Skew constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$

Mohammed Mahmoud AL-Ashker and Akram Qasem Mahmoud Abu-Jazar

Communicated by C. Flaut

MSC 2010 Classifications: 94B05, 94B15.

Keywords and phrases: Skew polynomial rings, Skew constacyclic codes, Skew cyclic codes

Abstract. In this paper, we study a special class of linear codes called skew constacyclic codes over finite non-chain rings of the form $\mathbb{F}_p + v\mathbb{F}_p$, where $p$ is an odd prime and $v^2 = v$. We use ideal $v$-constacyclic codes to define skew constacyclic codes, investigate the structural properties of skew polynomial ring $\mathcal{R}[x, \theta_v]/(x^n - \lambda)$ and determine them.

1 Introduction

Skew polynomial ring was introduced by Ore [14]. The set of skew cyclic codes is a generalization of cyclic codes but constructed using a non-commutative ring $\mathbb{F}_q[x; v]$, where $\mathbb{F}_q$ is a finite field and $\theta_v$ is a field automorphism of $\mathbb{F}_q$.

Recently, these family of codes are first described by D. Boucher, W. Geiselmann and F. Ulmer in [1], and [2]. In [8], G. Zhang, B. Chen studied the structure and properties of constacyclic codes over finite non-chain rings of the form $\mathbb{F}_p + v\mathbb{F}_p$, where $p$ is a prime number with $v^2 = v$. In [13], Jian Gao studied skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and determined their properties.

In this paper, we study skew constacyclic codes over finite non-chain rings of the form $\mathbb{F}_p + v\mathbb{F}_p$, where $p$ is a prime number with $v^2 = v$. We first define an automorphism over $\mathcal{R} = \mathbb{F}_p + v\mathbb{F}_p$. Also, we determine the units in $\mathcal{R}$ and show that skew constacyclic codes over $\mathcal{R}$ of arbitrary length are principally generated. Similar to [13], our results show that skew constacyclic code is equivalent to a constacyclic code over $\mathcal{R}$. Finally we study Euclidean dual codes of skew constacyclic codes over $\mathcal{R}$ and we then give some examples to illustrated our main results.

2 Preliminaries

Let $\mathcal{R} = \mathbb{F}_p + v\mathbb{F}_p = \{a + vb \mid a, b \in \mathbb{F}_p\}$, where $p$ is a prime number with $v^2 = v$ and $\mathbb{F}_p$ is a field with $p$ elements. The ring $\mathcal{R}$ has two maximal ideals which are $I_1 = \langle v \rangle = \{va \mid a \in \mathbb{F}_p\}$ and $I_2 = \langle 1 - v \rangle = \{(1 - v)b \mid b \in \mathbb{F}_p\}$, observe that $\mathcal{R}/ \langle v \rangle$ and $\mathcal{R}/ \langle 1 - v \rangle$ are isomorphic to $\mathbb{F}_p$. One can check that $\langle v \rangle$ and $\langle 1 - v \rangle$ are maximal ideals in $\mathcal{R}$, hence $\mathcal{R}$ is not a chain ring. The next definition, gives the structure of the automorphism group $Aut(\mathcal{R})$ of $\mathbb{F}_p + v\mathbb{F}_p$. By Chinese Remainder Theorem $\mathcal{R} = \langle 1 - v \rangle \oplus \langle v \rangle$ and for any element $a + vb$ in $\mathcal{R}$, $\exists c, d \in \mathbb{F}_q$ such that

$$a + bv = cv + d(1 - v)$$

for all $a, b \in \mathbb{F}_p$. Define a ring automorphism as follows

$$\theta_v : \mathbb{F}_p + v\mathbb{F}_p \longrightarrow \mathbb{F}_p + v\mathbb{F}_p$$

where

$$\theta_v(vc + (1 - v)d) = (1 - v)c + vd.$$ 

since

$$1 = v + (1 - v)$$

then

$$\theta_v(v + (1 - v)) = 1(1 - v) + v \text{ so } \theta_v(1) = 1.$$
Also

\[ \theta_v((vc_1 + (1 - v)d_1)(vc_2 + (1 - v)d_2)) = \theta_v(v^2c_1c_2 + (1 - v)^2d_2d_1) = (1 - v)^2c_1c_2 + v^2d_1d_2 = ((1 - v)c_1 + vd_1)((1 - v)c_2 + vd_2) = \theta_v((vc_1 + (1 - v)d_1))\theta_v((vc_2 + (1 - v)d_2)), \]

and

\[ \theta_v((vc_1 + (1 - v)d_1) + (vc_2 + (1 - v)d_2)) = \theta_v(v(c_1 + c_2) + (1 - v)(d_1 + d_2)) = (1 - v)(c_1 + c_2) + v(d_1 + d_2) = ((1 - v)c_1 + vd_1) + ((1 - v)c_2 + vd_2) = \theta_v(vc_1 + (1 - v)d_1) + \theta_v(vc_2 + (1 - v)d_2), \]

then \( \theta_v \) is ring homomorphism.

\[ \theta_v(vc_1 + (1 - v)d_1) = \theta_v(vc_2 + (1 - v)d_2) \implies ((1 - v)c_1 + vd_1) = ((1 - v)c_2 + vd_2) \implies c_1 - vc_1 + vd_1 = c_2 - vc_2 + vd_2 \implies c_1 = c_2 \text{ and } d_1 = d_2 \]

then \( \theta_v \) is one-to-one. To see \( \theta_v \) is onto let

\[ \theta_v(vc_1 + (1 - v)d_1) = vc_2 + (1 - v)d_2 \implies (1 - v)c_1 + vd_1 = vc_2 + (1 - v)d_2 \implies (1 - v)(c_1 - d_2) + v(d_1 - c_2) = 0 \implies c_1 - d_2 = 0 \implies c_1 = d_2 \]

\[ d_1 - c_2 = 0 \implies d_1 = c_2 \]

Hence

\[ (vc_1 + (1 - v)d_1) = \theta_v(vc_2 + (1 - v)d_2) \]

then \( \theta_v \) is onto, hence \( \theta_v \) is ring automorphism and \( \theta_v^2(e) = e \), for all \( e \) in \( R \), this implies that \( \theta_v \) is ring automorphism with order 2.

For a given automorphism \( \theta_v \) of \( R \), the set \( R[x; \theta_v] = \{0 \} \to a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} \} \) where \( a_i \in R, n \in N \setminus \{0\} \) of formal polynomials forms a ring under usual addition of polynomial and where multiplication is defined using the rule \((ax^i)(bx^j) = a\theta_v(b)x^{i+j}\) [11]. The ring \( R[x; \theta_v] \) is called skew polynomial ring over \( R \). It is non-commutative unless \( \theta_v \) is the identity automorphism on \( R[x] \).

**Lemma 2.1.** [8] Let \( \lambda = \zeta + v\mu \) be an element in \( R \), where \( \zeta \) and \( \mu \) are elements in \( F_p \). Then \( \lambda = \zeta + v\mu \) is a unit of \( R \) if and only if \( \zeta \neq 0 \) and \( \zeta + \mu \neq 0 \).

**Proof.** \( \implies \) Suppose that \( \lambda = \zeta + v\mu \) is a unit of \( R \). Then there exists elements \( a, b \in F_p \) and \( \lambda' = a + vb \in R \) such that \( \lambda'\lambda = 1 \), that is, \((\zeta + v\mu)(a + vb) = \zeta a + v(\zeta b + \mu a + \mu b) = 1 \). So we have that \( \zeta a = 1 \) and \((\zeta + \mu)b + \mu a = 0 \), which implies that \( \zeta \neq 0 \) and \( \zeta + \mu \neq 0 \).

\( \Leftarrow \) Let \( \lambda = \zeta + v\mu \in R \), where \( \zeta \neq 0 \) and \( \zeta + \mu \neq 0 \). Setting \( \lambda' = \zeta^{-1} + v[-1(\zeta + \mu)^{-1}\mu\zeta^{-1}] \).
Then
\[
\lambda \lambda = (\zeta + v \mu)(\zeta^{-1} + v(-1(\zeta + \mu)^{-1})\mu \zeta^{-1}) \\
= 1 + v[\mu \zeta^{-1} - \mu(\zeta + \mu)^{-1} - \mu(\zeta + \mu)^{-1} \cdot \mu \zeta^{-1}] \\
= 1 + v[\mu \zeta^{-1} - \mu(\zeta + \mu)^{-1}(1 + \mu \zeta^{-1})] \\
= 1 + v[\mu \zeta^{-1} - \mu(\zeta + \mu)^{-1}(\zeta \zeta^{-1} + \mu \zeta^{-1})] \\
= 1 + v[\mu \zeta^{-1} - \mu(\zeta + \mu)^{-1}(\zeta + \mu)\zeta^{-1}] \\
= 1.
\]

3 Skew Constacyclic Codes over $\mathbb{F}_p + v\mathbb{F}_p$

In this section we begin definition of $\lambda -$constacyclic codes and $(\theta_v - \lambda) -$constacyclic codes of skew constacyclic codes, then we will write all results of $\lambda -$constacyclic codes and $(\theta_v - \lambda) -$constacyclic codes.

Definition 3.1. [8] Let $\lambda$ be a unit in $R$. A linear code $C$ of length $n$ over $R$ is called $\lambda$-constacyclic if for every $(c_0, c_1, ..., c_{n-1}) \in C$, we have $(\lambda c_{n-1}, c_0, ..., c_{n-2}) \in C$

It is well known that a $\lambda$-constacyclic code of length $n$ over $R$ can be identified with an ideal in the quotient ring $R[x]/ < x^n - \lambda >$ via the $R$-module isomorphism as follows:

\[
R^n \rightarrow R[x]/ < x^n - \lambda > \\
n (c_0, c_1, ..., c_{n-1}) \rightarrow c_0, c_1 x, ..., c_{n-1} x^{n-1} \quad (mod < x^n - \lambda >).
\]

If $\lambda = 1$, $\lambda$-constacyclic codes are just cyclic codes and while $\lambda = -1$, $\lambda$-constacyclic codes are known as negacyclic codes.

Definition 3.2. Given an automorphism $\theta_v$ of $R = \mathbb{F}_p + v\mathbb{F}_p$, and a unit $\lambda = \zeta + v \mu$ in $R$, a code $C$ is said to be skew constacyclic, or specifically, $(\theta_v - \lambda) -$constacyclic if $C$ is closed under the $(\theta_v - \lambda) -$constacyclic shift vector $\rho_{\theta_v, \lambda} : R^n \rightarrow R^n$ defined by

\[
\rho_{\theta_v, \lambda}(c_0, c_1, ..., c_{n-1}) = (\theta_v((\zeta + v \mu)c_{n-1}),\theta_v(c_0),...,\theta_v(c_{n-2})).
\]

Analogous to the classical constacyclic codes, we characterize $\theta_v -(\zeta + v \mu) -$constacyclic codes in terms of left ideals in $R[x, \theta_v]/ < x^n - (\zeta + v \mu) >$.

Theorem 3.1. A code $C$ of length $n$ over $R$ is $\theta_v -(\zeta + v \mu) -$constacyclic if and only if the skew polynomial representation of $C$ is a left ideal in $R[x, \theta_v]/ < x^n - (\zeta + v \mu) >$.

Proof. Since $C$ is linear code, $C$ is an additive group. Let $a(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \in C$. Then $xa(x) = \theta_v((\zeta + v \mu)a_{n-1}) + \theta_v(a_0)x + ... + \theta_v(a_{n-2})x^{n-1} \in C$. And by iteration and linearity one can get $h(x)a(x) \in C$, for all $h(x) \in R_n$. This shows that $C$ is a left ideal in $R_n$.

3.1 Skew constacyclic codes generated by monic right divisors of $x^n - (\zeta + v \mu)$

The $\theta_v -(\zeta + v \mu) -$constacyclic codes which are principal left ideals in $R[x, \theta_v]/ < x^n - \lambda >$ generated by monic right divisors of $x^n - \lambda$, where $\lambda = \zeta + v \mu$. Let $C$ be a linear code of length $n$ over $R = \mathbb{F}_p + v\mathbb{F}_p$, define

\[
C_v = \{ a \in \mathbb{F}_p^n \mid (1 - v)a + vb \in C, \text{ for some } b \in \mathbb{F}_p^n \},
\]

and

\[
C_{1-v} = \{ b \in \mathbb{F}_p^n \mid (1 - v)a + vb \in C, \text{ for some } a \in \mathbb{F}_p^n \}.
\]

Obviously, $C_v$ and $C_{1-v}$ are linear codes over $\mathbb{F}_p$. By the definition of $C_v$ and $C_{1-v}$, we have that $C$ can be uniquely expressed as $C = (1-v)C_{1-v} \oplus vC_v$ [19].

In the following we give some properties about skew constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. 
Definition 3.3. The center $Z[R(x, \theta_v)]$ of $R(x, \theta_v)$ is the set of all elements that commute with all other elements of $R(x, \theta_v)$. We call an element $z \in Z[R(x, \theta_v)]$ central if $z$ commutes with all elements of $R(x, \theta_v)$.

Case 1: $n$ is even

Proposition 3.1. Let $\lambda = \zeta + v\mu$ be a unit in $R$. Then $x^n - \lambda$ is central in $Z[R(x, \theta_v)]$ if and only if $n$ is even.

Proof. Suppose $n$ is even, i.e., $2 | n$. Let $f(x) \in R[x, \theta_v]$ and $f(x) = a_0 + a_1 x + \ldots + a_m x^m$. Since $n$ is even, $f^n_0(a) = a$ for any element $a \in R$. Hence, $(x^n - \lambda)f(x) = (x^n - \lambda)a_0 + a_1 x + \ldots + a_m x^m = x^n a_0 + x^n a_1 x + \ldots + x^n a_m x^m - \lambda f(x) = \theta^n_v(a_0) + \theta^n_v(a_1) x + \ldots + \theta^n_v(a_m) x^n a_0 - \lambda f(x) = f(x) x^n - \lambda f(x) = f(x)(x^n - \lambda)$. Hence $(x^n - \lambda) \in Z[R(x, \theta_v)]$. Conversely, let $x^n - \lambda$ be in $Z[R(x, \theta_v)]$. Then $x^n - \lambda$ commutes with every element in $R[x, \theta_v]$. Particularly, $(x^n - \lambda)a_m x^m = a_m x^m (x^n - \lambda)$ for some $a_m \in R$. Since $(x^n - \lambda) a_m x^m = \theta^n_v(a_m) x^{n-m} - \lambda a_m x^m$ and $a_m x^m (x^n - \lambda) = a_m x^{n+m} - \lambda a_m x^m$, $\theta^n_v(a_m) = a_m$. Thus $n$ is even. □

Theorem 3.2. Let $n$ be even and $C$ be a $\theta_v - \lambda$–constacyclic code with length $n$, and $f(x)$ be a monic polynomial in $C$ with minimal degree, then $C = < f(x) >$, where $f(x)$ is a right divisor of $x^n - \lambda$.

Proof. Let $f(x)$ be a polynomial of minimal degree in $C$. There are two unique polynomials $q$ and $r$ such that $x^n - \lambda = qf + r$

where $\text{deg}(r) < \text{deg}(f)$. Since $r = (x^n - 1) - qf$ and $C$ is linear, $r \in C$. But $f(x)$ is with the minimal degree. Thus $r = 0$ and hence $f(x)$ is the right divisor of $x^n - \lambda$. □

Case 2: $n$ is odd

Let $n$ be odd. Then $| \theta | < \theta > | n$. This implies that $x^n - \lambda$ is non-commutative. Therefore the set $R_n = R[x, \theta_v]/(x^n - \lambda)$ is not a ring anymore. Define the addition on $R_n$ as usual and multiplication from left as $r(x)(g(x) + (x^n - \lambda)) = r(x)g(x) + (x^n - \lambda)$ for any $r(x) \in R[x, \theta_v]$. We can prove that $R_n$ is a left $R[x, \theta_v]$-module where multiplication is defined as above.

Theorem 3.3. Let $n$ be odd. Then $C$ is a skew constacyclic code of length $n$ over $R$ if and only if $C$ is a left $R[x, \theta_v]$-submodule of $R_n$.

Proof. Suppose $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ be any codeword in $C$. Since $C$ is a skew constacyclic code, $x^i c(x) \in C$. Since $C$ is linear, it follows that $r(x)c(x) \in C$ for any $r(x) \in R[x, \theta_v]$. Therefore $C$ is an $R[x, \theta_v]$-submodule of $R_n$. □

Theorem 4.4. Let $n$ be odd and $C$ be a skew constacyclic code with length $n$, and $f(x)$ be a polynomial in $C$ with minimal degree, then $C = < f(x) >$, where $f(x)$ is a right divisor of $x^n - \lambda$.

Proof. Similar to Theorem (3.2). □

Theorem 3.5. Let $n$ be odd and $C$ be a skew $\lambda$–constacyclic code of length $n$. Then $C$ is equivalent to a $\lambda$–constacyclic code of length $n$ over $R_n$.

Proof. Since $n$ is odd, it follows that $\gcd(2, n) = 1$. Therefore there exist integers $a, b$ such that $2a + bn = 1$. Thus $2a - 1 - bn = 1 + ln$, where $l > 0$. Let $c = c_0 + c_1 + \ldots + c_{n-1} x^{n-1}$ be a codeword in $C$. Note that $x^{2a} c(x) = \theta^{2a} c_0 x^{1 + 2ln} + \theta^{2a} c_1 x^{2 + 2ln} + \ldots + \theta^{2a} c_{n-1} x^{n-1 + 2ln} = \lambda^{1 + l c_0} c_{n-1} + c_0 x^l + \ldots + c_{n-2} x^{n-1-l} \in C$. Thus $C$ is a $\lambda$–constacyclic code of length $n$. □

Theorem 3.6. Let $C = (1 - v)C_{1-v} \oplus vC_v$ be a linear code of length $n$ over $R$. Then $C$ is a $\theta_v - \lambda$–constacyclic code of length $n$ over $R$ if and only if $C_v$ and $C_{1-v}$ are $\theta_v - (\zeta + \mu)$–constacyclic and $\theta_v - (\zeta - \mu)$–constacyclic codes of length $n$ over $\mathbb{F}_p$, respectively.
Proof. Let \((m_0, m_1, \ldots, m_{n-1})\) be an arbitrary element in \(C_{1-v}\), and let \((r_0, r_1, \ldots, r_{n-1})\) be an arbitrary element in \(C_v\). We assume that \(c_i = vm_i + (1-v)r_i, i = 0, 1, \ldots, n-1\); hence we get that \((c_0, c_1, \ldots, c_{n-1}) \in C\). Since \(C\) is a \(\theta_v-\lambda\)-constacyclic code of length \(n\) over \(R\), then 
\(\theta_v((\lambda c_{n-1}), (c_0), \ldots, (c_{n-2})) \in C\). Note that 
\[
\theta_v(\lambda c_{n-1}) = \theta_v((\zeta + v\mu)(vm_{n-1} + (1-v)r_{n-1}))
= \theta_v(v[(\zeta + \mu)m_{n-1} + (1-v)[r_{n-1}])
\]
then 
\[
(\theta_v(\lambda c_{n-1}), \theta_v(c_0), \ldots, \theta_v(c_{n-2})) = \theta_v(v[(\zeta + \mu)m_{n-1}, m_0, \ldots, m_{n-2}])
+ (1-v)([\zeta r_{n-1}, r_0, \ldots, r_{n-2}]) \in C,
\]
hence \(\theta_v((\zeta + \mu)m_{n-1}, m_0, \ldots, m_{n-2}) \in C_{1-v}\) and \(\theta_v((\zeta r_{n-1}, r_0, \ldots, r_{n-2}) \in C_v\), which implies that \(C_v\) and \(C_{1-v}\) are \(\theta_v-(\zeta + \mu)\)-constacyclic and \(\theta_v-\zeta\)-constacyclic codes of length \(n\) over \(F_p\), respectively.

Suppose that \(C_v\) and \(C_{1-v}\) are \(\theta_v-(\zeta + \mu)\)-constacyclic and \(\theta_v-\zeta\)-constacyclic codes of length \(n\) over \(F_p\), respectively. Let \((c_0, c_1, \ldots, c_{n-1}) \in C\), where \(c_i = vm_i + (1-v)r_i, i = 0, 1, \ldots, n-1\). It follows that \((m_0, m_1, \ldots, m_{n-1}) \in C_{1-v}\) and \((r_0, r_1, \ldots, r_{n-1}) \in C_v\). Note that 
\[
\theta_v((\lambda c_{n-1}), (c_0), \ldots, (c_{n-2})) = \theta_v(v[(\zeta + \mu)m_{n-1}, m_0, \ldots, m_{n-2}])
+ (1-v)([\zeta r_{n-1}, r_0, \ldots, r_{n-2}]) \in (1-v)C_{1-v} + vC_v = C,
\]
hence \(C\) is a \(\theta_v-\lambda\)-constacyclic code of length \(n\) over \(R\).

The next theorem is classical \(\lambda\)-constacyclic codes to determine the generators for codes.

Theorem 3.7. [8] Let \(C = vC_{1-v} \oplus (1-v)C_v\) be a \((\zeta + v\mu)\)-constacyclic code of length \(n\) over \(R\). Then \(C =< v g_{1-v}, (1-v)g_v >\), where \(g_{1-v}\) and \(g_v\) are the generator polynomials of \(C_{1-v}\) and \(C_v\), respectively.

Proposition 3.2. [8] Let \(C = vC_{1-v} \oplus (1-v)C_v\) be a \((\zeta + v\mu)\)-constacyclic code of length \(n\) over \(R\) and \(g_{1-v}(x), g_v(x)\) are the generator polynomials of \(C_{1-v}\) and \(C_v\) respectively. Then 
\[
|C| = p^2-\deg(g_{1-v}(x))-\deg(g_v(x)).
\]

Let \(C\) be a non-zero left ideal in \(F_p + vF_p\) over \(x^n - \lambda\) and let \(f_1(x)\) and \(f_2(x)\) denote the set of all non-zero skew polynomials of minimal degree in \(F_p\).

Theorem 3.8. Let \(C = vC_{1-v} \oplus (1-v)C_v\) be a \((\zeta + v\mu)\)-constacyclic code of length \(n\) over \(R\). If \(C =< v f_1(x), (1-v)f_2(x) >\), where \(f_1(x)\) and \(f_2(x)\) are monic skew polynomials with \(f_1(x) \mid (x^n - (\zeta + \mu))\) and \(f_2(x) \mid (x^n - \zeta)\), then \(C_{1-v} = [f_1(x)]\) and \(C_v = [f_2(x)]\), that is, \(f_1(x)\) and \(f_2(x)\) are the generator polynomials of constacyclic codes \(C_{1-v}\) and \(C_v\), respectively.

Example 3.1. Let \(R = F_3 + vF_3\) over \(x^{10} - 1 = (x-1)(x+1)(x^4 + x^3 - x + 1)(x^4 - x^3 + x + 1)\).

Then the constacyclic code of length 10 over \(R = F_3 + vF_3\) with generating polynomial 
\[
f_1(x) = (x^4 - x^3 + x + 1)\]
and \(f_2(x) = (x^4 + x^3 - x - 1)\), is 
\[
C = < v(x^4 - x^3 + x + 1), (1-v)(x^4 + x^3 - x + 1) > .
\]

If \(R = F_3 + vF_3\) over \(x, \theta_v\) and \(n = 10\). Then the skew constacyclic code of length 10 over \(R = F_3 + vF_3\) with generating polynomial 
\[
f_1(x) = (x^4-x^3+x+1)\]
and \(f_2(x) = (x^4+x^3+x-1)\), is 
\[
C = < (1-v)(x^4 - x^3 + x + 1), v(x^4 + x^3 - x + 1) > .
\]
4 Euclidean Dual Codes of Skew Constacyclic Codes over $\mathbb{F}_p + v\mathbb{F}_p$

We study Euclidean dual codes of $\theta_v - (\zeta + v\mu)$-constacyclic codes over $\mathcal{R}$. Their characterization is given in the next lemma.

Lemma 4.1. Let $C$ be a $\theta_v - (\zeta + v\mu)$-constacyclic code of length $n$ over $\mathcal{R}$. Then the dual code $C^\perp$ for $C$ is a $\theta_v - (\zeta + v\mu)^{-1}$-constacyclic code of length $n$ over $\mathcal{R}$.

Proof. For each unit $\lambda = \zeta + v\mu$ in $\mathcal{R} = \mathbb{F}_p + v\mathbb{F}_p$, then $\lambda^{-1}$ in $\mathcal{R}$. Let $u = (u_0, u_1, \ldots, u_{n-1}) \in C$ and $v = (v_0, v_1, \ldots, v_{n-1}) \in C^\perp$. Since $(\theta_v^{-1}(\lambda)u_1, \theta_v^{-1}(\lambda)u_2, \ldots, \theta_v^{-1}(\lambda)u_{n-1}), \theta_v^{-1}(u_0)) = \rho_{\theta_v, \lambda}^{-1}(u) \in C$, we have

$$0 = \langle \rho_{\theta_v, \lambda}^{-1}(u), v \rangle > = \lambda \langle (\theta_v^{-1}(\lambda)u_1, \theta_v^{-1}(\lambda)u_2, \ldots, \theta_v^{-1}(\lambda)u_{n-1}), (v_0, v_1, \ldots, v_{n-1}) \rangle > = \lambda (\theta_v^{-1}(\lambda)u_1, \theta_v^{-1}(\lambda)u_2, \ldots, \theta_v^{-1}(\lambda)u_{n-1}), (v_0, v_1, \ldots, v_{n-1}) > = \lambda (\theta_v^{-1}(\lambda)u_1) + \sum_{i=1}^{n-1} \theta_v^{-1}(u_i)v_{i-1}.
$$

As $n$ is a multiple of the order of $\theta_v$ and $\lambda^{-1}$ is fixed by $\theta_v$, it follows that

$$0 = \theta_v(0) = \theta_v(\lambda(\theta_v^{-1}(\lambda)u_1) + \sum_{i=1}^{n-1} \theta_v^{-1}(u_i)v_{i-1}) = \lambda(u_0\theta_v^0(\lambda)v_{n-1} + \sum_{i=1}^{n-1} u_i\theta_v^0v_{i-1}) = \lambda \rho_{\theta_v, \lambda^{-1}}(v), u >$$

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

Let $g_{1-v}(x)h_{1-v}(x) = x^n - \zeta, g_v(x)h_v(x) = x^n - (\zeta + v\mu)$. Let $h_{1-v}(x) = x^{\deg(h_{1-v}(x))}h_{1-v}(\frac{1}{x})$ and $h_v(x) = x^{\deg(h_v(x))}h_v(\frac{1}{x})$ be the reciprocal polynomials of $h_{1-v}$ and $h_v$, respectively. We write $h_{1-v}(x) = \frac{1}{h_{1-v}(0)}h_{1-v}(x)$ and $h_v(x) = \frac{1}{h_v(0)}h_v(x)$.

Theorem 4.1. Let $C = (1-v)C_{1-v} \oplus vC_v$ be a $\theta_v - (\zeta + v\mu)$-constacyclic code of length $n$ over $\mathcal{R}$. Then $C^\perp = (1-v)C_{1-v}^\perp \oplus vC_v^\perp$.

Proof. From Theorem (3.6) $C_{1-v}$ and $C_v$ in (3.1) and (3.2) are $\theta_v$-constacyclic codes over $\mathbb{F}_p$, then $C_{1-v}^\perp$ and $C_v^\perp$ are also $\theta_v$-constacyclic codes over $\mathbb{F}_p$. Let $g_{1-v}(x)$ and $g_v(x)$ are generator polynomials for $C_{1-v}$ and $C_v$, respectively. Then $C_{1-v}^\perp = [h_{1-v}^\perp(x)]$ and $C_v^\perp = [h_v^\perp(x)]$. Thus we have that $|C_{1-v}^\perp| = \deg(h_{1-v}^\perp(x))$ and $|C_v^\perp| = \deg(h_v^\perp(x))$. For any $a \in C_{1-v}^\perp$, $b \in C_v^\perp$ and $c = (1-v)r + vq \in C$, where $r, q \in C$, we have $\theta_v(c, ((1-v)r + vq)(1-v)a + vq)) = \theta_v((1-v)(r, a) + (v)(q, b)) = 0$, and hence $(1-v)C_{1-v}^\perp \oplus vC_v^\perp \subseteq C^\perp$.

Similarly we get $C^\perp \subseteq (1-v)C_{1-v}^\perp \oplus vC_v^\perp$. □

According to the above results and their proofs, we can carry out the results regarding skew constacyclic codes corresponding to their dual codes.

Theorem 4.2. Then the Euclidean dual code of a left ideal in $(\mathbb{F}_p + v\mathbb{F}_p)[x, \theta_v]/ < x^n - (\zeta + v\mu) >$ is also a left ideal in $(\mathbb{F}_p + v\mathbb{F}_p)[x, \theta_v]/ < x^n - (\zeta + v\mu) >$ determined as follows, if $C = (1-v)C_{1-v} \oplus vC_v$, then $C^\perp = (1-v)h_{1-v}^\perp(x), v=0$, and $C_v^\perp = \deg(h_v^\perp(x)) + \deg(g_v(x))$.

Proof. Since $C$ is a $\theta_v - (\zeta + v\mu)^{-1}$-constacyclic code over $\mathcal{R}$, and $C^\perp = (1-v)C_{1-v}^\perp \oplus vC_v^\perp$, where $C_{1-v}^\perp$ and $C_v^\perp$ are two $\theta_v$-constacyclic codes over $\mathbb{F}_p$. Since $h_{1-v}^\perp$ and $h_v^\perp$ are generator polynomials for $C_{1-v}^\perp$ and $C_v^\perp$, respectively, we have that $(1-v)h_{1-v}^\perp(x), v=0$ is the generating set in $C^\perp$ so $C^\perp = <(1-v)h_{1-v}^\perp(x), v=0 >$. In addition, $|C^\perp| = |C_{1-v}^\perp| \cdot |C_v^\perp| = \deg(g_{1-v}(x)) \cdot \deg(g_v(x)) + \deg(g_v(x))$. □
Example 4.1. From previous example 3.1 Let $R = \mathbb{F}_3 + v\mathbb{F}_3$, $n = 10$, and

$$(x^{10} - 1) = (x - 1)(x + 1)(x^4 + x^3 - x + 1)(x^4 - x^3 + x + 1).$$

Let

$$h_0 = x + 1, \ h_1 = x + 1, \ h_2 = x^4 + x^3 - x + 1, \ h_3 = x^4 - x^3 + x + 1.$$

Then we have

$$h_0 = x + 1 = h_0, \ h_1 = x - 1 = h_1, \ h_2 = x^4 - x^3 + x + 1 = h_3, \ h_3 = x^4 + x^3 - x + 1 = h_2.$$

Since

$$C = <(1 - v)(x^4 - x^3 + x + 1), v(x^4 + x^3 - x + 1) >,$$

Hence

$$C^\perp = <(1 - v)(x^4 - x^3 - x + 1), v(x^4 - x^3 + x + 1) >.$$

5 Conclusion

In this thesis we have defined skew polynomial rings, also studied skew constacyclic codes over finite non-chain rings of the form $\mathbb{F}_p + v\mathbb{F}_p$, where $p$ is a prime number with $v^2 = v$ and study Euclidean dual codes of skew constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$.

For future research one can extended this study to rings such as $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ or $\mathbb{F}_q + v\mathbb{F}_q + u^2\mathbb{F}_q$ where $q$ is a power of prime number $p$.

References


**Author information**

Mohammed Mahmoud AL-Ashker, Department of Mathematics, The Islamic University of Gaza, Palestine.
E-mail: mashker@iugaza.edu.ps

Akram Qasem Mahmoud Abu-Jazar, Department of Mathematics
The Islamic University of Gaza, Palestine.
E-mail: akrammath2010@hotmail.com

Received: March 18, 2015.

Accepted: August 7, 2015.