Research Article

Xiying Zheng* and Bo Kong

Constacyclic codes over
\[ \mathbb{F}_p^n[u_1, u_2, \cdots, u_k]/\langle u_i^2 = u_i, u_iu_j = u_ju_i \rangle \]

Abstract: In this paper, we study linear codes over ring \( R_k = \mathbb{F}_{p^m}[u_1, u_2, \cdots, u_k]/\langle u_i^2 = u_i, u_iu_j = u_ju_i \rangle \) where \( k \geq 1 \) and \( 1 \leq i, j \leq k \). We define a Gray map from \( R_1^n \) to \( \mathbb{F}_p^{2n} \) and give the generator polynomials of constacyclic codes over \( R_k \). We also study the MacWilliams identities of linear codes over \( R_k \).

Keywords: Constacyclic codes, Cyclic codes, Gray map, Self-orthogonal codes

MSC: 94B15

1 Introduction

Constacyclic codes are an important class of linear codes and have good error-correcting properties as well as have practical applications since they can be encoded with shift registers. Constacyclic codes over finite rings are well-known as they have rich algebraic structures for efficient error detection and correction, which explain their preferred role in engineering. In recent years, due to their rich algebraic structure, constacyclic codes have been studied over finite fields [1-4]. The class of finite chain rings has been studied by many authors, [5-8]. There is a lot of work on constacyclic codes over finite rings of the form \( \mathbb{F}_{p^m} + u \mathbb{F}_{p^m} + \cdots + u^{e-1} \mathbb{F}_{p^m} \) by many authors, where \( u^e = 0 \).

For example, Chen et al. in [9] gave the structures of all \((a + bu)\)-constacyclic codes of length \( 2p^s \) over ring \( \mathbb{F}_{p^m} + u \mathbb{F}_{p^m} \). Sobhani in [10] completely determined the structure of \((\alpha + u^2)\)-constacyclic codes of length \( p^k \) over \( \mathbb{F}_{p^m} + u \mathbb{F}_{p^m} + u^2 \mathbb{F}_{p^m} \). Liu and Xu in [11] gave the structure of cyclic and negacyclic codes of length \( 2p^s \) over \( \mathbb{F}_{p^m} + u \mathbb{F}_{p^m} \). Abualrub and Siap in [12] gave the structure of \((1 + u)\)-constacyclic codes of arbitrary length \( n \) over \( \mathbb{F}_2 + u \mathbb{F}_2 \). Kai et al. in [13] studied the \((1 + \lambda u)\)-constacyclic codes of arbitrary length \( n \) over \( \mathbb{F}_p[u]/(u^m) \), where \((1 + \lambda u)\) is a unities of \( \mathbb{F}_p[u]/(u^m) \). Guenda and Gulliver in [14] gave the structure of repeated root constacyclic codes of length \( mp^s \) over \( \mathbb{F}_{p^r} + u \mathbb{F}_{p^r} + \cdots + u^{e-1} \mathbb{F}_{p^r} \).

The class of finite commutative rings of the form \( R + uR \) has been studied by many authors, where \( u^2 = 1 \). For example, in [15] Cengellenmis gave the structure of cyclic codes over \( \mathbb{F}_3 + v \mathbb{F}_3 \), where \( v^2 = 1 \). Özen et al. in [16] gave the structure of cyclic and some constacyclic codes over the ring \( \mathbb{Z}_4[u]/(u^2 - 1) \). The class of finite commutative rings of the form \( \mathbb{F}_{p^m} + u \mathbb{F}_{p^m} \) has been studied by many authors, where \( u^2 = u \). For example, in [17], Kong and Chang described the structure of cyclic codes and self dual cyclic codes over \( \mathbb{F}_p + u \mathbb{F}_p \), where \( u^2 = u \). Cengellenmis et al. in [18] gave the structure of codes over \( \mathbb{F}_2[u_1, u_2, \cdots, u_k]/\langle u_i^2 = u_i, u_iu_j = u_ju_i \rangle \) with a Gray map. Li et al. in [19] gave the structure of linear codes over \( \mathbb{Z}_4[u, v]/(u^2 = u, v^2 = v, uv = vu) \). In [20], the generators of cyclic codes and \((\lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv)\)-constacyclic codes over \( \mathbb{F}_p + u \mathbb{F}_p + v \mathbb{F}_p + uv \mathbb{F}_p \) were...
The purpose of this paper is to continue this line of research. We determine the algebraic structures of all $\lambda$-constacyclic codes of $\mathbb{F}_{p^n}[u_1, u_2, \ldots, u_k]/(u_i^2 = u_i, u_iu_j = u_ju_i)$, where $\lambda$ is an arbitrary unit of the ring $\mathbb{F}_{p^n}[u_1, u_2, \ldots, u_k]/(u_i^2 = u_i, u_iu_j = u_ju_i)$.

The remainder of this paper is organized as follows. In section 2, we provide the preliminaries that we need and define a Gray map from $R_k^q$ to $\mathbb{F}_{p^n}^q$. In section 3, we study the Gray image of linear codes over $R_k$. In section 4, we give the structure of constacyclic codes of arbitrary length over $R_k$.

2 Preliminaries

An ideal $I$ of a finite commutative ring $R$ is called principal if it is generated by one element. $R$ is a principal ideal ring if its ideals are principal. $R$ is called a local ring if $R$ has a unique maximal ideal. $R$ is called a chain ring if its ideals are linearly ordered by inclusion.

As defined in [18], let

$$R_k = \mathbb{F}_{p^n}[u_1, u_2, \ldots, u_k]/(u_i^2 = u_i, u_iu_j = u_ju_i).$$

For any subset $A \subseteq \{1, 2, \ldots, k\}$, let

$$u_A = \prod_{i \in A} u_i$$

with the convention that $u_{\emptyset} = 1$. Then any element of $R_k$ can be represented as

$$\sum_{A \subseteq \{1,2,\ldots,k\}} c_A u_A, c_A \in \mathbb{F}_{p^n}.$$

We can easily observe that

$$u_Au_B = u_{A\cup B}.$$

Let $P_k$ be the power set of the set $\{1, 2, \ldots, k\}$.

It follows that

$$\left( \sum_{A \in P_k} c_A u_A \right) \left( \sum_{B \in P_k} c_B u_B \right) = \sum_{A \in P_k} \left( \sum_{A \subseteq B} c_A c_B \right) u_B.$$

By the same method of Theorem 2.3 and Lemma 2.4 in [18] we have the following theorem:

Theorem 2.1. The ideal $\langle w_1, w_2, \ldots, w_k \rangle$, where $w_i \in \{ u_i, 1 - u_i \}$, is an ideal of cardinality $p^m(2^k - 1)$ and there are $2^k$ such ideals.

Let $\omega_i = \langle w_1, w_2, \ldots, w_{ik} \rangle$ be an ideal as described in Theorem 2.1, where $w_{ij} \in \{ u_j, 1 - u_j \}$, $1 \leq i \leq 2^k$. An element $e$ is called an idempotent element if $e^2 = e$. For $x, y \in R_k$, $x, y$ are called orthogonal if $xy = 0$. Let $e_i = w_{i1}w_{i2}\cdots w_{ik}$, where $i = 1, 2, \ldots, 2^k$. We know that $u_i^2 = u_i$, $(1 - u_i)^2 = 1 - u_i$, $u_i(1 - u_i) = 0$, so $e_1, e_2, \ldots, e_{2^k}$ are pairwise orthogonal non-zero idempotent elements over $R_k$. By the induction method over $R_k$, we have $1 = e_1 + e_2 + \cdots + e_{2^k}$. By the Chinese Remainder Theorem, we have that $R_k = e_1R_k + e_2R_k + \cdots + e_{2^k}R_k$, and for any element $r \in R_k$, $r$ can be expressed uniquely as $r = r_1e_1 + r_2e_2 + \cdots + r_{2^k}e_{2^k}$, where $r_i \in \mathbb{F}_{p^n}, i = 1, 2, \ldots, 2^k$.

Theorem 2.2. $R_k \cong R_k/\omega_1 \times \cdots \times R_k/\omega_{2^k}$.

Proof. First, we prove that $\cap_{i=1}^{2^k} \omega_i = \{0\}$.

We use mathematical induction over $R_k$.

Base case: Setting over $R_1$, we get

$$\cap_{i=1}^{2} \omega_i = \langle u_1 \rangle \cap \{1 - u_1 \} = \langle u_1 - u_1^2 \rangle = \{0\}.$$

Induction step: Over $R_{k-1}$, suppose that

$$\cap_{i=1}^{2^{k-1}} \omega_i = \{0\},$$

$$\cap_{i=1}^{2^{k-1}} \omega_i = \{0\}.$$
where $\omega_i = \{w_{ij}, w_{ij+1}, \ldots, w_{ij+k-1}\}, w_{ij} \in \{u_j, 1-u_j\}, 1 \leq i \leq 2^{k-1}, 1 \leq j \leq k-1$.

Then over $R_k$

$$\bigotimes_{i=1}^{2^k} \omega_i = \bigotimes_{i=1}^{2^k} \{w_{ij}, w_{ij+1}, \ldots, w_{ij+k-1}\} \bigotimes_{i=1}^{2^k-1} \{w_{ij}, w_{ij+1}, \ldots, w_{ij+k-1}, 1-u_k\}$$

$$= \bigotimes_{i=1}^{2^k-1} \{\omega_i + (u_k)\} \bigotimes_{i=1}^{2^k-1} \{\omega_i + (1-u_k)\} = \bigotimes_{i=1}^{2^k-1} \omega_i + (u_k) \bigotimes_{i=1}^{2^k-1} \omega_i + (1-u_k)$$

$$= \{u_k\} \bigcap \{1-u_k\} = (u_k - u_k^2) = \{0\},$$

where $\omega_i = \{w_{ij}, w_{ij+1}, \ldots, w_{ij+k}\}, w_{ij} \in \{u_j, 1-u_j\}, 1 \leq i \leq 2^k, 1 \leq j \leq k$.

Secondly, we prove that $\omega_i, \omega_j$ are pairwise coprime. For any two different ideals $\omega_i, \omega_j$, there exist $u_i, u_j$ such that $1 \in \omega_i + \omega_j$, then $\omega_i + \omega_j = R_k$. So $\omega_i, \omega_j$ are pairwise coprime.

By the Chinese Remainder Theorem, we can get that $R_k \equiv R_k/\omega_1 \times \cdots \times R_k/\omega_{2^k}$.

**Theorem 2.3.** The ring $R_k$ has cardinality $p^{m2^k}$. The ideal $\omega_i$ is a maximal ideal of $R_k$, where $i = 1, 2, \ldots, 2^k$. Consequently, $R_k \cong \mathbb{F}_{p^{m}}$.

**Proof.** By Theorem 2.2, we have that $|R_k| = |R_k/\omega_i| \times \cdots \times |R_k/\omega_{2^k}|$. By Theorem 2.1 $|\omega_i| = p^{m(2^k-1)}$, where $i = 1, 2, \ldots, 2^k$.

We have that $|R_k| = p^{m2^k}$. Thus $|R_k/\omega_i| = p^m$, where $i = 1, 2, \ldots, 2^k$. So $\omega_i$ is a maximal ideal of $R_k$, we can get that $R_k/\omega_i \cong \mathbb{F}_{p^m}$, where $i = 1, 2, \ldots, 2^k$. So $R_k \cong \mathbb{F}_{p^{m}}$.

**Corollary 2.4.** There are $(p^m - 1)2^k$ units in the ring $R_k$.

**Proof.** There are $(p^m - 1)$ units in $\mathbb{F}_{p^m}$. By Theorem 2.3, we know there are $(p^m - 1)2^k$ units in the ring $R_k$.  

**Theorem 2.5 (cf. [21, Theorem 2]).** The ring $R_k$ is a principal ideal ring, not a chain ring.

We define the Gray map as follows:

For $r = r_1e_1 + r_2e_2 + \cdots + r_{2^k}e_{2^k} \in R_k$, we define $\phi : r \mapsto (r_1, r_2, \ldots, r_{2^k})$. We expand $\phi$ as:

$$\phi : R_k^n \rightarrow \mathbb{F}_{p^m}^{2^k \times n}$$

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto (r_1, 0, \ldots, r_{1,n-1}, r_2, 0, \ldots, r_{2,n-1}, \ldots, r_{2^k,0}, \ldots, r_{2^k,n-1}),$$

where $c_i = r_{i,0}e_1 + r_{i,1}e_2 + \cdots + r_{i,2^{k-1}}e_{2^k} \in R_k$.

A linear code $C$ of length $n$ over $R_k$ is an $R_k$-submodule of $R_k^n$. Every codeword $c$ in such a code $C$ is just an $n$-tuple of the form $c = (c_0, c_1, \ldots, c_{n-1}) \in R_k^n$, and can be represented by a polynomial in $R_k[x]$ as follows:

$$c = (c_0, c_1, \ldots, c_{n-1}) \leftrightarrow c(x) = \sum_{i=0}^{n-1} c_i x^i \in R_k[x].$$

We define a constacyclic shift operator as:

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

If for any $c \in C$, we have $\sigma_\lambda(c) \in C$, then $C$ is called $\lambda$-constacyclic code over $R_k$. Let $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$ be two elements of $R_k^n$. Then the usual inner product of $a$ and $b$ is defined as $a \cdot b = \sum_{i=0}^{n-1} a_i b_i$. If $a \cdot b = 0$, then $a$ and $b$ are said to be orthogonal.

The dual of a code $C$ is $C^\perp = \{ a \mid b \in C, a \cdot b = 0 \}$, which is also a linear code. A code $C$ is self-orthogonal if $C \subseteq C^\perp$ and self dual if $C = C^\perp$.

For all $r \in R_k$, define the Lee weight of $r$ as follows: $w_L(r) = w_H(\phi(r))$, where let $w_H(\phi(r))$ denote the Hamming weight of the image of $r$ under $\phi$.  

For all \( x = (x_1, x_2, \ldots, x_n) \in R_k^n \), define the Lee weight of \( x \) as follows \( w_L(x) = \sum_{i=1}^n w_L(x_i) \), the Lee distance of codewords \( x, y \) over \( R_k^n \) is defined as \( d_L(x, y) = w_L(x - y) \). The Lee distance of \( C \) is defined by

\[
\text{d}_L(C) = \min\{d_L(x - y), x, y \in C, x \neq y\}.
\]

By the definition of the Gray map and the Lee weight of \( R_k \), we can get that \( \Phi \) is one-to-one and a distance preserving linear map from \( R_k^n \) to \( \mathbb{F}_{p^n}^2 \).

### 3 Linear codes over \( R_k \)

Using the polynomial representation of codewords in \( R_k^n \), we easily have the following.

**Lemma 3.1.** A subset \( C \) of \( R_k^n \) is a \( \lambda \)-constacyclic code of length \( n \) over \( R_k \) if and only if its polynomial representation is an ideal of the ring \( R_k[x]/(x^n - \lambda) \).

For any \( r = (r^{(0)}, r^{(1)}, \ldots, r^{(n-1)}) \in R_k^n \), where \( r^{(i)} = \sum_{j=i}^{n-1} r_{ij} e_j, i = 0, 1, \ldots, n-1 \). Then \( r \) can be uniquely express as \( r = \sum_{j=1}^{2k} r_j e_j, r_j = (r_{0j}, r_{1j}, \ldots, r_{n-1,j}) \in \mathbb{F}_{p^n}, j = 1, 2, \ldots, 2^k \).

For any \( r, s \in R_k^n \), where \( s = \sum_{j=1}^{2k} s_j e_j, s_j = (s_{0j}, s_{1j}, \ldots, s_{n-1,j}) \in \mathbb{F}_{p^n} \), we can get that

\[
r \cdot s = \sum_{j=1}^{2k} (r_j \cdot s_j) e_j,
\]

where \( r_j \cdot s_j = \sum_{i=0}^{n-1} (r_{ij} s_{ij}) \).

Let \( C \) be a linear code over \( R_k \). For \( j = 1, 2, \ldots, 2^k \), we denote \( C_j \) as follows:

\[
C_j = \{(r_j \in \mathbb{F}_{p^n}, \sum_{i=1}^{2k} r_i e_i \in C, r_i \in \mathbb{F}_{p^n}, j = 1, 2, \ldots, 2^k \}.
\]

Clearly, \( C_j \) is a linear code of length \( n \) over \( \mathbb{F}_{p^n} \).

By the definition above we have the following theorems easily.

**Theorem 3.2.** Let \( C \) be a linear code over \( R_k \), then \( C = \sum_{j=1}^{2^k} e_j C_j, |C| = \prod_{j=1}^{2^k} |C_j| \), where \( C_1, C_2, \ldots, C_{2^k} \) are linear codes of length \( n \) over \( \mathbb{F}_{p^n} \), and the direct sum decomposition is unique.

**Theorem 3.3.** Let \( C \) be a linear code over \( R_k \), then \( C^\perp = \sum_{j=1}^{2^k} e_j C_j^\perp \), where \( C_j^\perp \) is the dual code of \( C_j \), where \( j = 1, 2, \ldots, 2^k \).

**Proof.** Let \( \tilde{C} = \sum_{j=1}^{2^k} e_j C_j^\perp \). For any \( c \in C, \tilde{c} \in \tilde{C}, c \cdot \tilde{c} = \sum_{j=1}^{2^k} (c_j \tilde{c}_j) e_j \), where \( c = \sum_{j=1}^{2^k} e_j c_j, \tilde{c} = \sum_{j=1}^{2^k} e_j \tilde{c}_j, c_j \in C_j, \tilde{c}_j \in C_j^\perp \). Then \( c \cdot \tilde{c} = 0 \), and thus \( \tilde{C} \subseteq C^\perp \). The ring \( R_k \) is a principal ideal ring and thus a Frobenius ring, we have \(|C||C^\perp| = |R_k|^n\). Thus

\[
|\tilde{C}| = \prod_{j=1}^{2^k} |C_j^\perp| = \prod_{j=1}^{2^k} \frac{p^n}{|C_j|} = \frac{|R_k|^n}{|C|} = |C^\perp|.
\]

So \( C^\perp = \tilde{C} \).

**Theorem 3.4.** Let \( C \) be a linear code over \( R_k \), then \( C \) is a self-orthogonal code if and only if \( C_j \) is a self-orthogonal code over \( \mathbb{F}_{p^n} \), where \( C = \sum_{j=1}^{2^k} e_j C_j \). \( C \) is a self-dual code if and only if \( C_j \) is a self-dual code over \( \mathbb{F}_{p^n} \), where \( j = 1, 2, \ldots, 2^k \).

**Proof.** By Theorems 3.2 and 3.3, \( C \subseteq C^\perp \) if and only if \( C_j \subseteq C_j^\perp \), so if \( C \) is a self-orthogonal code then \( C_j \) is a self-orthogonal code over \( \mathbb{F}_{p^n} \), where \( j = 1, 2, \ldots, 2^k \). Similarly, \( C \) is a self-dual code then \( C_j \) is a self-dual code over \( \mathbb{F}_{p^n} \), where \( j = 1, 2, \ldots, 2^k \).
Let $C$ be a linear code of length $n$ over $R_k$, for any $c = c_1 e_1 + c_2 e_2 + \cdots + c_{2^k} e_{2^k} \in C$, $\Phi(c) = (c_1, c_2, \cdots, c_{2^k}) \in \mathbb{F}_{p^m}^{2^k n}$. Let $C_1, C_2, \cdots, C_{2^k}$ be linear codes of length $n$ over $\mathbb{F}_{p^m}$, we define

$$C_1 \times C_2 \times \cdots \times C_{2^k} = \{ (c_1, c_2, \cdots, c_{2^k}) | c_i \in C_i, i = 1, 2, \cdots, 2^k \}. $$

**Proposition 3.6.** Let $C = e_1 C_1 + e_2 C_2 + \cdots + e_{2^k} C_{2^k}$ be a linear code of length $n$ over $R_k$ with $|C| = p^{m l}$ and the minimum Lee distance $d_L(C) = d$. Then $\Phi(C) = C_1 \times C_2 \times \cdots \times C_{2^k}$ is a linear code with parameter $[2^k n, 1, d]$ and $\Phi(C)^\perp = \Phi(C^\perp)$. If $C$ is a self-dual code over $R_k$, then $\Phi(C)$ is a self-dual code over $\mathbb{F}_{p^m}$.

**Proof.** By the definition above, we can know that

$$C_1 \times C_2 \times \cdots \times C_{2^k} \subseteq \Phi(C)$$

and

$$|C_1 \times C_2 \times \cdots \times C_{2^k}| = |C_1||C_2|\cdots|C_{2^k}| = |C|.$$ 

This gives that

$$\Phi(C) = C_1 \times C_2 \times \cdots \times C_{2^k}.$$ 

Let $c = \sum_{j=1}^{2^k} e_j c_j \in C$, $d = \sum_{j=1}^{2^k} e_j d_j \in C^\perp$, where $c_j \in C_j$, $d_j \in C_j^\perp$, then $c \cdot d = \sum_{j=1}^{2^k} e_j c_j d_j = 0$, which implies $c_j d_j = 0$, so

$$\Phi(c) \cdot \Phi(d) = \sum_{j=1}^{2^k} c_j d_j = 0,$$

which implies

$$\Phi(C)^\perp \supseteq \Phi(C^\perp).$$ 

By Theorem 3.3, we have

$$\Phi(C^\perp) = C_1^\perp \times C_2^\perp \times \cdots \times C_{2^k}^\perp.$$ 

Since $\Phi$ is one-to-one, we have

$$|\Phi(C^\perp)| = \frac{p^{m^2 n}}{|C|} = \frac{p^{m^2 n}}{|\Phi(C)|} = |\Phi(C)^\perp|.$$ 

So

$$\Phi(C)^\perp = \Phi(C^\perp). \quad \square$$

Let $\tau$ be a cyclic shift operator on $\mathbb{F}_{p^m}^n$. Let $a = (a^{(1)} | a^{(2)} | \cdots | a^{(2^k)}) \in \mathbb{F}_{p^m}^{2^k n}$, where $a^{(j)} \in \mathbb{F}_{p^m}^n$ for $j = 1, 2, \cdots, 2^k$. Let $\tau_{2^k}$ be the quasi-shift given by

$$\tau_{2^k}(a^{(1)} | a^{(2)} | \cdots | a^{(2^k)}) = (\tau(a^{(1)}) | \tau(a^{(2)}) | \cdots | \tau(a^{(2^k)})).$$

**Proposition 3.6.** Let $\sigma$ be a cyclic shift on $R_k^n$, let $\phi$ be the Gray map from $R_k^n$ to $\mathbb{F}_{p^m}^{2^k n}$, and let $\tau_{2^k}$ be as above. Then $\Phi \sigma = \tau_{2^k} \Phi$.

**Proof.** Let $r = (r_0, r_1, \cdots, r_{n-1}) \in R_k^n$, where $r_i = \sum_{j=1}^{2^k} r_{ij} e_j, i = 0, 1, \cdots, n-1$. We have $\sigma(r) = (r_{n-1}, r_0, \cdots, r_{n-2})$. If we apply $\phi$, we have

$$\Phi(\sigma(r)) = \Phi(r_{n-1}, r_0, \cdots, r_{n-2}) = (r_{1, n-1}, r_1, 0, \cdots, r_{1, n-2}, r_{2, n-1}, r_2, 0, \cdots, r_{2, n-2}, \cdots, r_{2^k, n-1}, r_{2^k, 0}, \cdots, r_{2^k, n-2}).$$

On the other hand,

$$\tau_{2^k}(\Phi(r)) = \tau_{2^k}(\Phi(r_0, r_1, \cdots, r_{n-1})) = \tau_{2^k}(r_1, 0, r_1, 0, \cdots, r_1, n-1, r_2, 0, \cdots, r_2, n-2, \cdots, r_{2^k, 0}, \cdots, r_{2^k, n-1})$$

$$= (r_1, n-1, r_1, 0, \cdots, r_1, n-2, r_2, n-1, r_2, 0, \cdots, r_2, n-2, \cdots, r_{2^k, n-1}, r_{2^k, 0}, \cdots, r_{2^k, n-2}).$$

Therefore, we have

$$\Phi \sigma = \tau_{2^k} \Phi. \quad \square$$
Theorem 3.7. Let $C$ be a cyclic code of length $n$ over $R_k$. Then $\Phi(C)$ is a quasi-cyclic code of index $2^k$ over $\mathbb{F}_{p^n}$ with length $2^k n$.

Proof. Since $C$ is a cyclic code, then $\sigma(C) = C$. If we apply $\Phi$, we have $\Phi\sigma(C) = \Phi(C)$. By the Proposition 3.6, $\Phi(\sigma(C)) = \Phi(C) = \tau_{2^k}(\Phi(C))$, so $\Phi(C)$ is a quasi-cyclic code of index $2^k$ over $\mathbb{F}_{p^n}$ with length $2^k n$. \hfill $\square$

Let $C$ be a linear code of length $n$ over $R_k$, let $A_0, A_1, \ldots, A_{2^k n}$ denote the number of codewords in $C$ of the Lee weight, and the Lee weight distribution of $C$ is simply the tuple of numbers $\{A_0, A_1, \ldots, A_{2^k n}\}$.

Let $\text{Lee}_C(x, y) = \sum_{i=0}^{2^k n} A_i x^{n-i} y^i$ denote the Lee weight enumerator of $C$, we get that

$$\text{Lee}_C(x, y) = \sum_{c \in C} x^{2^n - w(x)} y^{w(y)} = \sum_{\Phi(x) \equiv \Phi(y)} x^{2^n - w(\Phi(x))} y^{w(\Phi(y))} = W_{\Phi\phi}(C, y) = W_{\Phi\phi}(C, y).$$

By the results of [22], we have

$$W_{C_1}(x, y) = \frac{1}{|C|} W_C(x + (|R_k| - 1) y, x - y).$$

By a proof similar to (cf. [23, Lemma 1]), we obtain the following lemma.

Lemma 3.8. Let $x$ and $y$ be two vectors in $R_k^n$, and let $d_H(\Phi(x), \Phi(y))$ denote the Hamming distance of $\Phi(x), \Phi(y)$, where $\Phi(x), \Phi(y)$ are codewords in $\mathbb{F}_{2^k n}^n$. Let $w_H(\Phi(x))$ denote the Hamming weight of $\Phi$, then

1. $w_L(x) = w_H(\Phi(x))$,
2. $d_L(x, y) = d_H(\Phi(x), \Phi(y))$.

Theorem 3.9. Let $C$ be a linear code of length $n$ over $R_k$, then $\text{Lee}_C(x, y) = \frac{1}{|\Phi(C)|} W_{\Phi\phi}(C, x + (p^{m^2} - 1)y, x - y)$.

Proof. By Theorem 3.5, we have that

$$\text{Lee}_C(x, y) = W_{\Phi\phi}(C, y) = W_{\Phi\phi}(C, y).$$

So

$$\text{Lee}_C(x, y) = \sum_{c \in C} x^{2^n - w(x)} y^{w(y)} = \sum_{\Phi(x) \equiv \Phi(y)} x^{2^n - w(\Phi(x))} y^{w(\Phi(y))} = W_{\Phi\phi}(C, y).$$

As $\Phi$ is one-to-one, we have that $|\Phi(C)| = |C|$, hence

$$\text{Lee}_C(x, y) = W_{\Phi\phi}(C, x + (p^{m^2} - 1)y, x - y). \quad \square$$

4 \lambda-Constacyclic codes over $R_k$

Theorem 4.1. Let $C = c_1 C_1 + c_2 C_2 + \cdots + c_{2^k} C_{2^k}$ be a linear code over $R_k$, then $C$ is a $\lambda_1, \lambda_2, \cdots, \lambda_{2^k}$-constacyclic code over $R_k$ if and only if $C_1, C_2, \cdots, C_{2^k}$ are $\lambda_i$-constacyclic codes over $\mathbb{F}_{p^n}$, where $\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2^k} e_{2^k}$ is a unit over $R_k$.

Proof. For any $c_i = (c_{i,0}, c_{i,1}, \ldots, c_{i,n-1}) \in C_i$, where $i = 1, 2, \ldots, 2^k$. Then

$$c = c_1 C_1 + c_2 C_2 + \cdots + c_{2^k} C_{2^k} = \left( \sum_{i=1}^{2^k} e_i c_{i,0}, \sum_{i=1}^{2^k} e_i c_{i,1}, \ldots, \sum_{i=1}^{2^k} e_i c_{i,n-1} \right) \in C.$$

If $\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2^k} e_{2^k}$ is a unit over $R_k$, it is easy to know that for any element $r = r_1 e_1 + r_2 e_2 + \cdots + r_{2^k} e_{2^k} \in R_k$, $r$ is a unit if and only if $r_i \neq 0$, where $i = 1, 2, \ldots, 2^k$. 

For \( i = 1, 2, \ldots, 2^k \), if \( C_i \) is a \( \lambda_i \)-constacyclic code over \( \mathbb{F}_{p^n} \), then
\[
\sigma_{\lambda_i}(C_i) = \sigma_{\lambda_i}(C_i, 0, \cdots, C_i, n-1) = (\lambda_i C_i, 0, \cdots, \lambda_i C_i, n-2) \in C_i.
\]
Then we have
\[
\sigma_{\lambda_1 \lambda_2 \cdots \lambda_2}(g_k) = (\lambda_1 \lambda_2 \cdots \lambda_2) \sum_{i=1}^{2^k} e_i C_i, 0, \cdots, (\lambda_1 \lambda_2 \cdots \lambda_2) \sum_{i=1}^{2^k} e_i C_i, n-2 = e_1 \sigma_{\lambda_1}(C_1) + e_2 \sigma_{\lambda_2}(C_2) + \cdots + e_{2^k} \sigma_{\lambda_2}(C_2) \in C.
\]
This proves that \( C \) is a \( (\lambda_1 \lambda_2 \cdots \lambda_2) \)-constacyclic code over \( R_k \).
Conversely, if \( C \) is a \( (\lambda_1 \lambda_2 \cdots \lambda_2) \)-constacyclic code over \( R_k \), then
\[
\sigma_{\lambda_1 \lambda_2 \cdots \lambda_2}(g_k) = e_1 \sigma_{\lambda_1}(C_1) + e_2 \sigma_{\lambda_2}(C_2) + \cdots + e_{2^k} \sigma_{\lambda_2}(C_2) \in C.
\]
Thus \( \sigma_{\lambda_i}(C_i) \in C_i \), where \( i = 1, 2, \ldots, 2^k \).
So \( C_i \) is a \( \lambda_i \)-constacyclic code over \( \mathbb{F}_{p^n} \), where \( i = 1, 2, \ldots, 2^k \).

**Theorem 4.2.** Let \( C = e_1 C_1 + e_2 C_2 + \cdots + e_{2^k} C_{2^k} \) be a \( (\lambda_1 \lambda_2 \cdots \lambda_2) \)-constacyclic code of length \( n \) over \( R_k \), then there exists a polynomial \( e_1 g_1(x) + e_2 g_2(x) + \cdots + e_{2^k} g_{2^k}(x) \) in \( R_k[x] \) that divides \( x^n - (\lambda_1 \lambda_2 \cdots \lambda_2) \) generates the code, where \( g_i \) is the generator polynomial of \( C_i \), where \( i = 1, 2, \ldots, 2^k \). It follows that \( C \) has the form
\[
C = (e_1 g_1(x), e_2 g_2(x), \ldots, e_{2^k} g_{2^k}(x)).
\]
Let \( C' = (e_1 g_1(x) + e_2 g_2(x) + \cdots + e_{2^k} g_{2^k}(x)) \). We have that \( C' \subseteq C \).
Note that
\[
e_i[(e_1 g_1(x) + e_2 g_2(x) + \cdots + e_{2^k} g_{2^k}(x))] = e_i g_i(x),
\]
where \( i = 1, 2, \ldots, 2^k \).
We get that \( C \subseteq C' \). So \( C = C' \), and \( C \) is generated by a single element \( g(x) = e_1 g_1(x) + e_2 g_2(x) + \cdots + e_{2^k} g_{2^k}(x) \).

We know that \( g_i \) divides \( x^n - \lambda_i \), since \( g_i \) is the generator polynomial of \( C_i \), where \( i = 1, 2, \ldots, 2^k \). Let \( f_i(x) \) be the polynomial such that \( g_i(x) f_i(x) = x^n - \lambda_i \), where \( i = 1, 2, \ldots, 2^k \).
Then we have
\[
(e_1 g_1(x) + e_2 g_2(x) + \cdots + e_{2^k} g_{2^k}(x))[e_1 f_1(x) + e_2 f_2(x) + \cdots + e_{2^k} f_{2^k}(x)] = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2^k} e_{2^k}.
\]
So we have \( e_1 g_1(x) + e_2 g_2(x) + \cdots + e_{2^k} g_{2^k}(x) \) in \( R_k[x] \) that divides \( x^n - (\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2^k} e_{2^k}) \).

By Theorem 4.2 we have the following theorem easily:

**Theorem 4.3.** Let \( C = e_1 C_1 + e_2 C_2 + \cdots + e_{2^k} C_{2^k} \) be a \( (\lambda_1 \lambda_2 \cdots \lambda_2) \)-constacyclic code of length \( n \) over \( R_k \). Then \( C = (e_1 f_1^*(x) + e_2 f_2^*(x) + \cdots + e_{2^k} f_{2^k}^*(x)), \mid C^* \mid = p^{m(\sum_i \deg(g_i))} \), where \( f_i^*(x) \) is the reciprocal polynomial of \( f_i(x) \), i.e., \( f_i(x) = (x^d - \lambda_i) g_i(x), f_i^*(x) = x^{\deg(f_i)} (f(x)^{-1}) \), for \( i = 1, 2, \ldots, 2^k \).

**Example 4.4.** Let \( n = 10 \) and \( R_2 = \mathbb{F}_3 = u_1^3 + u_2^3 + u_3^3 + u_1 u_2 u_3^3, \lambda = -1, x^{10} + 1 = (x^2 + 1)(x^4 + x^3 + 2x + 1)(x^4 + 2x^3 + 1) \) \in \( \mathbb{F}_3(x) \). Let \( f_1(x) = f_2(x) = (x^4 + x^3 + 2x + 1), f_3(x) = f_4(x) = (x^4 + 2x^3 + 1) \), \( C = ((1 + u_1 + u_2)(1 + u_1 + u_2)) f_1(x), (u_1 + u_2 + u_1) f_2(x), (u_2 + u_1) f_3(x), (u_1 u_2) f_4(x) \). \( C_1, C_2, C_3, C_4 \) are \{10, 6, 4\} linear codes of length 10 with the minimum Lee weight \( d_L = 4 \). So \( \Phi(C) \) is a \{40, 24, 4\} linear code.

**Example 4.5.** Let \( n = 15 \) and \( R_3 = \mathbb{F}_2[u_1, u_2, u_3]/(u_1^3 = u_1, u_1 u_3 = u_3, u_2^3 - 1 = (x + 1)(x^4 + x^3 + 2x + 1)(x^4 + x^3 + 2x + 1) \) \in \( \mathbb{F}_2(x) \). Let \( f_1(x) = f_2(x) = f_3(x) = f_4(x) = f_5(x) = f_6(x) = f_7(x) = f_8(x) = (x^4 + x^3 + 1), C = ((1 + u_1)(1 + u_2) f_1(x), (u_1 + u_2)(1 + u_3)(1 + u_3) f_2(x), (u_2 + u_1) f_3(x), (u_1 u_2) f_4(x), (u_1 u_2 u_3) f_5(x)) \). \( C_1, C_2, C_3, C_4, C_5 \) are \{15, 11, 3\} linear code of length 15 with the minimum Lee weight \( d_L = 3, i = 1, 2, \ldots, 8 \). So \( \Phi(C) \) is a \{120, 88, 3\} linear code.
5 Conclusion

In this paper, we studied the constacyclic codes over $R_k = \mathbb{F}_p[u_1, u_2, \cdots, u_k]/(u_i^2 = u_i, u_iu_j = u_ju_i)$. We proved that the $(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_{2k} e_{2k})$-constacyclic codes of arbitrary length over $R_k$ can be generated by one polynomial.

Acknowledgement: This work was supported by the Basic and Advanced Technology Research Project of Henan Province (No.162300410083) and the Science and Technology Developing Project of Henan Province (No.172102210243).

References

[7] Cao Y., Repeated-root constacyclic codes of length $2p^k$ over $\mathbb{F}_p[u]/(u^m)$, Finite Fields Appl., 2016, 37, 108-130
[8] Cengellenmis Y., Dougherty S. T., Codes over an infinite family of rings with a Gray map, Des. Codes Cryptogr., 2010, 59, 213-224
[9] Liu X., Xu X., Cyclic and negacyclic codes of length $p^k$ over $\mathbb{F}_p[u]/(u^m)$, Finite Fields Appl., 2015, 34, 123-138
[15] Zheng X., Kong B., Cyclic codes and $\lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv$-constacyclic codes over $\mathbb{F}_p[u]/(u^2 + uv + vF_p), Appl. Math. Comput., 2017, 306, 86–91
[18] Dougherty S. T., Yildiz B., Karadeniz S., Codes over $R_k$, Gray maps and their binary images, Finite Fields Appl., 2011, 17, 205-219