SKEW CONSTACYCLIC CODES OVER FINITE COMMUTATIVE SEMI-SIMPLE RINGS

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

Abstract. This paper investigates skew \( \Theta\)-\( \lambda \)-constacyclic codes over \( R = \mathbb{F}_0 \oplus \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_{k-1} \), where \( \mathbb{F}_i \)'s are finite fields. The structures of skew \( \lambda \)-constacyclic codes over finite commutative semi-simple rings and their duals are provided. Moreover, skew \( \lambda \)-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 \( \Theta\)-\( \lambda \)-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 \( 2^n \).

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 \( \Theta \)-cyclic codes, skew \( \Theta \)-negacyclic codes, skew \( \Theta\)-\( \lambda \)-constacyclic codes.

\( \copyright \)2019 Korean Mathematical Society
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, 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 $\Theta$-$\lambda$-constacyclic (briefly, skew constacyclic) over finite chain rings. They studied the structure of skew $\Theta$-$\lambda$-constacyclic, the Euclidean and Hermitian dual codes of skew $\Theta$-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 $\mathbb{F}_p + v\mathbb{F}_p$ and $\mathbb{F}_q + v\mathbb{F}_q$ 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 $\Theta$-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 $\Theta$-$\lambda$-constacyclic codes over finite commutative semi-simple rings in Section 3. The dual codes of skew $\Theta$-$\lambda$-constacyclic codes over finite commutative semi-simple rings are investigated in Section 4. Finally, in the Section 5, we consider the structure of skew $\Theta$-$\lambda$-constacyclic codes over finite commutative semi-simple rings for arbitrary length.

2. Preliminaries

We first recall the definition of skew $\Theta$-$\lambda$-constacyclic codes over finite fields.

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

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

In particular, when $\lambda = 1$ or $\lambda = -1$, such codes are called *skew $\Theta$-cyclic* and *skew $\Theta$-negacyclic codes*, respectively. When $\Theta$ 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 $\mathbb{F}_p^m[x]$ is a commutative ring, so every ideals of $\mathbb{F}_p^m[x]$ is two-sided ideals, the skew polynomial ring $\mathbb{F}_p^m[x; \Theta]$ is noncommutative. Therefore, we need to have conditions of $\Theta$ and $\lambda$ 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 $\Theta$ and $\lambda$ is fixed by $\Theta$, then $\langle x^n - \lambda \rangle$ is a two-sided ideal of $F_{p^n}[x; \Theta]$. If $\Theta$ is not the identity, then $F_{p^n}[x; \Theta]$ 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 $\Theta$-$\lambda$-constacyclic codes.

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

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 $\Theta$ be an automorphism of $F_{p^n}$, and $n$ an integer divisible by the order of $\Theta$, and $\lambda$ a unit in $F_{p^n}$ which is fixed by $\Theta$. Then the code $C$ is a skew $\Theta$-$\lambda$-constacyclic code if and only if $C$ is a left ideal $(g(x)) \subseteq F_{p^n}[x; \Theta]_{\langle x^n - \lambda \rangle}$, where $g(x)$ is a right divisor of $x^n - \lambda$.

Given a monic right divisor of degree $n - k$ of $x^n - \lambda$ : $g(x) = \sum_{i=0}^{n-k} g_i x^i + x^{n-k}$. Then a generator matrix of the $\Theta$-$\lambda$-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 $\Theta$-$\lambda$-cyclic code of length $n$ over $F_q$ 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

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

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

**Lemma 2.5** ([5, Lemma 17]). Let $\Theta$ be an automorphism of $F_{p^n}$, and $n$ an integer divisible by the order of $\Theta$, and $\lambda$ a unit in $F_{p^n}$ which is fixed by $\Theta$. Let $C$ be the $\Theta$-$\lambda$-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

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

is a parity-check matrix for $C$.  

SKEW CONSTACYCLIC CODES 421
For skew $\Theta$-negacyclic and skew $\Theta$-cyclic codes, the following two corollaries are direct consequences of Theorem 2.3.

**Corollary 2.6** ([3, Lemma 1]). Let $\Theta$ be an automorphism of $F_{p^m}$, and $n$ an integer divisible by the order of $\Theta$. Then the code $C$ is a skew $\Theta$-cyclic code if and only if $C$ is a left ideal $\langle g(x) \rangle \subseteq F_{p^m}[x;\Theta] \langle x^n-1 \rangle$, where $g(x)$ is a right divisor of $x^n-1$.

**Corollary 2.7.** Let $\Theta$ be an automorphism of $F_{p^m}$, and $n$ an integer divisible by the order of $\Theta$. Then the code $C$ is a skew $\Theta$-negacyclic code if and only if $C$ is a left ideal $\langle g(x) \rangle \subseteq F_{p^m}[x;\Theta] \langle x^n+1 \rangle$, 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 $\lambda$-constacyclic codes over finite commutative semi-simple rings. We now consider the semi-simple ring $R = F_0 \oplus F_1 \oplus \cdots \oplus F_{k-1}$, where $F_i$'s are finite fields. Since $R = F_0 \oplus F_1 \oplus \cdots \oplus F_{k-1}$, the unit $\lambda$ of $R$ is uniquely expressed as

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

Assume that $\Theta$ is an automorphism of $R$. Then $\Theta$ can be written as $\Theta = (\Theta_0, \ldots, \Theta_{k-1})$, where $\Theta_i$ is an automorphism of $F_i$.

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

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

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

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

$$\Theta^t(\lambda) = (\lambda_0, \lambda_1, \ldots, \lambda_{k-1}).$$

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 $\Theta_i$ for all $i = 0, \ldots, k-1$. Hence, $u$ is an integer divisible by $t$, proving that $t$ is the order of $\Theta$. 

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

**Proof.** It is routine to check.
Assume that $\Theta$ is an automorphism of $R$ and $n$ is an integer divisible by the order of $\Theta$. If $\lambda$ is a unit in $R$ which is fixed by $\Theta$, then it is readily to check that the map
\[ \phi : \frac{R[x, \Theta]}{(x^n - \lambda)} \to \bigoplus_{i=0}^{k-1} \frac{F_i[x, \Theta]}{(x^n - \lambda_i)} \]
given by
\[ a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \mapsto (a_{0,0} + a_{0,1} x + \cdots + a_{0,n-1} x^{n-1}, \ldots, a_{k-1,0} + a_{k-1,1} x + \cdots + a_{k-1,n-1} x^{n-1}) \]
is a ring isomorphism. Hence, the ring $\frac{R[x, \Theta]}{(x^n - \lambda)}$ can be decomposed as
\[ \frac{R[x, \Theta]}{(x^n - \lambda)} \cong \bigoplus_{i=0}^{k-1} \frac{F_i[x, \Theta]}{(x^n - \lambda_i)}. \]

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

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

(i) Let $C$ be a skew $\Theta$-$\lambda$-constacyclic code over $R$. Then the skew $\Theta$-$\lambda$-constacyclic code $C$ has the form $C = \oplus_{i=0}^{k-1} C_i$, where $C_i$ is a skew $\Theta_i$-$\lambda_i$-constacyclic code of length $n$ over $F_i$ $(i = 0, \ldots, k - 1)$. Moreover, the skew $\Theta$-$\lambda$-constacyclic code $C$ is a linear code over $R$ if and only if the skew $\Theta$-$\lambda$-constacyclic code $C_i$ is a linear code over $F_i$.

(ii) Let $\lambda = (\lambda_0, \ldots, \lambda_{k-1})$ be a unit of $R$. A skew $\Theta$-$\lambda$-code $C = \oplus_{i=0}^{k-1} C_i$ is a skew $\Theta$-$\lambda$-constacyclic code of length $n$ over $R$ if and only if each code $C_i$ is a skew $\Theta_i$-$\lambda_i$-constacyclic code of length $n$ over $F_i$.

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

(ii) Consider any codeword $(c_0, c_1, \ldots, c_{k-1}) \in C$, where $c_i = (c_{i,0}, \ldots, c_{i,n-1}) \in C_i$. Since
\[ \lambda c_{n-1} = (\lambda_0, \lambda_1, \ldots, \lambda_{k-1})(c_{n-1,0}, c_{n-1,1}, \ldots, c_{n-1,k-1}) \]
\[ = (\lambda_0 c_{n-1,0}, \ldots, \lambda_{k-1} c_{n-1,k-1}) \]
we have
\[ (\Theta(\lambda c_{n-1}), c_0, \ldots, c_{n-2}) = \Theta_0(\lambda_0 c_{n-1,0}), c_0, \ldots, c_{n-2,0}) \]
Therefore, $C$ is a skew $\Theta$-$\lambda$-constacyclic code of length $n$ over $R$ if and only if $C_i$ is a skew $\Theta_i$-$\lambda_i$-constacyclic code of length $n$ over $F_i$. \hfill \Box$

For a skew $\Theta$-$\lambda$-constacyclic code $C = \bigoplus_{i=0}^{k-1} C_i$ of length $n$ over $R$, the code $C_i$ ($i = 0, \ldots, k-1$) is a skew $\Theta_i$-$\lambda_i$-constacyclic code of length $n$ over the field $F_i$, so $C_i$ is a principal left ideal of the ring $F_i[x, \Theta_i]_{x^n - \lambda_i}$ generated by right factors of $x^n - \lambda_i$, say $C_i = \langle g_i(x) \rangle$. Let $g(x) = (g_1(x), \ldots, g_k(x)) \in R[x, \Theta]$, then it is straightforward to see that $C = \langle g(x) \rangle$. Moreover, a generator matrix of $C$ is $G := \left( \begin{array}{c} G_0 \\ \vdots \\ G_{k-1} \end{array} \right)$, where the matrices $G_i$ are generator matrices of $C_i$ for all $i = 0, \ldots, k-1$. One can also deduce an expression for the parity check matrix of skew $\Theta$-$\lambda$-constacyclic code $C$ as follows: $H := \left( \begin{array}{c} H_0 \\ \vdots \\ H_{k-1} \end{array} \right)$, where the matrices $H_i$ are the parity check matrices of skew $\Theta_i$-$\lambda_i$-constacyclic codes $C_i$ for all $i = 0, \ldots, k-1$.

Thus, we have the following result.

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

(i) $C = \langle (g_0(x), \ldots, g_{k-1}(x)) \rangle$, where $g_0(x), \ldots, g_{k-1}(x)$ are the generator polynomials of $C_i$ ($i = 0, \ldots, k-1$).

(ii) $C$ is generated by $g(x) = (g_0(x), \ldots, g_{k-1}(x))$. In particular, $R[x, \Theta]_{x^n - \lambda}$ is a principal left ideal ring.

(iii) Suppose that $C$ is generated by $g(x) = (g_0(x), \ldots, g_{k-1}(x))$, where $\deg g_i(x) = r_i$ ($i = 0, \ldots, k-1$). Then $C$ has the following generator matrix:

$$G := \begin{pmatrix}
g_0(x) & xg_0(x) & \cdots & x^{n-r_0-1}g_0(x) \\
g_1(x) & xg_1(x) & \cdots & x^{n-r_1-1}g_1(x) \\
\vdots & \vdots & \ddots & \vdots \\
g_{k-1}(x) & xg_{k-1}(x) & \cdots & x^{n-r_{k-1}-1}g_{k-1}(x)
\end{pmatrix}$$
Lemma 3.5. Let \( \alpha = (\alpha_0, \ldots, \alpha_{k-1}) \) and \( \beta = (\beta_0, \ldots, \beta_{k-1}) \) be distinct nonzero unit elements of the ring \( R \) fixed by \( \Theta = (\Theta_0, \ldots, \Theta_{k-1}) \), where \( \Theta = (\Theta_0, \ldots, \Theta_{k-1}) \) is a ring automorphism of \( R \). Then \( C \) is both skew \( \alpha \)-and \( \beta \)-constacyclic if and only if each \( C_i \) is both skew \( \alpha_i \)-and \( \beta_i \)-constacyclic.

Proof. It is a direct consequence of Proposition 3.3. \( \square \)

4. Dual codes

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

\[
x \circ y = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1},
\]
evaluated in \( F_{p^m} \). Two codewords \( x, y \) are called orthogonal if \( x \circ y = 0 \). For a linear code \( C \) over \( F_{p^m} \), its dual code \( C^\perp \) is the set of \( n \)-tuples over \( F_{p^m} \) 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 \( \Theta \) be an automorphism of \( F_{p^m} \), and \( n \) an integer divisible by the order of \( \Theta \), and \( \lambda \) a unit in \( F_{p^m} \) which is fixed by \( \Theta \). 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 \( \Theta \)-cyclic code generated by \( g(x) \) in \( F_{p^m}[x, \Theta] \) is the skew \( \Theta \)-cyclic code generated by

\[
g^\perp(x) = 1 + \Theta(h_{n-r-1}) x + \cdots + \Theta^{n-r}(h_0) x^{n-r}.
\]

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

\[
g(x) = (g_0(x), \ldots, g_{k-1}(x)),
\]

then the dual of skew \( \Theta \)-cyclic code is generated by

\[
g^\perp(x) = (g_0^\perp(x), \ldots, g_{k-1}^\perp(x)).
\]

Proof. It is straightforward from Proposition 3.3 and Lemma 4.1. \( \square \)

It is well-known in [14] that \( C \) is a skew \( \Theta \)-cyclic code over \( F_{p^m} \) if and only if \( C^\perp \) is a skew \( \Theta \)-cyclic code over \( F_{p^m} \). The following result is used to characterize the dual code of a skew \( \Theta \)-cyclic code over \( R \).

Proposition 4.3. Let \( \Theta \) be an automorphism of \( R \), and \( n \) an integer divisible by the order of \( \Theta \) and \( \lambda \) a unit in \( R \) which is fixed by \( \Theta \). If \( C = \bigoplus_{i=0}^{k-1} C_i \) is a skew \( \Theta \)-cyclic code of length \( n \) over \( R \), then the dual code of skew \( \Theta \)-cyclic code \( C \) is a skew \( \Theta \)-cyclic code and \( C^\perp = \bigoplus_{i=0}^{k-1} C_i^\perp \).
Proof. Let \((x_0, x_1, \ldots, x_{k-1})\) be arbitrary in \(\oplus_{i=0}^{k-1} C_i^\perp\), i.e., \(x_i \in C_i^\perp\). For any codeword \((c_0, c_1, \ldots, c_{k-1})\) \(\in C\), \(c_i \in C_i\), so \(x_ic_i = 0\), and hence,

\[
(x_0, x_1, \ldots, x_{k-1}) \cdot (c_0, c_1, \ldots, c_{k-1}) = x_0c_0 + x_1c_1 + \cdots + x_kc_{k-1} = 0.
\]

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

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

Therefore, \(C^\perp = \oplus_{i=0}^{k-1} C_i^\perp\). \(\square\)

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

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

Using Proposition 4.4, we have the following result.

**Theorem 4.5.** Let \(\alpha, \beta\) be distinct nonzero elements of the field \(F\) fixed by \(\Theta\), where \(\Theta\) is an automorphism of \(F\). Assume that \(n\) is an integer divisible by the order of \(\Theta\). Then a skew \(\Theta\)-\(\alpha\) - and \(\beta\)-linear code \(C\) of length \(n\) over \(F\) is both skew \(\Theta\)-\(\alpha\) - and \(\beta\)-constacyclic if and only if \(C = \{0\}\) or \(C = F^n\).

**Proof.** \((\Leftarrow)\) is obvious.

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

The Hermitian inner product is defined as

\[
x \circ_{F^2} y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1},
\]

where \(x = (x_0, x_1, \ldots, x_{n-1})\), \(y = (y_0, y_1, \ldots, y_{n-1}) \in F^n_2\) and \(y_i = y_0^i\). The Hermitian dual code of \(C\) is defined as

\[
C^\perp = \{x \in F^n_2 \mid \sum_{i=0}^{n-1} x_i y_i = 0, \forall y \in C\}.
\]

If \(C \subseteq C^\perp\), then \(C\) is called a Hermitian self-orthogonal code. The code \(C\) satisfying \(C^\perp \subseteq C\) is called a Hermitian dual-containing code. Hermitian dual-containing codes are also known as weakly Hermitian self-dual codes. If \(C^\perp = C\), then \(C\) is called a Hermitian self-dual code. It is easy to see that \(\{0\}\) is a Hermitian self-orthogonal code and \(F^n_2\) 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 $F_q^n$, we define $V^\perp$ to be the set

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

It is well-known from [9] that $|V| = |V^\perp|$. If $C$ is a $q^2$-ary linear code, then $C^\perp$ is also a $q^2$-ary linear code, and by definition, $C^\perp = (C^\perp)^\perp$. Since $|C^\perp| = |(C^\perp)^\perp|$, it follows that $|C^\perp| = |C^\perp|$, i.e., $|C||C^\perp| = q^{2n}$. Furthermore, it is easy to check that $(C^\perp)^\perp = C$. Since the Hermitian inner product over $F_q$ 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 $\mathcal{R} = F_q \oplus F_1 \oplus \cdots \oplus F_{k-1}$, where $F_i = F_q^{q^i}$ for all $i = 0, \ldots, k-1$.

Recall that $x_i \circ_F y_i$ denotes the Hermitian inner product over $F_i$ for all $i = 0, \ldots, k-1$. Then the Hermitian inner product over $\mathcal{R}$ is defined as

$$x \circ_{\mathcal{R}} y = (x_0, \ldots, x_{k-1}) \circ_{\mathcal{R}} (y_0, \ldots, y_{k-1}) = (x_0 \circ_{F_0} y_0, x_1 \circ_{F_1} y_1, \ldots, x_{k-1} \circ_{F_{k-1}} y_{k-1}),$$

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

$$C^\perp = \{ x \in \mathcal{R}^n \mid x \circ_{\mathcal{R}} y = (x_0 \circ_{F_0} y_0, x_1 \circ_{F_1} y_1, \ldots, x_{k-1} \circ_{F_{k-1}} y_{k-1}) = 0_{\mathcal{R}}, \forall y \in C \}.$$  

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

(i) For any skew $\Theta$-$\lambda$-constacyclic code $C = \bigoplus_{i=0}^{k-1} C_i$ of length $n$ over $\mathcal{R}$, its Hermitian dual code is $C^\perp = \bigoplus_{i=0}^{k-1} C_i^\perp$.

(ii) $C$ is skew $\Theta$-$\lambda$-Hermitian self-dual if and only if $C_i$ are skew $\Theta_i$-$\lambda_i$-Hermitian self-dual for all $i = 0, \ldots, k-1$.

(iii) $C$ is Hermitian self-orthogonal if and only if $C_i$ are skew $\Theta_i$-$\lambda_i$-Hermitian self-orthogonal for all $i = 0, \ldots, k-1$.

(iv) $C$ is skew $\Theta$-$\lambda$-Hermitian dual-containing if and only if $C_i$ are skew $\Theta_i$-$\lambda_i$-Hermitian dual-containing for all $i = 0, \ldots, k-1$.

(v) $C$ is skew $\Theta$-$\lambda$-Hermitian LCD if and only if $C_i$ are skew $\Theta_i$-$\lambda_i$-Hermitian LCD for all $i = 0, \ldots, k-1$.

(vi) For any skew $\Theta$-linear code $C$ of length $n$ over $\mathcal{R}$, $|C||C^\perp| = |\mathcal{R}^n|$.  

Proof. We first prove the part (i). The proof of part (ii), (iii), (iv) and (v) are straightforward to see from (i). Let \((x, x_1, \ldots, x_{k-1})\) be arbitrary in \(\oplus_{i=0}^{k-1} C_i^{⊥,n}\). That means, for \(0 \leq i \leq k-1\), \(x_i \in C_i^{⊥,n}\), and hence, for any \(c = (c_0, c_1, \ldots, c_{k-1}) \in C\),
\[
x \circ_R c = (x, x_1, \ldots, x_{k-1}) \ast (c_0, c_1, \ldots, c_{k-1})
= (x_0 \circ_{F_q} c_0, x_1 \circ_{F_q} c_1, \ldots, x_{k-1} \circ_{F_q} c_{k-1}) = 0_R,
\]
implying \((x_0, x_1, \ldots, x_{k-1}) \in C^{⊥,n}\). This shows that \(\oplus_{i=0}^{k-1} C_i^{⊥,n} \subseteq C^{⊥,n}\). On the other hand, for all \(x = (x_0, x_1, \ldots, x_{k-1}) \in C^{⊥,n}\), we have
\[
(x_0, \ldots, x_{k-1}) \ast (y_0, \ldots, y_{k-1}) = (x_0 \circ_{F_q} y_0, \ldots, x_{k-1} \circ_{F_q} y_{k-1}) = 0_R
\]
for all \(y = (y_0, y_1, \ldots, y_{k-1}) \in C\). Note that \(x_i = (x_{i,0}, \ldots, x_{i,n-1})\), \(y_i = (y_{i,0}, \ldots, y_{i,n-1}) \in C_1\) for all \(i = 0, \ldots, k-1\). Since \(x_i \circ_{F_q} y_i = 0_{F_q}\), for any \(y_i \in C_1\), we have \(x_i \in C_i^{⊥,n}\) for all \(i = 0, \ldots, k-1\). This means that \(x \in \oplus_{i=0}^{k-1} C_i^{⊥,n}\).
It follows that \(C^{⊥,n} \subseteq \oplus_{i=0}^{k-1} C_i^{⊥,n}\). Hence \(C^{⊥,n} = \oplus_{i=0}^{k-1} C_i^{⊥,n}\). From (i), we have
\[
|C^{⊥,n}| = \prod_{i=0}^{k-1} |C_i^{⊥,n}| = \prod_{i=0}^{k-1} \left|\frac{q^{2n}}{|C_i|}\right| = \left|\frac{\prod_{i=0}^{k-1} q^2}{\prod_{i=0}^{k-1} |C_i|}\right| = |R^n| |C|.
\]
Therefore, \(|C||C^{⊥,n}| = |R^n|\). \hfill \qed

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

Lemma 4.7. Let \(C\) be a code of even length \(n\) over \(R\). Assume that the order of \(\Theta\) is 2. Then \(C\) is a skew \(\Theta\)-constacyclic code if and only if \(C^{⊥,n}\) is a skew \(\Theta\)-constacyclic code. In particular, if \(\lambda^2 = 1\), then \(C\) is a skew \(\Theta\)-constacyclic code if and only if \(C^{⊥,n}\) is a skew \(\Theta\)-constacyclic code.

Proof. We first observe that for each unit \(\lambda\) in \(F_q^2\), \(\lambda \in F_q^2\) if and only if \(\lambda^{-1} \in F_q^2\). Let \(u = (u_0, u_1, \ldots, u_{n-1}) \in C\) and \(v = (v_0, v_1, \ldots, v_{n-1}) \in C^{⊥,n}\). We have
\[
(\Theta^{-1}(u_1), \Theta^{-1}(u_2), \ldots, \Theta^{-1}(u_{n-1}), \Theta^{-1}(u_0)) \circ_R (v_0, v_1, \ldots, v_{n-1})
= \lambda((\Theta^{-1}(u_1), \Theta^{-1}(u_2), \ldots, \Theta^{-1}(u_{n-1}), \Theta^{-1}(u_0)) \circ_R (v_0, v_1, \ldots, v_{n-1}))
= \lambda(\Theta^{-1}(\lambda^{-1}u_0)v_{n-1} + \sum_{i=1}^{n-1} \Theta^{-1}(u_i)v_{i-1}).
\]
By assumption, \(n\) is a multiple of the order of \(\Theta\) and \(\lambda^{-1}\) is fixed by \(\Theta\). It follows that
\[
0 = \Theta(0) = \Theta(\lambda(\Theta^{-1}(\lambda^{-1}u_0)v_{n-1} + \sum_{i=1}^{n-1} \Theta^{-1}(u_i)v_{i-1}))
\]
Proof. \(\lambda\) is a skew \(\Theta\)-\(\lambda^{-1}\)-constacyclic code. The converse follows from the fact that \((C^{⊥\mu})^{⊥\mu} = C\). This implies that \(C\) is a skew \(\Theta\)-\(\lambda\)-constacyclic code if and only if \(C^{⊥\mu}\) is a skew \(\Theta\)-\(\lambda^{-1}\)-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 \(\varphi_i : F_{q^2}[x; \Theta] \rightarrow F_{q^2}[x; \Theta]S^{-1}\) be defined by

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

Then \(\varphi_i\) is a ring anti-monomorphism for all \(i = 0, \ldots, k - 1\).

(ii) [14, Section 3] Let \(\phi_i : F_{q^2}[x; \Theta] \rightarrow F_{q^2}[x; \Theta]\) be defined by

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

Then \(\phi_i\) is a ring automorphism for all \(i = 0, \ldots, k - 1\).

**Lemma 4.9.** Let \(\Theta\) be an automorphism of \(R\). Assume that the order of \(\Theta\) is 2 and \(\lambda^2 = 1 \in R\). Let \(a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}\) and \(b(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}\) be in \(R[x; \Theta]\), where \(a_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,k-1}); b_i = (b_{i,0}, b_{i,1}, \ldots, b_{i,k-1})\). Then the following statements are equivalent:

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

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

(iii) \(a(x)b(x) = 0\) in \(R[x; \Theta]\).

**Proof.** (i)\(\Leftrightarrow\)(ii) follows directly from the definition of \(\varphi\). We need to prove that (ii)\(\Leftrightarrow\)(iii). Suppose that \(a(x)b(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in R[x; \Theta]\). Since \(\lambda \in R\) such that \(\lambda^2 = 1\) and \(n\) is even, we have

\[
c_k = \sum_{i+j=k} a_i \Theta^j (b_j) + \sum_{i+j=k+n} \lambda a_i \Theta^j (b_j)
\]

\[
= \lambda \left( \sum_{i+j=k} a_i \Theta^{k-j} (\lambda b_j) + \sum_{i+j=k+n} a_i \Theta^{n+k+j} (b_j) \right)
\]
Let \( C \) be the skew polynomial \( \phi(x^{\text{deg}(h(x))}) \) be a right divisor of \( x^n - \lambda \) and \( h(x) := \frac{x^n - \lambda}{g(x)} \).

Let \( C \) be the skew \( \Theta \)-\( \lambda \)-constacyclic code generated by \( g(x) \). Then the following statements hold:

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

(ii) The Hermitian dual \( C^{\perp_H} \) is a skew \( \Theta \)-\( \lambda \)-constacyclic code generated by \( \phi(x^{\text{deg}(h(x))}) \varphi(h(x))) \).

Proof. We have

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

Therefore,

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

Hence, \( \phi(x^{\text{deg}(h(x))}) \varphi(h(x))) \) is a right divisor of \( x^n - \lambda \), proving (i). We can see that \( g(x)h(x) = x^n - \lambda = 0 \) in \( \mathbb{F}_{q^n}/(x^n - \lambda) \). Applying Lemma 4.7, we have

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

By Theorem 2.3, we have

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

This implies that \( \langle \phi(x^{\text{deg}(h(x))}) \varphi(h(x))) \rangle = C^{\perp_H} \), showing (ii). □
Theorem 4.11. Let Θ be an automorphism of R. Assume that the order of Θ is 2, λ² = 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 − λ. Then the skew Θ-λ-constacyclic code generated by g(x) is Hermitian self-dual if and only if

\[(\sum_{i=0}^{k-1} g_i x^i)(Θ^{-k-1}(g_0^{-1}) + \sum_{i=1}^{k-1} Θ^{i-k-1}(g_0^{-1} g_{k-i})x^i + x^k) = x^n − λ.\]

Proof. Let C be the skew Θ-λ-constacyclic code generated by g(x) and g^⊥ 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 = x^{\frac{n}{2}}. Applying Theorem 4.10, we have g^⊥ = Θ^{k+1}(h_0)x^k + \cdots + Θ^2(h_{k-1})x + 1. Since C is Hermitian self-dual, we have g^⊥(x) = Θ^{k+1}(h_0)g(x) = Θ^{k+1}(h_0)(\sum_{i=0}^{k-1} g_i x^i + x^k). Comparing coefficients, we have

\[(\sum_{i=0}^{k-1} g_i x^i)(Θ^{-k-1}(g_0^{-1}) + \sum_{i=1}^{k-1} Θ^{i-k-1}(g_0^{-1} g_{k-i})x^i + x^k) = x^n − λ.\]

Conversely, if

\[(\sum_{i=0}^{k-1} g_i x^i)(Θ^{-k-1}(g_0^{-1}) + \sum_{i=1}^{k-1} Θ^{i-k-1}(g_0^{-1} g_{k-i})x^i + x^k) = x^n − λ,\]

then h(x) = Θ^{-k-1}(g_0^{-1}) + \sum_{i=1}^{k-1} Θ^{i-k-1}(g_0^{-1} g_{k-i})x^i + x^k. By applying Theorem 4.10 again, g^⊥ = φ(x^{\deg h(x)}φ(h(x))), completing our proof. □

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 −λ = g_0 Θ^{-k-1}(g_0^{-1}). Since λ is fixed by Θ, we can see that λ can be expressed as λ = −Θ^{k+1}(g_0)g_0^{-1}. Note that the order of Θ is 2. Then we have λ = −1 if k is odd or λ = −Θ(g_0)g_0^{-1} if k is even. Therefore, if k is odd and λ ≠ −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{F[x]}{(x^n - 1)} 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{F[x; Θ]}{(x^n - 1)} can be considered as a left F[x; Θ] 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

SKEW CONSTACYCLIC CODES

431
the set $R_n$, and let $r(x) \in F[x; \Theta]$. Define multiplication of the element of $R_n$ by the elements of $F[x; \Theta]$ as follows:

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

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

**Theorem 5.1** ([16, Theorem 9]). $R_n$ is a left $F[x; \Theta]$-module where multiplication 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 $\Theta$-cyclic code if and only if $C$ is a left $F[x; \Theta]$-submodule of the left $F[x; \Theta]$-module $R_n$.

We now give a definition of skew $\Theta$-$\lambda$-constacyclic codes of arbitrary length over semi-simple rings $R = F_0 \oplus F_1 \oplus \cdots \oplus F_{k-1}$.

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

We have the following result.

**Proposition 5.4.** Let $C$ be a skew $\Theta$-$\lambda$-constacyclic code of arbitrary length $n$ over $R$. Then the following results hold true:

(i) The skew $\Theta$-$\lambda$-constacyclic code $C$ has the form $C = \oplus_{i=0}^{k-1} C_i$, where $C_i$ is a $\Theta$-$\lambda$-constacyclic code of length $n$ over $F_i$ $(i = 0, \ldots, k - 1)$. Moreover, the skew $\Theta$-$\lambda$-constacyclic code $C$ is a linear code over $R$ if and only if the skew $\Theta$-$\lambda$-constacyclic code $C_i$ is a linear code over $F_i$ $(i = 0, \ldots, k - 1)$.

(ii) Let $\lambda = (\lambda_0, \ldots, \lambda_{k-1})$ be a unit of $R$, where $\lambda_i$ is fixed by $\Theta_i$. A code $C = \oplus_{i=0}^{k-1} C_i$ is a skew $\Theta$-$\lambda$-constacyclic code of length $n$ over $R$ if and only if each code $C_i$ is a skew $\Theta_i$-$\lambda_i$-constacyclic code of length $n$ over $F_i$.

**Proof.** We can see that the structure of skew $\Theta$-$\lambda$-constacyclic code $C_i$ of length $n$ can be identified with the structure of the left $F_i[x; \Theta]$-submodule of $R$ for all $i = 0, \ldots, k - 1$. Therefore, part (i) and (ii) are held. \hfill $\square$

From Proposition 5.4, we have a characterization of skew $\Theta$-$\lambda$-constacyclic codes as follows.

**Theorem 5.5.** A code $C$ over $R$ is a skew $\Theta$-$\lambda$-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 $\Theta$-$\lambda$-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 $\Theta$-$\lambda$-constacyclic codes over $R$.

Proposition 5.7. Let $\lambda = (\lambda_0, \ldots, \lambda_{k-1})$ be a unit of $R$, and $C = \oplus_{i=0}^{k-1} C_i$ a skew $\Theta$-$\lambda$-constacyclic code of length $n$ over $R$, where $C_i$ is a skew $\Theta_i$-$\lambda_i$-constacyclic code of length $n$ over $F_i$. Then $C = \langle (g_0(x), \ldots, g_{k-1}(x)) \rangle$, where $C_i$ is a skew $\Theta_i$-$\lambda_i$-constacyclic code generated by a monic polynomial of minimal degree $g_i(x)$ in $C_i$ for $i = 0, \ldots, k-1$.

Proof. It is straightforward from that

$$\phi : R[x, \Theta] / \langle x^n - \lambda \rangle \rightarrow \bigoplus_{i=0}^{k-1} F_i[x, \Theta_i] / \langle x^n - \lambda_i \rangle$$

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 $g(x)$ is a right divisor of $x^n - \lambda$. Therefore, we can prove that if $C$ is a skew $\Theta$-$\lambda$-constacyclic code and $C = \langle g_0, \ldots, g_{k-1} \rangle$ is a left submodule of $R$, then each $g_i(x)$ is a right divisor of $x^n - \lambda_i$ over $F_i$ for $i = 0, \ldots, k-1$.

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

Definition 5.9. Let $F$ be a finite field. A subset $C$ of $F^n$ 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 $F^n$.

(b) If

$$c = (c_0, 0, \ldots, c_{l-1}, 0, c_1, 0, \ldots, c_{l-1}, 1, \ldots, c_s-1, 0, c_s, 0, \ldots, c_{s-1,l-1}) \in C,$$

then

$$T_{\Theta, sl}(c) = (c_{s-1,0}, c_{s-1,1}, \ldots, c_s-1, l-1, c_0, 0, \ldots, c_{l-1}, 0, \ldots, c_s-2, 0, \ldots, c_{s-2,l-1}) \in C.$$

Equivalently, $C$ is a quasi-cyclic code of length $n = sl$ and index $l$ if $C$ is a $F[x] / \langle x^s-1 \rangle^l$-submodule of $F[x] / \langle x^s-1 \rangle^l$.

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 $x^m - 1$ in $F[x; \Theta]$, then $f(x)$ is also a factor of $x^n - 1$ in the usual polynomial ring $F[x]$.

Applying Proposition 5.10, we have a result for skew $\Theta$-cyclic codes of length $n$ over $R$.
Theorem 5.11. Let \( \Theta = (\Theta_0, \ldots, \Theta_{k-1}) \) be an automorphism of \( R \) with \( |\langle \Theta_i \rangle| = m_i \), and \( C = (g(x)) = (g_0(x), \ldots, g_{k-1}(x)) \) be a skew \( \Theta \)-cyclic code of length \( n \) over \( R \). If \( \gcd(m_i, n) = 1 \) for all \( i = 0, \ldots, k-1 \), 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 \( F_i \) for all \( i = 0, \ldots, k-1 \). Hence, \( C = \bigoplus_{i=0}^{k-1} C_i \) is a cyclic code of length \( n \) over \( R \), by Proposition 3.3.

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

\[
\begin{align*}
c(x) &= c_{0,0} + c_{0,1}x + \cdots + c_{0,d-1}x^{d-1} + c_{1,0}x^d + \cdots + c_{s-1,0}x^{sd-d} + \cdots + c_{s-1,d-1}x^{sd-1} \\
&= x^{d-tn} + \cdots + x^{d-tn} * c_{0,0} + x^{d-tn} * c_{0,0} \cdot x^{d-tn} + \cdots + x^{d-tn} * c_{s-1,d-1} \cdot x^{d-tn} \cdot \Theta_{s-1,1} \cdot x^{d-tn} + \cdots + x^{d-tn} * c_{s-1,d-1} \cdot x^{d-tn}.
\end{align*}
\]

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

\[
x^{am} * c(x) = x^{d-tn} * (c_{0,0} + \cdots + c_{0,d-1}x^{d-1} + c_{1,0}x^d + \cdots + c_{s-1,0}x^{sd-d} + \cdots + c_{s-1,d-1}x^{sd-1})
\]

\[
= x^{d-tn} * c_{0,0} + \cdots + x^{d-tn} * c_{0,0} \cdot x^{d-tn} + \cdots + x^{d-tn} * c_{s-1,d-1} \cdot x^{d-tn} \cdot \Theta_{s-1,1} \cdot x^{d-tn} + \cdots + x^{d-tn} * c_{s-1,d-1} \cdot x^{d-tn}.
\]

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

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

Similarly, we can see that

\[
\Theta^{d-tn}(c_{s-1,1})x^{d-tn + sd - d + 1} = \Theta^{am}(c_{s-1,1})x^{n-tn+1} = c_{s-1,1} \cdot x,
\]

\[
\vdots
\]
This shows that \( \gcd(\langle \mathbf{T} \rangle) \) was provided in [16].

Let \( \Theta \) be an automorphism of \( F \) with \( |\langle \Theta \rangle| = m \), and \( C = \langle g(x) \rangle \) be a skew \( \Theta \)-cyclic code of length \( n \) over \( F \). 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 \( i = 0, \ldots, k-1 \), where \( d_i \) is not necessarily be equal to 1 as in Theorem 5.13.

**Theorem 5.13.** Let \( C = \langle g(x) \rangle = \langle g_0(x), g_1(x) \rangle \) be a skew \( \Theta \)-cyclic code of length \( n \) and \( \Theta \) an automorphism of \( F \) with \( |\langle \Theta \rangle| = m_i \). If \( \gcd(m_i, n) = d_i \) for all \( i = 0, \ldots, k-1 \), 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 \( i = 0, \ldots, k-1 \), 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 \( \Theta \)-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 $F_8 = F_2(a)$, where $a^3 = a + 1$. Let $\Theta$ be the Frobenius homomorphism of $F_8$, i.e., $\Theta(u) = u^2$ for all $u \in F_8$. It is easy to see that the order of $\Theta$ is $m = 3$. Let us consider the skew $\Theta$-cyclic code of length 5. According to Proposition 5.10, in this case $\gcd(3, 5) = 1$, if $f(x)$ is a factor of $x^3 - 1$ in $F_8[x, \Theta]$, then $f(x)$ is also a factor of $x^3 - 1$ in the usual polynomial ring $F_8[x]$. In fact, nontrivial right divisors of $x^3 - 1$ in $F_8[x, \Theta]$ are $f_1(x) = x - 1$, $f_2 = x^3 + x^2 + x + 1$. These factors are also factors of $x^3 - 1$ in $F_8[x]$.

Example 5.16. We consider $F = \mathbb{Z}_2(a)$, $a$ is a root of $x^4 + x + 1$, and $\Theta(z) = z^2$. It is clear that the order of $\Theta$ is 4. In $F[x; \Theta]$, we can see that $x^6 - 1 = (x^3 + a^{10}x^2 + a^7x + a^5)*(x^3 + a^3x^2 + a^5x + a^{15})$. As mentioned in Theorem 5.13, the skew $\Theta$-cyclic code generated by $f(x) = x^3 + a^5x^2 + a^7x + a^{15}$ 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, Chiang Mai University.

References


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