \alpha^{682}$. The pertubed codeword h is

$$\begin{aligned} f + e = {} & \alpha^{818}x^9 + \alpha^{775}x^8 + \alpha^{650}x^7 + \alpha^{16}x^6 + \alpha^{567}x^5 \\ & + \alpha^{29}x^4 + \alpha^{87}x^3 + \alpha^{696}x^2 + \alpha^{252}x + \alpha^{557}. \end{aligned} \tag{38}$$

Since $d = 7$ and polynomial h, we have the syndrome polynomial

$$\begin{aligned} S_7(z) = {} & \alpha^{404}z^5 + \alpha^{403}z^4 + \alpha^{601}z^3 + \alpha^{645}z^2 + \alpha^{614}z \\ & + \alpha^{406}. \end{aligned} \tag{39}$$

Applying Euclid Algorithm to $S_7(z)$ and z^6 in $\mathbb{F}_{2^{10}}[z]$ with $(d-1)/2 = 3$, we can get the pseudolocator polynomial $\sigma(z) = \alpha^{766}z^3 + \alpha^{642}z^2 + \alpha^{241}z + 1$ and the evaluator polynomial $w(z) = \alpha^{84}z^2 + \alpha^{185}z + \alpha^{406}$. The roots of the polynomial $\sigma(z)$ are 1, α^{512}, and α^{768}. From this, we have $r = 3$, $j_1 = 0$, $j_2 = 511$, and $j_3 = 255$. By the polynomial $w(z)$, we can find $e_{i_1} = \alpha^{682}$, $e_{i_2} = \alpha^{341}$, and $e_{i_3} = \alpha^{682}$. Combining this result and the equations $2^{i_k} - 1 \equiv j_k \pmod{10}$, we have $i_1 = 0 \pmod{10}$, $i_2 = 1, 5, 9 \pmod{10}$, and $i_3 = 4, 8 \pmod{10}$. Then we can list all possible errors as follows:

$$\begin{aligned} &\alpha^{341}x^9 + \alpha^{682}x^8 + \alpha^{682}; \\ &\alpha^{682}x^8 + \alpha^{341}x^5 + \alpha^{682}; \\ &\alpha^{341}x^5 + \alpha^{682}x^4 + \alpha^{682}; \\ &\alpha^{682}x^8 + \alpha^{341}x + \alpha^{682}; \\ &\alpha^{341}x^9 + \alpha^{682}x^4 + \alpha^{682}; \\ &\alpha^{682}x^4 + \alpha^{341}x + \alpha^{682}. \end{aligned} \tag{40}$$

It is easy to find that $e = \alpha^{341}x^9 + \alpha^{682}x^8 + \alpha^{682}$.

5. Skew Θ-λ-Constacyclic Codes over Finite Chain Rings

Constacyclic codes have practical applications as they can be efficiently encoded using simple shift registers. They have rich algebraic structures for efficient error detection and correction, which explains their preferred role in engineering. Classically, the algebraic structures of constacyclic codes are determined by ideals in the polynomial rings over finite fields, Galois rings, and finite chain rings. In [3], Boucher et al. generalized the notion of cyclic codes by using generator polynomial in noncommutative skew polynomial rings. Since

there are much more skew cyclic codes, the new class of codes allowed them to systematically search for codes. Later on, the approach has been extended to codes over Galois rings [29]. In 2012, Jitman et al. [26] studied skew Θ-λ-constacyclic codes over finite chain rings. These codes have been studied for a particular case when codes are generated by monic right divisors of $x^n - \lambda$, where λ is a unit in the finite chain rings fixed by a given automorphism. Similarly to the case of skew Θ-λ-constacyclic codes over finite fields, when Θ is the identity automorphism, they become classical constacyclic codes over finite chain rings. Therefore, skew Θ-λ-constacyclic codes over finite chain rings can be considered as a generalization of classical constacyclic codes over finite chain rings. This is the reason why the study of skew Θ-λ-constacyclic codes over finite chain rings is important. In this section, we overview the study of skew Θ-λ-constacyclic codes over finite chain rings studied by Jitman et al. [26].

A finite commutative ring with identity is called a *finite chain ring* if its ideals are linearly ordered by inclusion or, equivalently, its ideals are principal and its maximal ideal is unique. In [32], it is known that a finite chain ring is local and its unique maximal ideal is principal. Constacyclic codes over a finite commutative chain ring have been studied by many authors (see, e.g., [23, 33–36]). The structure of constacyclic codes is also introduced over a special family of finite chain rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Recently, skew Θ-codes over finite fields and Galois rings were studied by Boucher et al. Motivated by these results, in [26], Jitman et al. generalized the concept of skew Θ-λ-constacyclic codes over finite fields and Galois rings to that over finite chain rings. The structure of all skew Θ-λ-constacyclic codes over a finite chain ring is determined. Moreover, Euclidean and Hermitian dual codes of skew Θ-cyclic and negacyclic codes are considered. They also studied skew Θ-λ-constacyclic codes over a special case $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ of a finite chain ring.

In this section, let $\mathscr{R}$ be a finite chain ring with unique maximal ideal $\langle\gamma\rangle$. Then γ is a nilpotent ideal of $\mathscr{R}$ and we denote its nilpotency index by t. Hence, the ideals of $\mathscr{R}$ form the following chain:

$$\mathscr{R} = \langle 1\rangle \supsetneq \langle\gamma\rangle \supsetneq \cdots \supsetneq \left\langle\gamma^{t-1}\right\rangle \supsetneq \left\langle\gamma^{t}\right\rangle = \langle 0\rangle . \tag{41}$$

Analogous to the case of finite fields, the set of automorphisms of $\mathscr{R}$ forms a group under composition, denoted by $\mathrm{Aut}(\mathscr{R})$. Many classes of finite chain rings have nontrivial automorphism groups. For examples, $\mathrm{Aut}(\mathrm{GR}(p^e, m))$ is nontrivial if and only if $m \geq 2$ (cf. [16]) and $\mathrm{Aut}(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m})$ is nontrivial if and only if $m \geq 2$ or p is odd or $e \geq 3$ (cf. [37, Proposition 1]).

We know that $\mathbb{F}_{p^m}[x;\Theta]$ is left and right Euclidean ring whose left and right ideals are principal. Unlike the ring $\mathbb{F}_{p^m}[x;\Theta]$, if $\mathscr{R}$ is a finite chain ring, then the skew polynomial ring $\mathscr{R}[x;\Theta]$ is neither left nor right Euclidean ring. Therefore, we need to define left and right divisions. Suppose that $f(x) = \sum_{i=0}^{s} a_i x^i$ and $g(x) = \sum_{j=0}^{t} b_j x^j$, where b_t is a unit in $\mathscr{R}$ and $s \geqslant t$. We can see that the degree of polynomial

$$f(x) - a_s \cdot \Theta^{s-t}\left(b_t^{-1}\right) x^{s-t} g(x) \tag{42}$$

is less than the degree of $f(x)$. By the inductive method, we can obtain skew polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$ with $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$. If $r(x) = 0$, then we say that $g(x)$ is a right divisor of $f(x)$. The skew polynomials $q(x)$ and $r(x)$ are unique. They are called *the right quotient* and *right remainder*, respectively. Note that if $s < t$, then we put $f(x) = 0 \cdot g(x) + f(x)$. This algorithm is called the *Right Division Algorithm* in $\mathscr{R}[x;\Theta]$. The *Left Division Algorithm* in $\mathscr{R}[x;\Theta]$ can be defined similarly, using the fact that the degree of

$$f(x) - g(x)\,\Theta^{-t}\left(a_s b_t^{-1}\right) x^{s-t} \tag{43}$$

is less than the degree of $f(x)$. Now we recall the definition of skew Θ-λ-constacyclic codes in $\mathscr{R}[x;\Theta]$. Given an automorphism Θ of $\mathscr{R}$ and a unit in $\mathscr{R}$, a linear code C is said to be skew Θ-λ-constacyclic if C is closed under the Θ-λ-constacyclic shift $\tau_{\Theta,\lambda} : \mathscr{R}^n \to \mathscr{R}^n$ defined by

$$\begin{aligned}&\tau_{\Theta,\lambda}(c_0, c_1, \ldots, c_{n-1})\\ &\quad = \left(\Theta(\lambda c_{n-1}), \Theta(c_0), \ldots, \Theta(c_{n-2})\right).\end{aligned} \tag{44}$$

5.1. Skew Θ-λ-Constacyclic Codes over Finite Chain Rings. For a skew polynomial $g(x)$ in $\mathscr{R}[x;\Theta]$, then a left ideal generated by $g(x)$, denoted by $\langle g(x)\rangle$, is in general not a two-sided ideal. However, if $g(x) = x^t h(x)$ ($t \in \mathbb{N}_0$) such that $h(x)$ is central (i.e., commutes with all elements of $\mathscr{R}[x;\Theta]$), then $\langle f(x)\rangle$ is a principal two-sided ideal in $\mathscr{R}[x;\Theta]$. From this remark, the following corollary is a direct consequence.

Corollary 34 (see [26, Corollary 2.2]). *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 $\mathscr{R}[x;\Theta]/\langle f(x)\rangle$.*

Analogous to classical constacyclic codes, we study skew Θ-λ-constacyclic codes as left ideals in $\mathscr{R}[x;\Theta]/\langle x^n - \lambda\rangle$. Note that $\mathscr{R}[x;\Theta]$ is a noncommutative ring. So we need to have the conditions of Θ and λ which ensure that $\langle x^n - \lambda\rangle$ is a two-sided ideal.

Lemma 35 (see [26, Proposition 2.2]). *Let n be a positive integer and λ a unit in $\mathscr{R}$. Then the following statements are equivalent:*

(i) *$x^n - \lambda$ is central in $\mathscr{R}[x;\Theta]$.*

(ii) *$\langle x^n - \lambda\rangle$ is a two-sided ideal.*

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

For Θ-λ-constacyclic codes over finite fields, a code C is a skew Θ-λ-constacyclic code if and only if C is a left ideal $\langle g(x)\rangle \subseteq \mathbb{F}_{p^m}[x;\Theta]/\langle x^n - \lambda\rangle$, where $g(x)$ is right divisor of $x^n - \lambda$. In the case finite chain rings, the following theorem is analogous to that for Θ-λ-constacyclic codes over finite fields.

Theorem 36 (see [26, Theorem 2.2]). *Let Θ be an automorphism of $\mathscr{R}$, n an integer divisible by the order of Θ, and λ a unit in $\mathscr{R}$ which is fixed by Θ. Then the code C is a skew*

Θ-λ-*constacyclic code if and only if* C *is a left ideal* $\langle g(x)\rangle \subseteq \mathscr{R}[x;\Theta]/\langle x^n-\lambda\rangle$, *where* $g(x)$ *is a right divisor of* $x^n-\lambda$.

From this theorem, we can find a skew Θ-λ-constacyclic code as a left ideal $\langle g(x)\rangle \subseteq \mathscr{R}[x;\Theta]/\langle x^n-\lambda\rangle$, where $g(x)$ is a right divisor of $x^n-\lambda$. However, it is not easy to list all skew Θ-λ-constacyclic codes because $\mathscr{R}[x;\Theta]$ is not unique factorization ring. Therefore, there are many more right factors than in the commutative case, which in turn produces many more skew Θ-λ-constacyclic codes.

Example 37. Let $\mathscr{R} = \mathbb{F}_3 + u\mathbb{F}_3$ be a finite chain ring. We consider the automorphism $\Theta_{id,2}$ of $\mathbb{F}_3 + u\mathbb{F}_3$, where $\Theta_{id,2}(a+ub) = a+2bu$. Then we have two irreducible factorizations of x^6-1 in $(\mathbb{F}_3+u\mathbb{F}_3)[x;\Theta_{id,2}]$:

$$x^6-1 = (x+1)^3(x+2)^3 = \left(x^2+ux+2\right)^3. \tag{45}$$

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

$$G \coloneqq \begin{pmatrix} g_0 & \cdots & g_{n-k-1} & 1 & 0 & \cdots & 0 \\ 0 & \Theta(g_0) & \cdots & \Theta(g_{n-k-1}) & 1 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \Theta^2(g_{n-k-1}) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \Theta^{k-1}(g_0) & \cdots & \Theta^{k-1}(g_{n-k-1}) & 1 \end{pmatrix}. \tag{46}$$

The rows of G are linearly independent. Then we have the following result.

Proposition 38 (see [26, Proposition 3.1]). *Let* $g(x)$ *be a right divisor of* $x^n-\lambda$. *Then the* Θ-λ-*constacyclic code* C *generated by* $g(x)$ *is a free* $\mathscr{R}$-*module with* $|C| = |\mathscr{R}|^{n-\deg(g(x))}$.

Similarly, in the case of finite fields, we denote $\mathscr{R}^\Theta$, the subring of $\mathscr{R}$ fixed by Θ. Then we have the following result.

Proposition 39 (see [26, Proposition 3.2]). *Let* $g(x)$ *be a monic right divisor of* $x^n-\lambda$ *in* $\mathscr{R}[x;\Theta]$. *The skew* Θ-λ-*constacyclic code generated by* $g(x)$ *is* λ-*constacyclic if and only if* $g(x) \in \mathscr{R}^\Theta[x;\Theta]$.

Let C be a Θ-λ-constacyclic code. In the following lemma, the parity-check matrix for C is introduced.

Lemma 40 (see [26, Proposition 3.3]). *Let* C *be the* Θ-λ-*constacyclic code generated by a monic right divisor* $g(x)$ *of* $x^n-\lambda$ *and* $h(x) \coloneqq (x^n-\lambda)/g(x)$. *Then the following statements hold:*

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

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

$$H \coloneqq \begin{pmatrix} 1 & \Theta(h_{k-1}) & \cdots & \Theta^k(h_0) & 0 & \cdots & 0 \\ 0 & 1 & \Theta^2(h_{k-1}) & \cdots & \Theta^{k+1}(h_0) & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \Theta^{n-k}(h_{k-1}) & \cdots & \Theta^{n-1}(h_0) \end{pmatrix} \tag{47}$$

is a parity-check matrix for C.

In the next part, we study the Euclidean and Hermitian dual codes of skew Θ-λ-constacyclic codes over finite chain rings. Suppose that the length n of codes is divisible by the order of Θ, and λ is a unit in $\mathscr{R}$ which is fixed by Θ. Euclidean inner product is defined by $\langle u,v\rangle = \sum_{i=0}^{n-1} u_i v_i$, for $u = (u_0,u_1,\ldots,u_{n-1})$ and $v = (v_0,v_1,\ldots,v_{n-1})$ in $\mathscr{R}^n$. In special case, if the order of Θ is 2, then we can also give the Hermitian inner product, denoted by $\langle u,v\rangle_H = \sum_{i=0}^{n-1} u_i\Theta(v_i)$. If $\langle u,v\rangle = 0$ (resp., $\langle u,v\rangle_H = 0$), then u and v are called Euclidean orthogonal (resp., Hermitian orthogonal). The Euclidean and Hermitian dual code of a code C are defined to be

$$C^\perp = \{v \in \mathscr{R}^n \mid \langle v,c\rangle = 0,\ \forall c \in C\}, \tag{48}$$

$$C^{\perp_H} = \{v \in \mathscr{R}^n \mid \langle v,c\rangle_H = 0,\ \forall c \in C\}, \tag{49}$$

respectively. If $C = C^{\perp}$ ($C = C^{\perp_H}$), then C is said to be Euclidean (Hermitian) self-dual code. We get a main result which describes the relationship between a skew Θ-λ-constacyclic code and its dual.

Lemma 41 (see [26, Lemma 3.1]). *Let C be a code of length n over $\mathscr{R}$. Then C is skew 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.*

5.2. Euclidean Dual Codes. We denote that $\mathscr{R}[x;\Theta]S^{-1}$ is the right localization of $\mathscr{R}[x;\Theta]$. The following theorem will discuss the necessary and sufficient conditions for $\mathscr{R}[x;\Theta]$ to have the right localization.

Theorem 42 (see [26, Theorem 2.1]). *Let $S = \{x^i \mid i \in \mathbb{N}\}$. Then $\mathscr{R}[x;\Theta]$ has the right localization at S if and only if both the following conditions hold:*

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

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

Before determining the structure of dual codes, we get the following result.

Lemma 43 (see [26, Proposition 2.4]). *Let $\varphi : \mathscr{R}[x;\Theta] \to \mathscr{R}[x;\Theta]S^{-1}$ defined by*

$$\varphi\left(\sum_{i=0}^{k} a_i x^i\right) = \sum_{i=0}^{k} x^{-i} a_i. \tag{50}$$

Then φ is a ring antimonomorphism.

From Lemma 41, it is easy to verify that the Euclidean dual of a skew Θ-λ-constacyclic code C is again a skew Θ-λ-constacyclic code. We introduce a result about Euclidean dual codes. To do that, we need the following lemma.

Lemma 44 (see [26, Lemma 3.2]). *Assume that $\lambda^2 = 1$. 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 polynomials in $\mathscr{R}[x;\Theta]$. Then the following statements are equivalent:*

(i) *The coefficient vector of $a(x)$ is Euclidean orthogonal to the coefficient vector of $x^i(x^{n-1}\varphi(b(x)))$ for all $i \in \{0, 1, \ldots, n-1\}$, where $\varphi : \mathscr{R}[x;\Theta] \to \mathscr{R}[x;\Theta]S^{-1}$ is a ring antimonomorphism defined in Lemma 43.*

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

(iii) *$a(x)b(x) = 0$ in $\mathscr{R}[x;\Theta]/\langle x^n - \lambda\rangle$.*

Theorem 45 (see [26, Theorem 3.3]). *Assume that $\lambda^2 = 1$. Let $g(x)$ be a right divisor of $x^n - \lambda$ and $h(x) \coloneqq (x^n - \lambda)/g(x)$. Let C be the Θ-λ-constacyclic code generated by $g(x)$. Then the following statements hold:*

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

(ii) *The Euclidean dual $C^{\perp}$ is a Θ-λ-constacyclic code generated by $x^{\deg(h(x))}\varphi(h(x))$.*

Theorem 46 (see [26, Theorem 3.4]). *Assume that $\lambda^2 = 1$ 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 Euclidean self-dual if and only if*

$$\left(\sum_{i=0}^{k-1} g_i x^i + x^k\right) \cdot \left(\Theta^{-k}\left(g_0^{-1}\right) + \sum_{i=0}^{k-1} \Theta^{i-k}\left(g_0^{-1} g_{k-i}\right) x^i + x^k\right) = x^n - \lambda. \tag{51}$$

Theorem 46 provided the necessary and sufficient conditions for a skew Θ-λ-constacyclic code to be Euclidean self-dual code. By applying Theorem 46, we can see that if the order of Θ divides k and $\lambda \neq -1$, then there are no Euclidean self-dual skew constacyclic codes of length $2k$. Moreover, if Θ is the identity automorphism and $\lambda \neq -1$, then there are no Euclidean self-dual codes.

5.3. Hermitian Dual Codes. The Hermitian inner product is defined only when the order of Θ is 2. Therefore, in this subsection, we always suppose that the order of Θ is 2. We first have some characterizations of Hermitian duality.

Lemma 47 (see [26, Lemma 3.5]). *Let C be a code of length n over $\mathscr{R}$. Then C is skew 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.*

Let ϕ be a ring automorphism of $\mathscr{R}[x;\Theta]$ defined by $\phi(\sum_{i=0}^{s} a_i x^i) = \sum_{i=0}^{s} \Theta(a_i)x^i$. Then we have the following result.

Lemma 48 (see [26, Lemma 3.6]). *Assume that $\lambda^2 = 1$. 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 polynomials in $\mathscr{R}[x;\Theta]$. Then the following statements are equivalent:*

(i) *The coefficient vector of $a(x)$ is Euclidean orthogonal to the coefficient vector of $x^i\phi(x^{n-1}\varphi(b(x)))$ for all $i \in \{0, 1, \ldots, n-1\}$, where $\varphi : \mathscr{R}[x;\Theta] \to \mathscr{R}[x;\Theta]S^{-1}$ is a ring antimonomorphism defined in Lemma 43.*

(ii) *$(a_0, a_1, \ldots, a_{n-1})$ 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.*

(iii) *$a(x)b(x) = 0$ in $\mathscr{R}[x;\Theta]/\langle x^n - \lambda\rangle$.*

Theorem 49 (see [26, Theorem 3.7]). *Assume that $\lambda^2 = 1$. Let $g(x)$ be a right divisor of $x^n - \lambda$ and $h(x) \coloneqq (x^n - \lambda)/g(x)$. 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* $\phi(x^{\deg(h(x))}\varphi(h(x)))$.

Similar to the case of the Euclidean self-dual code, we have the necessary and sufficient conditions for a Θ-λ-constacyclic code to be Hermitian self-dual.

Theorem 50 (see [26, Theorem 3.8]). *Assume that* $\lambda^2 = 1$ *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*

$$\left(\sum_{i=0}^{k-1} g_i x^i + x^k\right) \cdot \left(\Theta^{-k-1}\left(g_0^{-1}\right) + \sum_{i=0}^{k-1} \Theta^{i-k-1}\left(g_0^{-1} g_{k-i}\right) x^i + x^k\right) = x^n - \lambda. \tag{52}$$

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

5.4. Skew Constacyclic Codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. The class of finite chain rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ has been used widely as alphabets in certain constacyclic codes. It has been studied by many researchers (see, for more details, [23–25, 33, 35, 38]). In recent years, we have studied constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. All constacyclic codes of length p^s over the ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are considered. The purpose of this subsection is to investigate the structure of all skew Θ-λ-constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where λ is fixed by Θ and the length n of codes is a multiple of the order of Θ. Note that the set of automorphisms of $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ forms a group under composition, denoted by $\mathrm{Aut}(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})$. The group $\mathrm{Aut}(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})$ is completely characterized by Alkhamees [37] as follows.

Theorem 51. *For* $\alpha \in \mathrm{Aut}(\mathbb{F}_{p^m})$ *and* $\beta \in \mathbb{F}_{p^m}^*$, *let*

$$\Theta_{\alpha,\beta} : \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} \tag{53}$$

be defined by

$$\Theta_{\alpha,\beta}(a + bu) = \alpha(a) + \beta\alpha(b)\, u. \tag{54}$$

Then $\mathrm{Aut}(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}) = \{\Theta_{\alpha,\beta} \mid \alpha \in \mathrm{Aut}(\mathbb{F}_{p^m}), \beta \in \mathbb{F}_{p^m}^*\}$.

In the next part, the structure of skew Θ-cyclic and negacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ is studied. We refer the readers to [26, 38] for more details.

Assume that C is a nonzero left ideal in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$. Let A be the set of all nonzero skew polynomials of minimal degree in C. Then the classifications of Θ-λ-constacyclic codes are given in terms of generators of left ideals in $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$.

Theorem 52 (see [26, Theorem 4.1]). *Let* C *and* A *be as above. Then consider the following:*

(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 such unique 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 exists 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,* $C = \langle g(x), f(x)\rangle$.

We categorize the left ideals of $(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n - \lambda\rangle$ into three types: Type LI-1 refers to the trivial ideal $(\langle 0\rangle, \langle 1\rangle)$ or a left ideal satisfying part (i) of the theorem above. Similarly, LI-2 and LI-3 refer to a left ideal satisfying Theorem 52 ((ii) and (iii)), respectively. Next, we provide some properties of left ideals of each type LI-i ($i = 1, 2, 3$.) First, we consider type LI-i by the following lemmas.

Lemma 53 (see [26, Proposition 4.1]). *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* $\mathbb{F}_{p^m}[x;\Theta]$.

Lemma 54 (see [26, Proposition 4.2]). *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* $\deg(g_1(x)) < n$.

We write $\overleftarrow{f(x)}$ to indicate that $\overleftarrow{f(x)}$ is the skew polynomial such that $f(x)u = u\overleftarrow{f(x)}$.

Lemma 55 (see [26, Proposition 4.3]). *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* $\overleftarrow{((x^n - \lambda)/f_0(x))} f_1(x)$ *in* $\mathbb{F}_{p^m}[x;\Theta]$.

Example 56. Let $\mathscr{R} = \mathbb{F}_3 + u\mathbb{F}_3$ be a finite chain ring. We consider the automorphism $\Theta_{id,2}$ of $\mathbb{F}_3 + u\mathbb{F}_3$, where $\Theta_{id,2}(a + ub) = a + 2bu$ for all $a, b \in \mathbb{F}_3$. We list all left ideals in three types LI-i ($i = 1, 2, 3$) in $(\mathbb{F}_3 + u\mathbb{F}_3)[x;\Theta_{id,2}]/\langle x^2 - 1\rangle$. All left ideals in type LI-1 are $\langle 0\rangle$, $\langle 1\rangle$, $\langle x+1\rangle$, $\langle x+2\rangle$, $\langle x+1+u\rangle$, $\langle x+$

$1+2u\rangle, \langle x+2+u\rangle, \langle x+2+2u\rangle$. All left ideals in type LI-2 are $\langle u\rangle, \langle u(x+1)\rangle, \langle u(x+2)\rangle$, and all left ideals in type LI-3 are $\langle u, x+1\rangle, \langle u, x+2\rangle$.

Applying Theorem 52, the structure of skew Θ-λ-constacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ is introduced. We have three types of the left ideals in the ring $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x;\Theta]/\langle x^n-\lambda\rangle$. From this, we study the structure of the Euclidean dual codes of skew Θ-cyclic and negacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$.

Theorem 57 (see [26, Theorem 4.2]). *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 $C^\perp = \langle x^{n-\deg(g_0(x))}\varphi((x^n-\lambda)/(g_0(x)+ug_1(x)))\rangle$.*

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

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

$$C^\perp = \left\langle x^{n-\deg(f_0(x))\varphi(((x^n-\lambda)/f_0(x))u)}, \; x^{n-\deg(g_1(x))}\varphi\left(\frac{x^n-\lambda}{g_1(x)} - um(x)\right)\right\rangle, \tag{55}$$

where $\varphi : \mathscr{R}[x;\Theta] \to \mathscr{R}[x;\Theta]S^{-1}$ defined by $\varphi(\sum_{i=0}^k a_i x^i) = \sum_{i=0}^k x^{-i}a_i$.

For Hermitian dual codes, we assume that the order of Θ is 2. We have the structure of Hermitian dual codes of skew Θ-cyclic and negacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ as follows.

Theorem 58 (see [26, Theorem 4.3]). *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 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 $C^{\perp_H} = \langle \phi(x^{n-\deg(g_0(x))}\varphi((x^n-\lambda)/(g_0(x)+ug_1(x))))\rangle$.*

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

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

$$C^\perp = \left\langle x^{n-\deg(f_0(x))}\varphi\left(\frac{x^n-\lambda}{f_0(x)}u\right), \; x^{n-\deg(g_1(x))}\varphi\left(\frac{x^n-\lambda}{g_1(x)} - u\cdot m(x)\right)\right\rangle, \tag{56}$$

where $\varphi : \mathscr{R}[x;\Theta] \to \mathscr{R}[x;\Theta]S^{-1}$ defined by $\varphi(\sum_{i=0}^k a_i x^i) = \sum_{i=0}^k x^{-i}a_i$.

Table 3

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

Note that the subscripts 1, 2, and 3 indicate the types of ideals LI-1, LI-2, and LI-3, respectively.

Finally, we give an example for Euclidean and Hermitian dual codes.

Example 59. We knew in previous example that all left ideals of type LI-1 in $(\mathbb{F}_3+u\mathbb{F}_3)[x;\Theta_{id,2}]/\langle x^2-1\rangle$ are $\langle 0\rangle, \langle 1\rangle, \langle x+1\rangle, \langle x+2\rangle, \langle x+1+u\rangle, \langle x+2+u\rangle, \langle x+1+2u\rangle, \langle x+2+2u\rangle$. Then their Euclidean dual codes are $\langle 1\rangle, \langle 0\rangle, \langle x+2\rangle, \langle x+1\rangle, \langle x+2+u\rangle, \langle x+1+u\rangle, \langle x+2+2u\rangle, \langle x+1+2u\rangle$, respectively. Similarly, Hermitian dual codes are $\langle 1\rangle, \langle 0\rangle, \langle x+2\rangle, \langle x+1\rangle, \langle x+2+2u\rangle, \langle x+2+u\rangle, \langle x+1+2u\rangle, \langle x+1+u\rangle$. All left ideals in type LI-2 are $\langle u\rangle, \langle u(x+1)\rangle, \langle u(x+2)\rangle$. The Euclidean dual codes coincided with the Hermitian dual codes of all left ideals in type LI-2. They are $\langle u\rangle, \langle u, x+2\rangle$, and $\langle u, x+1\rangle$, respectively. Similarly, the Euclidean dual codes also coincided with the Hermitian dual codes of all left ideals in type LI-3. They are $\langle u(x+1)\rangle, \langle u(x+2)\rangle$. We summarize discussion above in Table 3.

Disclosure

The main part of this paper was written during the visits of Bac T. Nguyen to Hai Q. Dinh at Department of Mathematical Sciences, Kent State University, USA, from November 2014 to January 2015, and Hai Q. Dinh to Songsak Sriboonchitta at Faculty of Economics, Chiang Mai University, Thailand, in January 2015.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors are grateful for the Department of Mathematical Sciences, Kent State University; Faculty of Economics, Chiang Mai University; and Department of Mathematics, Mahidol University, for their hospitality and financial support. The

authors' thanks are extended to the Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, for partial financial support. Bac T. Nguyen was supported by Postgraduate Student Exchange Scholarship, Mahidol University, to visit Department of Mathematical Sciences, Kent State University, USA.

Endnotes

1. Claude Elwood Shannon (April 30, 1916–February 24, 2001) was an American mathematician, electronic engineer, and cryptographer, who is refered to as "the father of information theory" [39]. Shannon is also known as the founder of both digital computer and digital circuit design theory, when, as a 21-year-old M.S. student at MIT in 1937, he wrote a thesis establishing that electrical application of Boolean algebra could construct and resolve any logical, numerical relationship [40]. It has been claimed that this was the most important M.S. thesis of all time. Shannon contributed to the field of cryptanalysis during World War II and afterwards, including basic work on code breaking.
2. Turbo codes were first introduced and developed in 1993 by Berrou et al. [41]. Turbo codes are a class of high-performance forward error correction codes, which were the first practical codes to closely approach the channel capacity, a theoretical maximum for the code rate at which reliable communication is still possible given a specific noise level. Turbo codes are widely used in deep space communications and other applications where designers seek to achieve reliable information transfer over bandwidth-constrained or latency-constrained communication links in the presence of data-corrupting noise. The first class of turbo code was the parallel concatenated convolutional code. Since the introduction of the original parallel turbo codes in 1993, many other classes of turbo code have been discovered, including serial versions and repeat-accumulate codes. Iterative turbo decoding methods have also been applied to more conventional forward error correction systems, including Reed-Solomon corrected convolutional codes.
3. LDPC (low-density parity-check) codes were first introduced in 1963 by Gallager in his doctoral dissertation at MIT [42]. At that time, it was impractical to implement and LDPC codes were forgotten, but they were rediscovered in 1996. LDPC code is a linear error correcting code, a method of transmitting a message over a noisy transmission channel, and is constructed using a sparse bipartite graph. LDPC codes are capacity-approaching codes, which means that practical constructions exist that allow the noise threshold to be set arbitrarily close on the binary erasure channel to the Shannon limit for a symmetric memoryless channel. The noise threshold defines an upper bound for the channel noise, up to which the probability of lost information can be made as small as desired. Using iterative belief propagation techniques, LDPC codes can be decoded in time linear to their block length.
4. Richard Wesley Hamming (February 11, 1915–January 7, 1998) was an American mathematician whose work had many implications for computer science and telecommunications. His contributions include the Hamming code (which makes use of a Hamming matrix), the Hamming window, Hamming numbers, sphere-packing (or Hamming bound), and the Hamming distance.
5. During the late 1940s at Bell laboratories, Richard Hamming decided that a better system was needed. As folklore has it, Richard Hamming was working for Bell Labs. He was allowed to use the computer for research over the weekends. He would put together his punch cards during the week and submit them to be run over the weekend. This would work great as long as his punch cards were completely error-free; however, a single error would cause the computer to pass the job over and move on to the next. He would have to make corrections and resubmit his program at a later time. Richard Hamming thought that if the computer was smart enough to know that there was a mistake, why not have the computer find the mistake, correct it, and continue running the program. He then created the first error correction code, the Hamming Code. This not only solved an important problem in telecommunications and computer science, it opened up a whole new field of study.

References

[1] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[2] R. W. Hamming, "Error detecting and error correcting codes," *The Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[3] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew-cyclic codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 18, no. 4, pp. 379–389, 2007.

[4] E. Prange, "Cyclic error-correcting codes in two symbols," Tech. Rep. TN-57-103, Air Force Cambridge Research Labs, 1957.

[5] E. Prange, "Some cyclic error-correcting codes with simple decoding algorithms," Tech. Rep. TN-58-156, Air Force Cambridge Research Center, 1958.

[6] E. Prange, "The use of coset equivalence in the analysis and decoding of group codes," Tech. Rep. TN-59-164, 1959.

[7] E. Prange, "An algorithm for factoring xn1 over a finite field," Tech. Rep. TN-59-175, 1959.

[8] E. R. Berlekamp, "Negacyclic codes for the Lee metric," in *Proceedings of the Conference on Combinatorial Mathematics and Its Applications*, pp. 298–316, University of North Carolina Press, Chapel Hill, NC, USA, 1968.

[9] E. R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, 1984.

[10] S. D. Berman, "Semisimple cyclic and Abelian codes. II," *Kibernetika*, vol. 3, pp. 21–30, 1967 (Russian), Translated as: *Cybernetics*, vol. 3, pp. 17–23, 1967.

[11] J. L. Massey, D. J. Costello, and J. Justesen, "Polynomial weights and code constructions," *IEEE Transactions on Information Theory*, vol. 19, pp. 101–110, 1973.

[12] G. Falkner, B. Kowol, W. Heise, and E. Zehendner, "On the existence of cyclic optimal codes," *Atti del Seminario Matematico e Fisico dell'Universita di Modena*, vol. 28, no. 2, pp. 326–341, 1979.

[13] R. M. Roth and G. Seroussi, "On cyclic MDS codes of length q over GF(q)," *IEEE Transactions on Information Theory*, vol. 32, no. 2, pp. 284–285, 1986.

[14] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, "On repeated-root cyclic codes," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 337–342, 1991.

[15] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 343–345, 1991.

[16] D. Boucher, P. Solé, and F. Ulmer, "Skew constacyclic codes over Galois rings," *Advances in Mathematics of Communications*, vol. 2, no. 3, pp. 273–292, 2008.

[17] D. Boucher and F. Ulmer, "A note on the dual codes of module skew codes," in *Cryptography and Coding*, vol. 7089 of *Lecture Notes in Computer Science*, pp. 230–243, Springer, Berlin, Germany, 2011.

[18] D. Boucher and F. Ulmer, "Self-dual skew codes and factorization of skew polynomials," *Journal of Symbolic Computation*, vol. 60, pp. 47–61, 2014.

[19] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa, and M. Oura, "Type II codes over $F_2 + 11F_2$ and applications to Hermitian modular forms," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 73, no. 1, pp. 13–42, 2003.

[20] M. M. Al-Ashker, "Simplex codes over the ring $F_2 + uF_2$," *The Arabian Journal for Science and Engineering, Section A: Sciences*, vol. 30, no. 24, pp. 277–285, 2005.

[21] W. C. Huffman, "On the decomposition of self-dual codes over $F_2 + uF_2$ with an automorphism of odd prime order," *Finite Fields and their Applications*, vol. 13, no. 3, pp. 681–712, 2007.

[22] I. Siap, "Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and their complete weight enumerators," in *Codes and Designs, Columbus, OH, 2000*, vol. 10 of *Ohio State University Mathematical Research Institute Publications*, pp. 259–271, De Gruyter, Berlin, Germany, 2002.

[23] A. Bonnecaze and P. Udaya, "Cyclic codes and self-dual codes over F_2+uF_2," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1250–1255, 1999.

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

[25] H. Q. Dinh, "Constacyclic codes of length 2^s over Galois extension rings of $BBF_2 + uBBF_2$," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1730–1740, 2009.

[26] S. Jitman, S. Ling, and P. Udomkavanich, "Skew constacyclic codes over finite chain rings," *Advances in Mathematics of Communications*, vol. 6, no. 1, pp. 39–63, 2012.

[27] V. Pless and W. C. Huffman, *Handbook of Coding Theory*, Elsevier, Amsterdam, The Netherlands, 1998.

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

[29] D. Boucher and F. Ulmer, "Coding with skew polynomial rings," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1644–1656, 2009.

[30] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system I: the user language," *Journal of Symbolic Computation*, vol. 24, no. 3-4, pp. 235–265, 1997.

[31] S. A. Vanstone and P. C. van Oorschot, *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic, 1989.

[32] H. Q. Dinh and S. R. López-Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1728–1744, 2004.

[33] M. C. V. Amarra and F. R. Nemenzo, "On $(1u)$- cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$," *Applied Mathematics Letters*, vol. 21, no. 11, pp. 1129–1133, 2008.

[34] G. H. Norton and A. Sălăgean, "On the structure of linear and cyclic codes over a finite chain ring," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, no. 6, pp. 489–506, 2000.

[35] J. F. Qian, L. N. Zhang, and S. X. Zhu, "$(1 + u)$ constacyclic and cyclic codes over $F_2 + uF_2$ constacyclic and cyclic codes over," *Applied Mathematics Letters*, vol. 19, no. 8, pp. 820–823, 2006.

[36] R. Sobhani and M. Esmaeili, "Cyclic and negacyclic codes over the Galois ring GR(p^2, m)," *Discrete Applied Mathematics*, vol. 157, no. 13, pp. 2892–2903, 2009.

[37] Y. Alkhamees, "The determination of the group of automorphisms of a finite chain ring of characteristic p," *The Quarterly Journal of Mathematics*, vol. 42, no. 1, pp. 387–391, 1991.

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

[39] I. James, "Claude elwood shannon 30 April 1916–24 February 2001," *Biographical Memoirs of Fellows of the Royal Society*, vol. 55, pp. 257–265, 2009.

[40] C. E. Shannon, *A symbolic analysis of relay and switching circuits [M.S. thesis]*, Massachusetts Institute of Technology, Cambridge, Mass, USA, 1937.

[41] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo-codes," in *Proceedings of the IEEE International Conference on Communications*, pp. 1064–1070, Geneva, Switzerland, May 1993.

[42] R. G. Gallager, *Low Density Parity-Check Codes*, MIT Press, Cambridge, Mass, USA, 1963.