

SKEW CONSTACYCLIC CODES OVER FINITE COMMUTATIVE SEMI-SIMPLE RINGS

HAI Q. DINH, BAC TRONG NGUYEN, AND SONGSAK SRIBOONCHITTA

ABSTRACT. This paper investigates skew Θ - λ -constacyclic codes over $R = \mathbf{F}_0 \oplus \mathbf{F}_1 \oplus \cdots \oplus \mathbf{F}_{k-1}$, where \mathbf{F}_i 's are finite fields. The structures of skew λ -constacyclic codes over finite commutative semi-simple rings and their duals are provided. Moreover, skew λ -constacyclic codes of arbitrary length are studied under a new definition. We also show that a skew cyclic code of arbitrary length over finite commutative semi-simple rings is equivalent to either a cyclic code over R or a quasi-cyclic code over R .

1. Introduction

It has been shown that skew polynomial rings are an important class of non-commutative rings. In 2007, D. Boucher et al. [3] initiated the study of skew cyclic codes. They generalized the notion of cyclic codes by using generator polynomials in noncommutative skew polynomial rings. The principle motivation for studying codes in this setting is that polynomials in skew polynomial rings have more factorizations than that in the commutative case. In 2009 and 2011, motivated by the work in 2007, D. Boucher and F. Ulmer ([4] and [6]) continued to study skew Θ - λ -constacyclic codes over Galois rings and codes as modules over skew polynomial rings.

In [4], D. Boucher, P. Sole and F. Ulmer 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. D. Boucher and F. Ulmer also studied the factorization of skew polynomial in skew polynomial rings [7]. These results allowed them to study the skew self-dual cyclic codes with length 2^s .

Received April 4, 2018; Revised October 18, 2018; Accepted January 8, 2019.

2010 *Mathematics Subject Classification.* Primary 94B15, 94B05; Secondary 11T71.

Key words and phrases. cyclic codes, constacyclic codes, dual codes, skew Θ -cyclic codes, skew Θ -negacyclic codes, skew Θ - λ -constacyclic codes.

The class of finite rings of the form $\mathbf{F}_{p^m} + u\mathbf{F}_{p^m}$ has been widely used as alphabets of certain constacyclic codes. For example, the structure of $\mathbf{F}_2 + u\mathbf{F}_2$ is interesting, it is lying between \mathbf{F}_4 and \mathbb{Z}_4 in the sense that it is additively analogous to \mathbf{F}_4 , and multiplicatively analogous to \mathbb{Z}_4 . It has been studied by a lot of researchers (see, for example, [1, 2, 17]).

In 2009, I. Siap et al. developed the study of skew codes by presenting the structures of skew cyclic codes of arbitrary length [16]. Further, in 2012, Jitman et al. [14] introduced the notion of skew Θ - λ -constacyclic (briefly, skew constacyclic) 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.

More recently, codes over rings are a very important class and many types of codes with good parameters can be constructed over rings. J. Gao [11] and F. Gursoy et al. [13] determined skew cyclic codes over $\mathbf{F}_p + v\mathbf{F}_p$ and $\mathbf{F}_q + v\mathbf{F}_q$ with different automorphisms. In addition, skew generalized quasi-cyclic codes over finite fields are also studied by J. Gao [12]. In a recent paper [9], we established successfully constacyclic codes over semi-simple rings. As a generalization of constacyclic codes over semi-simple rings [10], the aim of this paper is to study skew Θ -constacyclic codes over finite commutative semi-simple rings.

This paper is arranged as follows. Basic concepts are reviewed in Section 2. After presenting preliminary concepts in Section 2, we study algebraic structures of skew Θ - λ -constacyclic codes over finite commutative semi-simple rings in Section 3. The dual codes of skew Θ - λ -constacyclic codes over finite commutative semi-simple rings are investigated in Section 4. Finally, in the Section 5, we consider the structure of skew Θ - λ -constacyclic codes over finite commutative semi-simple rings for arbitrary length.

2. Preliminaries

We first recall the definition of skew Θ - λ -constacyclic codes over finite fields.

Definition 2.1. Given an automorphism Θ of \mathbf{F}_{p^m} and a unit λ in \mathbf{F}_{p^m} , a linear code C is said to be a *skew Θ - λ -constacyclic* of length n if it is closed under the skew Θ - λ -constacyclic shift $\tau_{\Theta, \lambda} : \mathbf{F}_{p^m}^n \rightarrow \mathbf{F}_{p^m}^n$ defined by

$$\tau_{\Theta, \lambda}(c_0, c_1, \dots, c_{n-1}) = (\Theta(\lambda c_{n-1}), \Theta(c_0), \dots, \Theta(c_{n-2})).$$

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 a $[n, k]$ linear code. While the ring $\mathbf{F}_{p^m}[x]$ is a commutative ring, so every ideals of $\mathbf{F}_{p^m}[x]$ is two-sided ideals, the skew polynomial ring $\mathbf{F}_{p^m}[x; \Theta]$ 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 $\mathbf{F}_{p^m}[x; \Theta]$.

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 $\mathbf{F}_{p^m}[x; \Theta]$. If Θ is not the identity, then $\mathbf{F}_{p^m}[x; \Theta]$ 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.

Lemma 2.2 ([3, Lemma 1]). *Let Θ be an automorphism of \mathbf{F}_{p^m} , n an integer divisible by the order of Θ , and λ a unit in \mathbf{F}_{p^m} which is fixed by Θ . The ring $\frac{\mathbf{F}_{p^m}[x; \Theta]}{\langle x^n - \lambda \rangle}$ 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 $\mathbf{F}_{p^m}[x; \Theta]$.*

The following result is considered as a generalization of Lemma 1 and Theorem 1 in [3].

Theorem 2.3 (Extended Theorem 1 of [3]). *Let Θ be an automorphism of \mathbf{F}_{p^m} , and n an integer divisible by the order of Θ , and λ a unit in \mathbf{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 $\langle g(x) \rangle \subseteq \frac{\mathbf{F}_{p^m}[x; \Theta]}{\langle x^n - \lambda \rangle}$, where $g(x)$ is a right divisor of $x^n - \lambda$.*

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

Proposition 2.4 ([14, Proposition 3.1]). *Let C be a skew Θ - λ -cyclic code of length n over \mathbf{F}_q generated by a right divisor $g(x) = \sum_{i=0}^{n-k-1} g_i x^i + x^{n-k}$ of $x^n - \lambda$. Then the generator matrix of C is given by*

$$G := \begin{pmatrix} g_0 & \cdots & g_{n-k-1} & 1 & 0 & \cdots & 0 \\ 0 & \Theta(g_0) & \cdots & \Theta(g_{n-k-1}) & 1 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \Theta^2(g_{n-k-1}) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \Theta^{k-1}(g_0) & \cdots & \Theta^{k-1}(g_{n-k-1}) & 1 \end{pmatrix}$$

and $|C| = q^{n-\deg(g(x))}$.

Lemma 2.5 ([5, Lemma 17]). *Let Θ be an automorphism of \mathbf{F}_{p^m} , and n an integer divisible by the order of Θ , and λ a unit in \mathbf{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 $h(x) := \frac{x^n - \lambda}{g(x)}$. If $h = h_0 + h_1 x + \cdots + x^{n-r}$, then the following matrix*

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

is a parity-check matrix for C .

For skew Θ -negacyclic and skew Θ -cyclic codes, the following two corollaries are direct consequences of Theorem 2.3.

Corollary 2.6 ([3, Lemma 1]). *Let Θ be an automorphism of \mathbf{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 $\langle g(x) \rangle \subseteq \frac{\mathbf{F}_{p^m}[x;\Theta]}{\langle x^n - 1 \rangle}$, where $g(x)$ is a right divisor of $x^n - 1$.*

Corollary 2.7. *Let Θ be an automorphism of \mathbf{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 $\langle g(x) \rangle \subseteq \frac{\mathbf{F}_{p^m}[x;\Theta]}{\langle x^n + 1 \rangle}$, where $g(x)$ is a right divisor of $x^n + 1$.*

3. Structures of skew constacyclic codes over finite commutative semi-simple rings

In this section, we study skew λ -constacyclic codes over finite commutative semi-simple rings. We now consider the semi-simple ring $R = \mathbf{F}_0 \oplus \mathbf{F}_1 \oplus \cdots \oplus \mathbf{F}_{k-1}$, where \mathbf{F}_i 's are finite fields. Since $R = \mathbf{F}_0 \oplus \mathbf{F}_1 \oplus \cdots \oplus \mathbf{F}_{k-1}$, the unit λ of R is uniquely expressed as

$$\lambda = (\lambda_0, \dots, \lambda_{k-1}).$$

Assume that Θ is an automorphism of R . Then Θ can be written as $\Theta = (\Theta_0, \dots, \Theta_{k-1})$, where Θ_i is an automorphism of \mathbf{F}_i .

Proposition 3.1. *The order of Θ is the least common multiple of the orders of Θ_i for all $i = 0, \dots, k - 1$.*

Proof. Assume that the least common multiple of the orders of Θ_i is t . For any unit $\lambda = (\lambda_0, \dots, \lambda_{k-1})$ of R , we can see that

$$\Theta(\lambda) = (\Theta_0(\lambda_0), \Theta_1(\lambda_1), \dots, \Theta_{k-1}(\lambda_{k-1})).$$

This implies that $\Theta^t(\lambda) = (\Theta_0^t(\lambda_0), \Theta_1^t(\lambda_1), \dots, \Theta_{k-1}^t(\lambda_{k-1}))$. Since t is the least common multiple of the orders of Θ_i , we have

$$\Theta^t(\lambda) = (\Theta_0^t(\lambda_0), \Theta_1^t(\lambda_1), \dots, \Theta_{k-1}^t(\lambda_{k-1})) = (\lambda_0, \lambda_1, \dots, \lambda_{k-1}).$$

Suppose that $\Theta^u(\lambda) = \lambda$. We must show that u is an integer divisible by t . Indeed, since $\Theta^u(\lambda) = \lambda$, it follows that u is an integer divisible by the orders of Θ_i for all $i = 0, \dots, k - 1$. Hence, u is an integer divisible by t , proving that t is the order of Θ . \square

Proposition 3.2. *Assume that Θ is an automorphism of R . Then $\lambda = (\lambda_0, \dots, \lambda_{k-1})$ is a unit of R fixed by Θ if and only if λ_i is fixed by Θ_i for all $i = 0, \dots, k - 1$.*

Proof. It is routine to check. \square

Assume that Θ is an automorphism of R and n is an integer divisible by the order of Θ . If λ is a unit in R which is fixed by Θ , then it is readily to check that the map

$$\phi : \frac{R[x, \Theta]}{\langle x^n - \lambda \rangle} \longrightarrow \bigoplus_{i=0}^{k-1} \frac{\mathbf{F}_i[x, \Theta_i]}{\langle x^n - \lambda_i \rangle}$$

given by

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mapsto (a_{0,0} + a_{0,1}x + \cdots + a_{0,n-1}x^{n-1}, \dots, a_{k-1,0} + a_{k-1,1}x + \cdots + a_{k-1,n-1}x^{n-1})$$

is a ring isomorphism. Hence, the ring $\frac{R[x, \Theta]}{\langle x^n - \lambda \rangle}$ can be decomposed as

$$\frac{R[x, \Theta]}{\langle x^n - \lambda \rangle} \cong \bigoplus_{i=0}^{k-1} \frac{\mathbf{F}_i[x, \Theta_i]}{\langle x^n - \lambda_i \rangle}.$$

This implies that C is a left ideal of $\frac{R[x, \Theta]}{\langle x^n - \lambda \rangle}$ if and only if C can be expressed as $C = \bigoplus_{i=0}^{k-1} C_i$, where C_i is a left ideal of $\frac{\mathbf{F}_i[x, \Theta_i]}{\langle x^n - \lambda_i \rangle}$. We refer to this as the standard representation of C .

Proposition 3.3. *Let Θ be an automorphism of R , and n an integer divisible by the order of Θ and λ a unit in R which is fixed by Θ .*

- (i) *Let C be a skew Θ - λ -constacyclic code over R . Then the skew Θ - λ -constacyclic code C has the form $C = \bigoplus_{i=0}^{k-1} C_i$, where C_i is a skew Θ_i - λ_i -constacyclic code of length n over \mathbf{F}_i ($i = 0, \dots, k - 1$). Moreover, the skew Θ - λ -constacyclic C is a linear code over R if and only if the skew Θ - λ -constacyclic code C_i is a linear code over \mathbf{F}_i .*
- (ii) *Let $\lambda = (\lambda_0, \dots, \lambda_{k-1})$ be a unit of R . A skew Θ - λ -code $C = \bigoplus_{i=0}^{k-1} C_i$ is a skew Θ - λ -constacyclic code of length n over R if and only if each code C_i is a skew Θ_i - λ_i -constacyclic code of length n over \mathbf{F}_i .*

Proof. (i) Since $\lambda = (\lambda_0, \dots, \lambda_{k-1})$ is fixed by $\Theta = (\Theta_0, \dots, \Theta_{k-1})$, then λ_i is a unit in \mathbf{F}_i fixed by Θ_i , where $i = 0, \dots, k - 1$. It is well-known that $\phi : \frac{R[x, \Theta]}{\langle x^n - \lambda \rangle} \longrightarrow \bigoplus_{i=0}^{k-1} \frac{\mathbf{F}_i[x, \Theta_i]}{\langle x^n - \lambda_i \rangle}$ is a ring isomorphism. Hence, $C = \bigoplus_{i=0}^{k-1} C_i$, where C_i is a skew Θ_i - λ_i constacyclic code over \mathbf{F}_i ($i = 0, \dots, k - 1$). Then, it is easy to verify that the skew Θ - λ -constacyclic C is a linear code of length n over R if and only if the skew Θ_i - λ_i -constacyclic code C_i is a linear code of length n over \mathbf{F}_i ($i = 0, \dots, k - 1$).

(ii) Consider any codeword $(c_0, c_1, \dots, c_{k-1}) \in C$, where $c_i = (c_{i,0}, \dots, c_{i,n-1}) \in C_i$. Since

$$\begin{aligned} \lambda c_{n-1} &= (\lambda_0, \lambda_1, \dots, \lambda_{k-1})(c_{n-1,0}, c_{n-1,1}, \dots, c_{n-1,k-1}) \\ &= (\lambda_0 c_{n-1,0}, \dots, \lambda_{k-1} c_{n-1,k-1}), \end{aligned}$$

we have

$$(\Theta(\lambda c_{n-1}), c_0, \dots, c_{n-2}) = \Theta_0(\lambda_0 c_{n-1,0}), c_{0,0}, \dots, c_{n-2,0}$$

$$\begin{aligned} & \oplus (\Theta_1(\lambda_1 c_{n-1,1}), c_{0,1}, \dots, c_{n-2,1}) \cdots \\ & \oplus (\Theta_{k-1}(\lambda_{k-1} c_{n-1,k-1}), c_{0,k-1}, \dots, c_{n-2,k-1}). \end{aligned}$$

Therefore, C is a skew Θ - λ -constacyclic code of length n over R if and only if C_i is a skew Θ_i - λ_i -constacyclic code of length n over \mathbf{F}_i . \square

For a skew Θ - λ -constacyclic code $C = \bigoplus_{i=0}^{k-1} C_i$ of length n over R , the code C_i ($i = 0, \dots, k-1$) is a skew Θ_i - λ_i -constacyclic code of length n over the field \mathbf{F}_i , so C_i is a principal left ideal of the ring $\frac{\mathbf{F}_i[x, \Theta]}{\langle x^n - \lambda_i \rangle}$ generated by right factors of $x^n - \lambda_i$, say $C_i = \langle g_i(x) \rangle$. Let $g(x) = (g_0(x), \dots, g_k(x)) \in R[x, \Theta]$, then it is straightforward to see that $C = \langle g(x) \rangle$. Moreover, a generator matrix of C is $G := \begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ G_{k-1} \end{pmatrix}$, where the matrices G_i are generator matrices of C_i for all $i = 0, \dots, k-1$. One can also deduce an expression for the parity check matrix of skew Θ - λ -constacyclic code C as follows: $H := \begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_{k-1} \end{pmatrix}$, where the matrices H_i are the parity check matrices of skew Θ_i λ_i -constacyclic codes C_i for all $i = 0, \dots, k-1$.

Thus, we have the following result.

Proposition 3.4. *Let Θ be an automorphism of R , and n an integer divisible by the order of Θ and λ a unit in R which is fixed by Θ . Suppose that $C = \bigoplus_{i=0}^{k-1} C_i$ is a skew Θ - λ -constacyclic code of length n over R , where each C_i is a skew Θ_i - λ_i -constacyclic code of length n over \mathbf{F}_i . Then*

- (i) $C = \langle (g_0(x), \dots, g_{k-1}(x)) \rangle$, where $g_0(x), \dots, g_{k-1}(x)$ are the generator polynomials of C_i ($i = 0, \dots, k-1$).
- (ii) C is generated by $g(x) = (g_0(x), \dots, g_{k-1}(x))$. In particular, $\frac{R[x, \Theta]}{\langle x^n - \lambda \rangle}$ is a principal left ideal ring.
- (iii) Suppose that C is generated by $g(x) = (g_0(x), \dots, g_{k-1}(x))$, where $\deg g_i(x) = r_i$ ($i = 0, \dots, k-1$). Then C has the following generator matrix:

$$G := \begin{pmatrix} g_0(x) & & & & \\ & xg_0(x) & & & \\ & & \ddots & & \\ & & & x^{n-r_0-1}g_0(x) & \\ g_1(x) & & & & \\ & xg_1(x) & & & \\ & & \ddots & & \\ & & & x^{n-r_1-1}g_1(x) & \\ \vdots & \vdots & \vdots & \vdots & \\ g_{k-1}(x) & & & & \\ & xg_{k-1}(x) & & & \\ & & \ddots & & \\ & & & x^{n-r_{k-1}-1}g_{k-1}(x) & \end{pmatrix}$$

Lemma 3.5. *Let $\alpha = (\alpha_0, \dots, \alpha_{k-1})$ and $\beta = (\beta_0, \dots, \beta_{k-1})$ be distinct nonzero unit elements of the R fixed by $\Theta = (\Theta_0, \dots, \Theta_{k-1})$, where $\Theta = (\Theta_0, \dots, \Theta_{k-1})$ is a ring automorphism of R . Then C is both skew α - and β -constacyclic if and only if each C_i is both skew α_i - and β_i -constacyclic.*

Proof. It is a direct consequence of Proposition 3.3. □

4. Dual codes

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

$$x \circ y = x_0y_0 + x_1y_1 + \dots + x_{n-1}y_{n-1},$$

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

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

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. [5]).

Lemma 4.1 ([5, Corollary 18]). *Let Θ be an automorphism of \mathbf{F}_{p^m} , and n an integer divisible by the order of Θ , and λ a unit in \mathbf{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 $h(x)g(x) = x^n - \lambda$. The dual of the skew Θ - λ -cyclic code generated by $g(x)$ in $\frac{\mathbf{F}_{p^m}[x; \Theta]}{\langle x^n - \lambda \rangle}$ is the skew Θ - λ -cyclic code generated by*

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

Theorem 4.2. *Let Θ be an automorphism of R , and n an integer divisible by the order of Θ and λ a unit in R which is fixed by Θ . If $C = \bigoplus_{i=0}^{k-1} C_i$ is a skew Θ - λ -constacyclic code of length n over R generated by*

$$g(x) = (g_0(x), \dots, g_{k-1}(x)),$$

then the dual of skew Θ - λ -cyclic code is generated by

$$g^\perp(x) = (g_0^\perp(x), \dots, g_{k-1}^\perp(x)).$$

Proof. It is straightforward from Proposition 3.3 and Lemma 4.1. □

It is well-known in [14] that C is a skew Θ - λ -constacyclic code over \mathbf{F}_{p^m} if and only if C^\perp is a skew Θ - λ^{-1} -constacyclic code over \mathbf{F}_{p^m} . The following result is used to characterize the dual code of a skew Θ - λ -constacyclic code over R .

Proposition 4.3. *Let Θ be an automorphism of R , and n an integer divisible by the order of Θ and λ a unit in R which is fixed by Θ . If $C = \bigoplus_{i=0}^{k-1} C_i$ is a skew Θ - λ -constacyclic code of length n over R , then the dual code of skew Θ - λ -constacyclic code C is a skew Θ - λ^{-1} -constacyclic code and $C^\perp = \bigoplus_{i=0}^{k-1} C_i^\perp$.*

Proof. Let $(x_0, x_1, \dots, x_{k-1})$ be arbitrary in $\bigoplus_{i=0}^{k-1} C_i^\perp$, i.e., $x_i \in C_i^\perp$. For any codeword $(c_0, c_1, \dots, c_{k-1}) \in C$, $c_i \in C_i$, so $x_i c_i = 0$, and hence,

$$(x_0, x_1, \dots, x_{k-1}) \cdot (c_0, c_1, \dots, c_{k-1}) = x_0 c_0 + x_1 c_1 + \dots + x_{k-1} c_{k-1} = 0.$$

It follows that $(x_0, x_1, \dots, x_{k-1}) \in C^\perp$. Thus, $\bigoplus_{i=0}^{k-1} C_i^\perp \subseteq C^\perp$. On the other hand,

$$|C^\perp| = \frac{|R|^n}{|C|} = \frac{\left(\prod_{i=0}^{k-1} q_i\right)^n}{\prod_{i=0}^{k-1} |C_i|} = \prod_{i=0}^{k-1} \frac{q_i^n}{|C_i|} = \prod_{i=0}^{k-1} |C_i^\perp| = \left|\bigoplus_{i=0}^{k-1} C_i^\perp\right|.$$

Therefore, $C^\perp = \bigoplus_{i=0}^{k-1} C_i^\perp$. \square

The following result is well-known from [8].

Proposition 4.4 ([8, Proposition 2.5]). *Let α, β be distinct nonzero elements of the field \mathbf{F} . Then a linear code C of length n over \mathbf{F} is both α - and β -constacyclic if and only if $C = \{0\}$ or $C = \mathbf{F}^n$.*

Using Proposition 4.4, we have the following result.

Theorem 4.5. *Let α, β be distinct nonzero elements of the field \mathbf{F} fixed by Θ , where Θ is an automorphisms of \mathbf{F} . Assume that n is an integer divisible by the order of Θ . Then a skew Θ - α - and β -linear code C of length n over \mathbf{F} is both skew Θ - α - and β -constacyclic if and only if $C = \{0\}$ or $C = \mathbf{F}^n$.*

Proof. (\Leftarrow) is obvious.

To prove (\Rightarrow), we assume that C is a non-zero code of length n over \mathbf{F} , and C is both skew α - and β -constacyclic. Hence, there exists a codeword with a nonzero entry in C . Without loss of generality, assume that $(c_0, c_1, \dots, c_{n-1}) \in C$, where $c_{n-1} \neq 0$. Since C is both skew α - and β -constacyclic, we can see that $(\Theta(\alpha c_{n-1}), \Theta(c_0), \dots, \Theta(c_{n-2}))$ and $(\Theta(\beta c_{n-1}), \Theta(c_0), \dots, \Theta(c_{n-2}))$ belong to C . Therefore, $(1, 0, \dots, 0) \in C$. Because $(1, 0, \dots, 0)$ and all its shifts give a basis for \mathbf{F}^n , implying that $C = \mathbf{F}^n$. \square

The Hermitian inner product is defined as

$$x \circ_{\mathbf{F}_{q^2}} y = x_0 \bar{y}_0 + x_1 \bar{y}_1 + \dots + x_{n-1} \bar{y}_{n-1},$$

where $x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in \mathbf{F}_{q^2}^n$ and $\bar{y}_i = y_i^q$. The Hermitian dual code of C is defined as

$$C^{\perp H} = \left\{ x \in \mathbf{F}_{q^2}^n \mid \sum_{i=0}^{n-1} x_i \bar{y}_i = 0, \forall y \in C \right\}.$$

If $C \subseteq C^{\perp H}$, then C is called a *Hermitian self-orthogonal* code. The code C satisfying $C^{\perp H} \subseteq C$ is called a *Hermitian dual-containing* code. Hermitian dual-containing codes are also known as weakly Hermitian self-dual codes. If $C^{\perp H} = C$, then C is called a *Hermitian self-dual* code. It is easy to see that $\{0\}$ is a Hermitian self-orthogonal code and $\mathbf{F}_{q^2}^n$ is a Hermitian dual-containing

code, which are referred to as the trivial Hermitian self-orthogonal and trivial Hermitian dual-containing codes, respectively.

For a nonempty subset V of $\mathbf{F}_{q^2}^n$, we define V^q to be the set

$$V^q = \{(v_0^q, v_1^q, \dots, v_{n-1}^q) : (v_0, v_1, \dots, v_{n-1}) \in V\}.$$

It is well-known from [9] that $|V| = |V^q|$. If C is a q^2 -ary linear code, then C^q is also a q^2 -ary linear code, and by definition, $C^{\perp_H} = (C^\perp)^q$. Since $|C^\perp| = |(C^\perp)^q|$, it follows that $|C^{\perp_H}| = |C^\perp|$, i.e., $|C||C^{\perp_H}| = q^{2n}$. Furthermore, it is easy to check that $(C^{\perp_H})^{\perp_H} = C$. Since the Hermitian inner product over \mathbf{F}_q is only defined when q is a square, hereafter, we only consider finite fields whose cardinalities are even powers of primes. From now on, our finite commutative semi-simple rings are of the form $\mathcal{R} = \mathbf{F}_0 \oplus \mathbf{F}_1 \oplus \dots \oplus \mathbf{F}_{k-1}$, where $\mathbf{F}_i = \mathbf{F}_{q_i^2}$ for all $i = 0, \dots, k - 1$.

Recall that $x_i \circ_{\mathbf{F}_i} y_i$ denotes the Hermitian inner product over \mathbf{F}_i for all $i = 0, \dots, k - 1$. Then the Hermitian inner product over \mathcal{R} is defined as

$$\begin{aligned} x \circ_{\mathcal{R}} y &= (x_0, \dots, x_{k-1}) \circ_{\mathcal{R}} (y_0, \dots, y_{k-1}) \\ &= (x_0 \circ_{\mathbf{F}_0} y_0, x_1 \circ_{\mathbf{F}_1} y_1, \dots, x_{k-1} \circ_{\mathbf{F}_{k-1}} y_{k-1}), \end{aligned}$$

where $x_i = (x_{i,0}, x_{i,1}, \dots, x_{i,n-1})$, $y_i = (y_{i,0}, y_{i,1}, \dots, y_{i,n-1})$ for all $i = 0, \dots, k - 1$. The Hermitian dual code of C is defined as

$$\begin{aligned} C^{\perp_H} &= \{x \in \mathcal{R}^n \mid x \circ_{\mathcal{R}} y = (x_0 \circ_{\mathbf{F}_0} y_0, x_1 \circ_{\mathbf{F}_1} y_1, \dots, x_{k-1} \circ_{\mathbf{F}_{k-1}} y_{k-1}) \\ &= 0_{\mathcal{R}}, \forall y \in C\}. \end{aligned}$$

A skew code is called *skew linear code with complementary dual* if $C \cap C^\perp = 0$. In particular, a code is called a *linear code with complementary dual*, or an LCD code if $C \cap C^\perp = 0$. The concept of LCD code was first given by Massey [15] in 1992. We get the following result for the case of Hermitian dual codes.

Proposition 4.6. *Let Θ be an automorphism of R , and n an integer divisible by the order of Θ and λ a unit in R which is fixed by Θ . Suppose that $C = \bigoplus_{i=0}^{k-1} C_i$ is a skew Θ - λ -constacyclic code of length n over R . Then the following statements hold:*

- (i) *For any skew Θ - λ -constacyclic code $C = \bigoplus_{i=0}^{k-1} C_i$ of length n over \mathcal{R} , its Hermitian dual code is $C^{\perp_H} = \bigoplus_{i=0}^{k-1} C_i^{\perp_H}$.*
- (ii) *C is skew Θ - λ -Hermitian self-dual if and only if C_i are skew Θ_i - λ_i -Hermitian self-dual for all $i = 0, \dots, k - 1$.*
- (iii) *C is Hermitian self-orthogonal if and only if C_i are skew Θ_i - λ_i -Hermitian self-orthogonal for all $i = 0, \dots, k - 1$.*
- (iv) *C is skew Θ - λ -Hermitian dual-containing if and only if C_i are skew Θ_i - λ_i -Hermitian dual-containing for all $i = 0, \dots, k - 1$.*
- (v) *C is skew Θ - λ -Hermitian LCD if and only if C_i are skew Θ_i - λ_i -Hermitian LCD for all $i = 0, \dots, k - 1$.*
- (vi) *For any skew Θ -linear code C of length n over \mathcal{R} , $|C||C^{\perp_H}| = |\mathcal{R}^n|$.*

Proof. We first prove the part (i). The proof of part (ii), (iii), (iv) and (v) are straightforward to see from (i). Let $(x_0, x_1, \dots, x_{k-1})$ be arbitrary in $\bigoplus_{i=0}^{k-1} C_i^{\perp H}$. That means, for $0 \leq i \leq k-1$, $x_i \in C_i^{\perp H}$, and hence, for any $c = (c_0, c_1, \dots, c_{k-1}) \in C$,

$$\begin{aligned} x \circ_{\mathcal{R}} c &= (x_0, x_1, \dots, x_{k-1}) * (\bar{c}_0, \bar{c}_1, \dots, \bar{c}_{k-1}) \\ &= (x_0 \circ_{\mathbf{F}_0} \bar{c}_0, x_1 \circ_{\mathbf{F}_1} \bar{c}_1, \dots, x_{k-1} \circ_{\mathbf{F}_{k-1}} \bar{c}_{k-1}) = 0_{\mathcal{R}}, \end{aligned}$$

implying $(x_0, x_1, \dots, x_{k-1}) \in C^{\perp H}$. This shows that $\bigoplus_{i=0}^{k-1} C_i^{\perp H} \subseteq C^{\perp H}$. On the other hand, for all $x = (x_0, \dots, x_{k-1}) \in C^{\perp H}$, we have

$$(x_0, \dots, x_{k-1}) * (\bar{y}_0, \dots, \bar{y}_{k-1}) = (x_0 \circ_{\mathbf{F}_0} \bar{y}_0, \dots, x_{k-1} \circ_{\mathbf{F}_{k-1}} \bar{y}_{k-1}) = 0_{\mathcal{R}}$$

for all $y = (y_0, y_1, \dots, y_{k-1}) \in C$. Note that $x_i = (x_{i,0}, \dots, x_{i,n-1})$, $\bar{y}_i = (\bar{y}_{i,0}, \dots, \bar{y}_{i,n-1}) \in C_i$ for all $i = 0, \dots, k-1$. Since $x_i \circ_{\mathbf{F}_i} \bar{y}_i = 0_{\mathbf{F}_i}$ for any $\bar{y}_i \in C_i$, we have $x_i \in C_i^{\perp H}$ for all $i = 0, \dots, k-1$. This means that $x \in \bigoplus_{i=0}^{k-1} C_i^{\perp H}$. It follows that $C^{\perp H} \subseteq \bigoplus_{i=0}^{k-1} C_i^{\perp H}$. Hence $C^{\perp H} = \bigoplus_{i=0}^{k-1} C_i^{\perp H}$. From (i), we have

$$|C^{\perp H}| = \prod_{i=0}^{k-1} |C_i^{\perp H}| = \prod_{i=0}^{k-1} \frac{|q_i^{2n}|}{|C_i|} = \frac{\left(\prod_{i=0}^{k-1} q_i^2\right)^n}{\prod_{i=0}^{k-1} |C_i|} = \frac{|\mathcal{R}^n|}{|C|}.$$

Therefore, $|C||C^{\perp H}| = |\mathcal{R}^n|$. \square

Due to the constraint in the definition of the Hermitian inner product, the Hermitian dual codes of skew Θ - λ -constacyclic codes are studied only when the order of Θ is 2. Therefore, we always suppose that the order of Θ is 2.

Lemma 4.7. *Let C be a code of even length n over R . Assume that the order of Θ is 2. Then C is a skew Θ - λ -constacyclic code if and only if $C^{\perp H}$ is a skew Θ - λ^{-1} -constacyclic code. In particular, if $\lambda^2 = 1$, then C is a skew Θ - λ -constacyclic code if and only if $C^{\perp H}$ is a skew Θ - λ -constacyclic code.*

Proof. We first observe that for each unit λ in \mathbf{F}_{q^2} , $\lambda \in \mathbf{F}_{q^2}^{\Theta}$ if and only if $\lambda^{-1} \in \mathbf{F}_{q^2}^{\Theta}$. Let $u = (u_0, u_1, \dots, u_{n-1}) \in C$ and $v = (v_0, v_1, \dots, v_{n-1}) \in C^{\perp H}$. We have

$$\begin{aligned} &((\Theta^{n-1}(\lambda u_1), \Theta^{n-1}(\lambda u_2), \dots, \Theta^{n-1}(\lambda u_{n-1}), \Theta^{n-1}(u_0)) \circ_{\mathcal{R}} (v_0, v_1, \dots, v_{n-1})) \\ &= \lambda \langle (\Theta^{n-1}(u_1), \Theta^{n-1}(u_2), \dots, \Theta^{n-1}(u_{n-1}), \Theta(\lambda^{-1} u_0)) \circ_{\mathcal{R}} (v_0, v_1, \dots, v_{n-1}) \rangle \\ &= \lambda (\Theta^{n-1}(\lambda^{-1} u_0) \bar{v}_{n-1} + \sum_{i=1}^{n-1} \Theta^{n-1}(u_i) \bar{v}_{i-1}). \end{aligned}$$

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

$$0 = \Theta(0) = \Theta(\lambda (\Theta^{n-1}(\lambda^{-1} u_0) \bar{v}_{n-1} + \sum_{i=1}^{n-1} \Theta^{n-1}(u_i) \bar{v}_{i-1}))$$

$$= \lambda(u_0\Theta(\lambda^{-1}\bar{v}_{n-1}) + \sum_{i=1}^{n-1} u_i\Theta(\bar{v}_{i-1})).$$

Hence, C^{\perp_H} is a skew Θ - λ^{-1} -constacyclic code. The converse follows from the fact that $(C^{\perp_H})^{\perp_H} = C$. This implies that C is a skew Θ - λ -constacyclic code if and only if C^{\perp_H} is a skew Θ - λ^{-1} -constacyclic code over R . \square

Put $S = \{x^i \mid i \in \mathbb{N}\}$. Before determining the structure of Hermitian dual codes, we recall the following results.

Proposition 4.8.

- (i) [14, Proposition 2.4] Let $\varphi_i : \mathbf{F}_{q_i^2}[x; \Theta] \rightarrow \mathbf{F}_{q_i^2}[x; \Theta]S^{-1}$ be defined by

$$\varphi_i(\sum_{j=0}^t a_j x^j) = \sum_{j=0}^t x^{-j} a_j.$$

Then φ_i is a ring anti-monomorphism for all $i = 0, \dots, k - 1$.

- (ii) [14, Section 3] Let $\phi_i : \mathbf{F}_{q_i^2}[x; \Theta] \rightarrow \mathbf{F}_{q_i^2}[x; \Theta]$ be defined by

$$\phi_i(\sum_{j=0}^t a_j x^j) = \sum_{j=0}^t \theta_j(a_j) x^j.$$

Then ϕ_i is a ring automorphism for all $i = 0, \dots, k - 1$.

Lemma 4.9. Let Θ be an automorphism of R . Assume that the order of Θ is 2 and $\lambda^2 = 1 \in R$. Let $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ and $b(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$ be in $R[x; \Theta]$, where $a_i = (a_{i,0}, a_{i,1}, \dots, a_{i,k-1})$; $b_i = (b_{i,0}, b_{i,1}, \dots, b_{i,k-1})$. Then the following statements are equivalent:

- (i) The coefficient vector of $a(x)$ is Hermitian orthogonal to the coefficient vector of $x^i \phi(x^{n-1} \varphi(b(x)))$ for all $i \in \{0, 1, \dots, n - 1\}$, where $\phi = (\phi_0, \dots, \phi_{k-1})$ and $\varphi = (\varphi_0, \dots, \varphi_{k-1})$.
- (ii) $(a_0, a_1, \dots, a_{n-1})$ is Hermitian orthogonal to

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

and all its Θ - λ -constacyclic shifts.

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

Proof. (i) \Leftrightarrow (ii) follows directly from the definition of φ . We need to prove that (ii) \Leftrightarrow (iii). Suppose that $a(x)b(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in \frac{R[x; \Theta]}{\langle x^n - \lambda \rangle}$. Since $\lambda \in R$ such that $\lambda^2 = 1$ and n is even, we have

$$\begin{aligned} c_k &= \sum_{i+j=k} a_i \Theta^i(b_j) + \sum_{i+j=k+n} \lambda a_i \Theta^i(b_j) \\ &= \lambda \left(\sum_{i+j=k} a_i \Theta^{k-j}(\lambda b_j) + \sum_{i+j=k+n} a_i \Theta^{n+k+j}(b_j) \right) \end{aligned}$$

$$\begin{aligned}
 &= \lambda(a_0, a_1, \dots, a_{n-1}) \circ_R (\lambda b_k, \Theta(\lambda b_{k-1}), \dots, \Theta^k(\lambda b_0), \Theta^{k+1}(b_{n-1}), \dots, \\
 &\quad \Theta^{n-1}(b_{k+1})) \\
 &= \lambda(a_0, a_1, \dots, a_{n-1}) \circ_R (\Theta^n(\lambda b_k), \Theta^{n+1}(\lambda b_{k-1}), \dots, \\
 &\quad \Theta^k(\lambda b_0), \Theta^{k+1}(b_{n-1}), \dots, \Theta^{n-1}(b_{k+1})) \\
 &= \lambda(a_0, a_1, \dots, a_{n-1}) \circ_R \left(\Theta^{(n-k)+k}(\lambda b_k), \Theta^{(n-k+1)+k}(\lambda b_{k-1}), \dots, \right. \\
 &\quad \left. \Theta^k(\lambda b_0), \Theta^{k+1}(b_{n-1}), \dots, \Theta^{(n-k-1)+k}(b_{k+1}) \right)
 \end{aligned}$$

for $0 \leq i \leq n-1, 0 \leq j \leq n-1$. Hence, $a(x)b(x) = 0$ if and only if $c_k = 0$ for all $k \in \{0, 1, \dots, n-1\}$. This implies that $(a_0, a_1, \dots, a_{n-1})$ is Hermitian orthogonal to $(b_{n-1}, \Theta(b_{n-2}), \dots, \Theta^{n-1}(b_0))$ and its skew constacyclic shifts. \square

Theorem 4.10. *Let Θ be an automorphism of R . Assume that the order of Θ is 2 and $\lambda^2 = 1$. Let $g(x)$ be a right divisor of $x^n - \lambda$ and $h(x) := \frac{x^n - \lambda}{g(x)}$. Let C be the skew 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 skew Θ - λ -constacyclic code generated by $\phi(x^{\deg h(x)}\varphi(h(x)))$.*

Proof. We have

$$\begin{aligned}
 (\varphi(g(x))(-\lambda)x^{n-\deg(h(x))})\phi(x^{\deg(h(x))}\varphi(h(x))) &= \varphi(g(x))(-\lambda)x^n\varphi(h(x)) \\
 &= -\lambda x^n\varphi(g(x))\varphi(h(x)) \\
 &= -\lambda x^n\varphi(h(x)g(x)) \\
 &= -\lambda x^n\varphi(x^n - \lambda) \\
 &= -\lambda x^n(x^{-n} - \lambda) \\
 &= x^n - \lambda.
 \end{aligned}$$

Therefore,

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

Hence, $\phi(x^{\deg(h(x))}\varphi(h(x)))$ is a right divisor of $x^n - \lambda$, proving (i). We can see that $g(x)h(x) = x^n - \lambda = 0$ in $\frac{\mathbf{F}_q[x; \Theta]}{\langle x^n - \lambda \rangle}$. Applying Lemma 4.7, we have

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

By Theorem 2.3, we have

$$|\langle \phi(x^{\deg(h(x))}\varphi(h(x))) \rangle| = q^{2(n-\deg(h(x)))}.$$

This implies that $\langle \phi(x^{\deg(h(x))}\varphi(h(x))) \rangle = C^{\perp_H}$, showing (ii). \square

Theorem 4.11. *Let Θ be an automorphism of R . Assume that the order of Θ is 2, $\lambda^2 = 1$ and n is even, i.e., $n = 2k$. Suppose that $g(x) = \sum_{i=0}^{k-1} g_i x^i + x^k$ is a right divisor of $x^n - \lambda$. Then the skew Θ - λ -constacyclic code generated by $g(x)$ is Hermitian self-dual if and only if*

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

Proof. Let C be the skew Θ - λ -constacyclic code generated by $g(x)$ and $g^{\perp H}$ be the generator polynomial of the Hermitian dual code C . By assumption, we have $g(x) = \sum_{i=0}^{k-1} g_i x^i + x^k$ and $h(x) = \sum_{i=0}^{k-1} h_i x^i + x^k = \frac{x^n - \lambda}{g(x)}$. Applying Theorem 4.10, we have $g^{\perp H} = \Theta^{k+1}(h_0)x^k + \dots + \Theta^2(h_{k-1})x + 1$. Since C is Hermitian self-dual, we have $g^{\perp H}(x) = \Theta^{k+1}(h_0)g(x) = \Theta^{k+1}(h_0)(\sum_{i=0}^{k-1} g_i x^i + x^k)$. Comparing coefficients, we have

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

Conversely, if

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

then $h(x) = \Theta^{-k-1}(g_0^{-1}) + \sum_{i=1}^{k-1} \Theta^{i-k-1}(g_0^{-1} g_{k-i})x^i + x^k$. By applying Theorem 4.10 again, $g^{\perp H} = \phi(x^{\deg h(x)} \varphi(h(x)))$, completing our proof. \square

Remark 4.12. Suppose that there is a Hermitian self-dual skew Θ - λ -constacyclic code over R . By theorem above, we must have a condition $-\lambda = g_0 \Theta^{-k-1}(g_0^{-1})$. Since λ is fixed by Θ , we can see that λ can be expressed as $\lambda = -\Theta^{k+1}(g_0)g_0^{-1}$. Note that the order of Θ is 2. Then we have $\lambda = -1$ if k is odd or $\lambda = -\Theta(g_0)g_0^{-1}$ if k is even. Therefore, if k is odd and $\lambda \neq -1$, then there are no Hermitian self-dual skew λ -constacyclic codes of length $n = 2k$.

5. Skew constacyclic codes of arbitrary length over finite semi-simple rings

If n is divisible by the order of Θ , then there is a one-to-one correspondence between skew Θ - λ -constacyclic codes and left ideals in R . However, the set $R_n = \frac{\mathbf{F}[x; \Theta]}{\langle x^n - 1 \rangle}$ fails to be a ring if n is not divisible by the order of Θ [5]. This is the reason why we can not study skew Θ - λ -constacyclic codes as previous way when n is not divisible by the order of Θ . In [16], Siap et al. gave a new way to study skew Θ -codes that $R_n = \frac{\mathbf{F}[x; \Theta]}{\langle x^n - 1 \rangle}$ can be considered as a left $\mathbf{F}[x; \Theta]$ module when n is not divisible by the order of Θ . From this, the skew Θ -cyclic codes of arbitrary length were studied. Let $(f(x) + (x^n - 1))$ be an element in

the set R_n , and let $r(x) \in \mathbf{F}[x; \Theta]$. Define multiplication of the element of R_n by the elements of $\mathbf{F}[x; \Theta]$ as follows:

$$r(x) \star (f(x) + (x^n - 1)) = r(x) \star f(x) + (x^n - 1) \quad (1)$$

for any $r(x) \in \mathbf{F}[x; \Theta]$. Then, we have the following result provided in [16].

Theorem 5.1 ([16, Theorem 9]). R_n is a left $\mathbf{F}[x; \Theta]$ -module where multiplications is defined as in Equation 1.

Using theorem above, Siap et al. [16] gave the definition of skew cyclic codes for any length as follows.

Theorem 5.2 ([16, Theorem 10]). A code C in R_n is a skew Θ -cyclic code if and only if C is a left $\mathbf{F}[x; \Theta]$ -submodule of the left $\mathbf{F}[x; \Theta]$ -module R_n .

We now give a definition of skew Θ - λ -constacyclic codes of arbitrary length over semi-simple rings $R = \mathbf{F}_0 \oplus \mathbf{F}_1 \oplus \cdots \oplus \mathbf{F}_{k-1}$.

Definition 5.3. A code C in R is a skew Θ -constacyclic code if C is a left R -submodule of the left $R[x; \Theta]$ -module R_n .

We have the following result.

Proposition 5.4. Let C be a skew Θ - λ -constacyclic code of arbitrary length n over R . Then the following results hold true:

- (i) The skew Θ - λ -constacyclic code C has the form $C = \bigoplus_{i=0}^{k-1} C_i$, where C_i is a Θ - λ -constacyclic code of length n over \mathbf{F}_i ($i = 0, \dots, k-1$). Moreover, the skew Θ - λ -constacyclic code C is a linear code over R if and only if the skew Θ - λ -constacyclic code C_i is a linear code over \mathbf{F}_i ($i = 0, \dots, k-1$).
- (ii) Let $\lambda = (\lambda_0, \dots, \lambda_{k-1})$ be a unit of R , where λ_i is fixed by Θ_i . A code $C = \bigoplus_{i=0}^{k-1} C_i$ is a skew Θ - λ -constacyclic code of length n over R if and only if each code C_i is a skew Θ_i - λ_i -constacyclic code of length n over \mathbf{F}_i .

Proof. We can see that the structure of skew Θ - λ_i -constacyclic code C_i of length n can be identified with the structure of the left $\mathbf{F}_i[x; \Theta]$ -submodule of R for all $i = 0, \dots, k-1$. Therefore, part (i) and (ii) are held. \square

From Proposition 5.4, we have a characterization of skew Θ - λ -constacyclic codes as follows.

Theorem 5.5. A code C over R is a skew Θ - λ -constacyclic code if and only if C is a left $R[x; \Theta]$ -submodule of the left $R[x; \Theta]$ -module R_n .

Suppose that M is an R -module and U is a submodule of M . If U is generated by $m \in M$, i.e.,

$$U = \langle m \rangle = \{rm : r \in R\},$$

then U is called a *cyclic submodule* generated by m . The following lemma is given in [16]. It is easy to extend for skew Θ - λ -constacyclic codes over R .

Proposition 5.6 ([16, Lemma 11]). *Let C be a left submodule of R_n . Then C is a cyclic submodule generated by a monic polynomial of minimal degree in C .*

Motivated by this, we have the following result for the case of skew Θ - λ -constacyclic codes over R .

Proposition 5.7. *Let $\lambda = (\lambda_0, \dots, \lambda_{k-1})$ be a unit of R , and $C = \bigoplus_{i=0}^{k-1} C_i$ a skew Θ - λ -constacyclic code of length n over R , where C_i is a skew Θ_i - λ_i -constacyclic code of length n over \mathbf{F}_i . Then $C = \langle (g_0(x), \dots, g_{k-1}(x)) \rangle$, where C_i is a skew Θ_i - λ_i -constacyclic code generated by a monic polynomial of minimal degree $g_i(x)$ in C_i for $i = 0, \dots, k - 1$.*

Proof. It is straightforward from that

$$\phi : \frac{R[x, \Theta]}{\langle x^n - \lambda \rangle} \longrightarrow \bigoplus_{i=0}^{k-1} \frac{\mathbf{F}_i[x, \Theta_i]}{\langle x^n - \lambda_i \rangle}$$

is a ring isomorphism. □

Remark 5.8. It is well-known from [16, Theorem 12] that if $C_i = \langle g_i(x) \rangle$ is a left submodule of R_n , then $g_i(x)$ is a right divisor of $x^n - \lambda$. Therefore, we can prove that if C is a skew Θ - λ -constacyclic code and $C = \langle g_0, \dots, g_{k-1} \rangle$ is a left submodule of R , then each $g_i(x)$ is a right divisor of $x^n - \lambda_i$ over \mathbf{F}_i for $i = 0, \dots, k - 1$.

We recall the definition of quasi-cyclic codes over finite fields.

Definition 5.9. Let \mathbf{F} be a finite field. A subset C of \mathbf{F}^n is called a *quasi-cyclic code* of length $n = sl$ and index l if C satisfies the following conditions:

- (a) C is a subspace of \mathbf{F}^n .
- (b) If

$$c = (c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}) \in C,$$

then

$$T_{\Theta, s, l}(c) = (c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}, c_{0,0}, \dots, c_{0,l-1}, \dots, c_{s-2,0}, \dots, c_{s-2,l-1}) \in C.$$

Equivalently, C is a quasi-cyclic code of length $n = sl$ and index l if C

$$\text{is a } \frac{\mathbf{F}[x]}{\langle x^s - 1 \rangle}\text{-submodule of } \left(\frac{\mathbf{F}[x]}{\langle x^s - 1 \rangle} \right)^l.$$

The following result was proven in [16].

Proposition 5.10 ([16, Corollary 17]). *For $\gcd(m, n) = 1$, if $f(x)$ is a factor of $x^n - 1$ in $\mathbf{F}[x; \Theta]$, then $f(x)$ is also a factor of $x^n - 1$ in the usual polynomial ring $\mathbf{F}[x]$.*

Applying Proposition 5.10, we have a result for skew Θ -cyclic codes of length n over R .

Theorem 5.11. *Let $\Theta = (\Theta_0, \dots, \Theta_{k-1})$ be an automorphism of R with $|\langle \Theta_i \rangle| = m_i$, and $C = \langle g(x) \rangle = (g_0(x), \dots, g_{k-1}(x))$ be a skew Θ - λ -cyclic code of length n over R . If $\gcd(m_i, n) = 1$ for all $i = 0, \dots, k-1$, then C is a cyclic code of length n over R .*

Proof. From Proposition 5.10, we can see that C_i is a cyclic code of length n over \mathbf{F}_i for all $i = 0, \dots, k-1$. Hence, $C = \bigoplus_{i=0}^{k-1} C_i$ is a cyclic code of length n over R , by Proposition 3.3. \square

Let Θ be an automorphism with order m such that $\gcd(m, n) = d$ and C be a skew Θ -cyclic code of length n over \mathbf{F} . Suppose that $n = sd$ and

$$\begin{aligned} c(x) = & c_{0,0} + c_{0,1}x + \dots + c_{0,d-1}x^{d-1} + c_{1,0}x^d + \dots + c_{1,d-1}x^{2d-1} + \dots \\ & + c_{s-1,0}x^{sd-d} + \dots + c_{s-1,d-1}x^{sd-1} \in C. \end{aligned}$$

Since $\gcd(m, n) = d$, there exist integers a, t such that $am = d - tn > 0$. Now, we consider

$$\begin{aligned} x^{am} * c(x) &= x^{d-tn} * (c_{0,0} + \dots + c_{0,d-1}x^{d-1} + c_{1,0}x^d + \dots \\ & \quad + c_{1,d-1}x^{2d-1} + \dots + c_{s-1,0}x^{sd-d} + \dots + c_{s-1,d-1}x^{sd-1}) \\ &= x^{d-tn} * c_{0,0} + \dots + x^{d-tn} * c_{0,d-1}x^{d-1} + x^{d-tn} * c_{1,0}x^d + \dots \\ & \quad + x^{d-tn} * c_{1,d-1}x^{2d-1} + \dots + x^{d-tn} * c_{s-1,0}x^{sd-d} + \dots \\ & \quad + x^{d-tn} * c_{s-1,d-1}x^{sd-1} \\ &= \Theta^{d-tn}(c_{0,0})x^{d-tn} + \dots + \Theta^{d-tn}(c_{0,d-1})x^{d-tn+d-1} + \dots \\ & \quad + \Theta^{d-tn}(c_{s-2,0})x^{d-tn+sd-2d} + \dots \\ & \quad + \Theta^{d-tn}(c_{s-2,d-1})x^{d-tn+sd-d-1} \\ & \quad + \Theta^{d-tn}(c_{s-1,0})x^{d-tn+sd-d} + \Theta^{d-tn}(c_{s-1,1})x^{d-tn+sd-d+1} + \dots \\ & \quad + \Theta^{d-tn}(c_{s-1,d-1})x^{d-tn+sd-1} \\ &= \Theta^{d-tn}(c_{s-1,0})x^{d-tn+sd-d} + \Theta^{d-tn}(c_{s-1,1})x^{d-tn+sd-d+1} + \dots \\ & \quad + \Theta^{d-tn}(c_{s-1,d-1})x^{d-tn+sd-1} + \Theta^{d-tn}(c_{0,0})x^{d-tn} + \dots \\ & \quad + \Theta^{d-tn}(c_{0,d-1})x^{d-tn+d-1} + \dots \\ & \quad + \Theta^{d-tn}(c_{s-2,0})x^{d-tn+sd-2d} + \dots \\ & \quad + \Theta^{d-tn}(c_{s-2,d-1})x^{d-tn+sd-d-1}. \end{aligned}$$

Since $x^n = 1$ and $\Theta^{d-tn}(c_{s-1,0}) = \Theta^{am}(c_{s-1,0}) = c_{s-1,0}$, we have

$$\Theta^{d-tn}(c_{s-1,0})x^{d-tn+sd-d} = \Theta^{am}(c_{s-1,0})x^{n-tn} = c_{s-1,0}.$$

Similarly, we can see that

$$\begin{aligned} \Theta^{d-tn}(c_{s-1,1})x^{d-tn+sd-d+1} &= \Theta^{am}(c_{s-1,1})x^{n-tn+1} = c_{s-1,1} \cdot x, \\ & \vdots \end{aligned}$$

$$\begin{aligned}
 \Theta^{d-tn}(c_{s-1,d-1})x^{d-tn+sd-1} &= \Theta^{am}(c_{s-1,d-1})x^{n-tn+d-1} = c_{s-1,d-1} \cdot x^{d-1}, \\
 \Theta^{d-tn}(c_{0,0})x^{d-tn} &= \Theta^{am}(c_{0,0})x^d = c_{0,0} \cdot x^d, \\
 &\vdots \\
 \Theta^{d-tn}(c_{0,d-1})x^{d-tn+d-1} &= \Theta^{am}(c_{0,d-1})x^{2d-1} = c_{0,d-1} \cdot x^{2d-1}, \\
 &\vdots \\
 \Theta^{d-tn}(c_{s-2,0})x^{d-tn+sd-2d} &= \Theta^{am}(c_{s-2,0})x^{-d} = c_{s-2,0} \cdot x^{n-d}, \\
 &\vdots \\
 \Theta^{d-tn}(c_{s-2,d-1})x^{d-tn+sd-d-1} &= \Theta^{am}(c_{s-2,d-1})x^{-1} = c_{s-2,d-1} \cdot x^{n-1}.
 \end{aligned}$$

Thus,

$$\begin{aligned}
 x^{am} * c(x) &= c_{s-1,0} + c_{s-1,1}x + \dots + c_{s-1,d-1}x^{d-1} + c_{0,0}x^d + \dots \\
 &\quad + c_{0,d-1}x^{2d-1} + \dots + c_{s-2,0}x^{n-d} + \dots + c_{s-2,d-1}x^{n-1}.
 \end{aligned}$$

Since $(x^{am} * c(x)) \in C$, we can conclude that

$$(c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,d-1}, c_{0,0}, \dots, c_{0,d-1}, \dots, c_{s-2,0}, \dots, c_{s-2,d-1}) \in C.$$

This shows that C is equivalent to a quasi-cyclic code of length n with index d over \mathbf{F} . This relationship between skew Θ -cyclic codes and quasi-cyclic codes was provided in [16].

Theorem 5.12 ([16, Theorem 18]). *Let Θ be an automorphism of \mathbf{F} with $|\langle \Theta \rangle| = m$, and $C = \langle g(x) \rangle$ be a skew Θ -cyclic code of length n over \mathbf{F} . If $\gcd(m, n) = d$, then C is equivalent to a quasi-cyclic code of length n and index d .*

We consider the general case $\gcd(m_i, n) = d_i$ for all $i = 0, \dots, k-1$, where d_i is not necessarily be equal to 1 as in Theorem 5.13.

Theorem 5.13. *Let $C = \langle g(x) \rangle = \langle g_0(x), g_1(x), \dots, g_{k-1}(x) \rangle$ be a skew Θ -cyclic code of length n and Θ an automorphism of \mathbf{F}_i with $|\langle \Theta_i \rangle| = m_i$. If $\gcd(m_i, n) = d_i$ for all $i = 0, \dots, k-1$, then $C = \bigoplus_{i=0}^{k-1} C_i$, where C_i is equivalent to a quasi-cyclic code of length n and index d_i .*

Proof. Since $\gcd(m_i, n) = d_i$ for all $i = 0, \dots, k-1$, by applying Theorem 5.12, we can see that C_i is equivalent to a quasi-cyclic code of length n and index d_i . □

Remark 5.14.

- (i) Theorem 5.11 is a special case of Theorem 5.13, where all $d_i = 1$.
- (ii) When all $d_i = d$, the skew Θ -cyclic code C is equivalent to a quasi-cyclic code of index d .

We conclude this section by providing some examples to illustrate our results.

Example 5.15. We consider $\mathbf{F}_8 = \mathbf{F}_2(a)$, where $a^3 = a + 1$. Let Θ be the Frobenius homomorphism of \mathbf{F}_8 , i.e., $\Theta(u) = u^2$ for all $u \in \mathbf{F}_8$. It is easy to see that the order of Θ is $m = 3$. Let us consider the skew Θ -cyclic code of length 5. According to Proposition 5.10, in this case $\gcd(3, 5) = 1$, if $f(x)$ is a factor of $x^5 - 1$ in $\mathbf{F}_8[x, \Theta]$, then $f(x)$ is also a factor of $x^5 - 1$ in the usual polynomial ring $\mathbf{F}_8[x]$. In fact, nontrivial right divisors of $x^5 - 1$ in $\mathbf{F}_8[x, \Theta]$ are $f_1(x) = x - 1$, $f_2 = x^4 + x^3 + x^2 + x + 1$. These factors are also factors of $x^5 - 1$ in $\mathbf{F}_8[x]$.

Example 5.16. We consider $\mathbf{F} = \mathbb{Z}_2(a)$, a is a root of $x^4 + x + 1$, and $\Theta(z) = z^2$. It is clear that the order of Θ is 4. In $\mathbf{F}[x; \Theta]$, we can see that $x^6 - 1 = (x^3 + a^{10}x^2 + a^5x + a^5) * (x^3 + a^5x^2 + a^5x + a^{10})$. As mentioned in Theorem 5.13, the skew Θ -cyclic code generated by $f(x) = x^3 + a^5x^2 + a^5x + a^{10}$ is equivalent to a quasi-cyclic code of length 6 and index 2 generated by $g(x) = x + a^5$.

Acknowledgements. H. Q. Dinh and S. Sriboonchitta are grateful to the Centre of Excellence in Econometrics, Chiang Mai University, for partial financial support. This research is partially supported by the Research Administration Centre, Chaing Mai University.

References

- [1] M. M. Al-Ashker, *Simplex codes over the ring $F_2 + uF_2$* , Arab. J. Sci. Eng. Sect. A Sci. **30** (2005), no. 2, 277–285.
- [2] A. Bonnetcaze and P. Udaya, *Cyclic codes and self-dual codes over $F_2 + uF_2$* , IEEE Trans. Inform. Theory **45** (1999), no. 4, 1250–1255.
- [3] D. Boucher, W. Geiselmann, and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 379–389.
- [4] D. Boucher, P. Solé, and F. Ulmer, *Skew constacyclic codes over Galois rings*, Adv. Math. Commun. **2** (2008), no. 3, 273–292.
- [5] D. Boucher and F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. **44** (2009), no. 12, 1644–1656.
- [6] ———, *A note on the dual codes of module skew codes*, in Cryptography and coding, 230–243, Lecture Notes in Comput. Sci., 7089, Springer, Heidelberg, 2011.
- [7] ———, *Self-dual skew codes and factorization of skew polynomials*, J. Symbolic Comput. **60** (2014), 47–61.
- [8] H. Q. Dinh, *On repeated-root constacyclic codes of length $4p^s$* , Asian-Eur. J. Math. **6** (2013), no. 2, 1350020, 25 pp.
- [9] H. Q. Dinh, B. T. Nguyen, and S. Sriboonchitta, *Skew constacyclic codes over finite fields and finite chain rings*, Math. Probl. Eng. **2016** (2016), Art. ID 3965789, 17 pp.
- [10] ———, *Constacyclic codes over finite commutative semi-simple rings*, Finite Fields Appl. **45** (2017), 1–18.
- [11] J. Gao, *Skew cyclic codes over $F_p + vF_p$* , J. Appl. Math. Inform. **31** (2013), no. 3-4, 337–342.
- [12] J. Gao, L. Shen, and F.-W. Fu, *A Chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields*, Cryptogr. Commun. **8** (2016), no. 1, 51–66.
- [13] F. Gursoy, I. Siap, and B. Yildiz, *Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$* , Adv. Math. Commun. **8** (2014), no. 3, 313–322.
- [14] S. Jitman, S. Ling, and P. Udomkavanich, *Skew constacyclic codes over finite chain rings*, Adv. Math. Commun. **6** (2012), no. 1, 39–63.

- [15] J. L. Massey, *Linear codes with complementary duals*, Discrete Math. **106/107** (1992), 337–342.
- [16] I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne, *Skew cyclic codes of arbitrary length*, Int. J. Inf. Coding Theory **2** (2011), no. 1, 10–20.
- [17] P. Udaya and A. Bonnecaze, *Decoding of cyclic codes over F_2+uF_2* , IEEE Trans. Inform. Theory **45** (1999), no. 6, 2148–2157.

HAI Q. DINH
DIVISION OF COMPUTATIONAL MATHEMATICS AND ENGINEERING
INSTITUTE FOR COMPUTATIONAL SCIENCE
TON DUC THANG UNIVERSITY
HO CHI MINH CITY, VIETNAM
AND
FACULTY OF MATHEMATICS AND STATISTICS
TON DUC THANG UNIVERSITY
HO CHI MINH CITY, VIETNAM
Email address: dinhquanghai@tdtu.edu.vn

BAC TRONG NGUYEN
NGUYEN TAT THANH UNIVERSITY
300 A NGUYEN TAT THANH STREET
HO CHI MINH CITY, VIETNAM
AND
DEPARTMENT OF BASIC SCIENCES
UNIVERSITY OF ECONOMICS AND BUSINESS ADMINISTRATION
THAI NGUYEN UNIVERSITY
THAI NGUYEN PROVINCE, VIETNAM
Email address: bacnt2008@gmail.com

SONGSAK SRIBOONCHITTA
FACULTY OF ECONOMICS
CHIANG MAI UNIVERSITY
CHIANG MAI 52000, THAILAND
Email address: songsakecon@gmail.com