Palestine Journal of Mathematics

Vol. 5(2) (2016) , 96–103

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 θ_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 $\mathbb{F}_q[x, \theta_v]$, where $\mathbb{F}_q$ is a finite field and θ_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 $I_1 =< v >= \{va \mid a \in \mathbb{F}_p\}$ and $I_2 =< 1 - v >= \{(1 - v)b \mid b \in \mathbb{F}_p\}$, observe that $\mathcal{R}/ < v >$ and $\mathcal{R}/ < 1 - v >$ are isomorphic to $\mathbb{F}_p$. One can check that $< v >$ and $< 1 - v >$ 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 $\mathcal{R} =< 1 - v > \oplus < v >$ 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

$$\begin{aligned}
&\theta_v((vc_1 + (1-v)d_1)(vc_2 + (1-v)d_2))\\
&= \theta_v(v^2 c_1 c_2 + (1-v)^2 d_2 d_1)\\
&= (1-v)^2 c_1 c_2 + v^2 d_1 d_2\\
&= ((1-v)c_1 + vd_1)((1-v)c_2 + vd_2)\\
&= \theta_v((vc_1 + (1-v)d_1))\theta_v((vc_2 + (1-v)d_2)),
\end{aligned}$$

and

$$\begin{aligned}
&\theta_v((vc_1 + (1-v)d_1) + (vc_2 + (1-v)d_2))\\
&= \theta_v(v(c_1 + c_2) + (1-v)(d_1 + d_2))\\
&= (1-v)(c_1 + c_2) + v(d_1 + d_2)\\
&= ((1-v)c_1 + vd_1) + ((1-v)c_2 + vd_2)\\
&= \theta_v(vc_1 + (1-v)d_1) + \theta_v(vc_2 + (1-v)d_2),
\end{aligned}$$

then θ_v is ring homomorphism.

$$\begin{aligned}
&\theta_v(vc_1 + (1-v)d_1) = \theta_v(vc_2 + (1-v)d_2)\\
\Longrightarrow &((1-v)c_1 + vd_1) = ((1-v)c_2 + vd_2)\\
\Longrightarrow &c_1 - vc_1 + vd_1 = c_2 - vc_2 + vd_2\\
\Longrightarrow &c_1 = c_2 \text{ and } d_1 = d_2
\end{aligned}$$

then θ_v is one-to-one. To see θ_v is onto
let

$$\begin{aligned}
&\theta_v(vc_1 + (1-v)d_1) = vc_2 + (1-v)d_2\\
\Longrightarrow &(1-v)c_1 + vd_1 = vc_2 + (1-v)d_2\\
\Longrightarrow &(1-v)(c_1 - d_2) + v(d_1 - c_2) = 0\\
\Longrightarrow &c_1 - d_2 = 0 \Longrightarrow c_1 = d_2\\
\Longrightarrow &d_1 - c_2 = 0 \Longrightarrow d_1 = c_2\\
\text{Hence} \quad &(vc_1 + (1-v)d_1) = \theta_v(vc_2 + (1-v)d_2)
\end{aligned}$$

then θ_v is onto, hence θ_v is ring automorphism and $\theta_v^2(e) = e$, for all e in $\mathcal{R}$, this implies that θ_v is ring automorphism with order 2.
For a given automorphism θ_v of $\mathcal{R}$, the set $\mathcal{R}[x, \theta_v] = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} |$ where $a_i \in \mathcal{R}, n \in N \backslash \{0\}\}$ of formal polynomials forms a ring under usual addition of polynomial and where multiplication is defined using the rule $(ax^i)(bx^j) = a\theta_v^i(b)x^{i+j}$ [11]. The ring $\mathcal{R}[x, \theta_v]$ is called skew polynomial ring over $\mathcal{R}$. It is non-commutative unless θ_v is the identity automorphism on $\mathcal{R}[x]$.

Lemma 2.1. [8] Let $\lambda = \zeta + v\mu$ be an element in $\mathcal{R}$, where ζ and μ are elements in $\mathbb{F}_p$. Then $\lambda = \zeta + v\mu$ is a unit of $\mathcal{R}$ if and only if $\zeta \neq 0$ and $\zeta + \mu \neq 0$.

Proof. $\Longrightarrow$ Suppose that $\lambda = \zeta + v\mu$ is a unit of $\mathcal{R}$. Then there exists elements $a, b \in \mathbb{F}_p$ and $\lambda' = a + vb \in \mathcal{R}$ 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 $\zeta + \mu \neq 0$.
$\Longleftarrow$ Let $\lambda = \zeta + v\mu \in \mathcal{R}$, where $\zeta \neq 0$ and $\zeta + \mu \neq 0$. Setting $\lambda' = \zeta^{-1} + v[-1(\zeta + \mu)^{-1}\mu\zeta^{-1}]$.

Then

$$\begin{aligned}
\lambda^{'}\lambda &= (\zeta+v\mu)[\zeta^{-1}+v(-1(\zeta+\mu)^{-1}\mu\zeta^{-1})] \\
&= 1+v[\,\mu\zeta^{-1}-\mu(\zeta+\mu)^{-1}-\mu(\zeta+\mu)^{-1}.\,\mu\zeta^{-1}] \\
&= 1+v[\,\mu\zeta^{-1}-\mu(\zeta+\mu)^{-1}(1+\mu\zeta^{-1})] \\
&= 1+v[\,\mu\zeta^{-1}-\mu(\zeta+\mu)^{-1}(\zeta\zeta^{-1}+\mu\zeta^{-1})] \\
&= 1+v[\,\mu\zeta^{-1}-\mu(\zeta+\mu)^{-1}(\zeta+\mu)\zeta^{-1})] \\
&= 1
\end{aligned}$$

□

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

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

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

$$\mathcal{R}^n \longrightarrow \mathcal{R}[x]/ < x^n - \lambda >$$

$$(c_0, c_1, ..., c_{n-1}) \longrightarrow c_0, c_1x, ..., c_{n-1}x^{n-1} \quad (mod < x^n - \lambda >).$$

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

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

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

Proof. Since $\mathcal{C}$ is linear code, $\mathcal{C}$ is an additive group. Let $a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in \mathcal{C}$. Then $xa(x) = \theta_v((\zeta + v\mu)a_{n-1}) + \theta_v(a_0)x + ... + \theta_v(a_{n-2})x^{n-1} \in \mathcal{C}$. And by iteration and linearity one can get $h(x)a(x) \in \mathcal{C}$, for all $h(x) \in \mathcal{R}_n$. This shows that $\mathcal{C}$ is a left ideal in $\mathcal{R}_n$. □

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 $\mathcal{R}[x, \theta_v]/ < x^n - \lambda >$ generated by monic right divisors of $x^n - \lambda$, where $\lambda = \zeta + v\mu$. Let $\mathcal{C}$ be a linear code of length n over $\mathcal{R} = \mathbb{F}_p + v\mathbb{F}_p$, define

$$\mathcal{C}_v = \{a \in \mathbb{F}_p^n \mid (1 - v)a + vb \in \mathcal{C}, \text{for some } b \in \mathbb{F}_p^n\}, \tag{3.1}$$

and

$$\mathcal{C}_{1-v} = \{b \in \mathbb{F}_p^n \mid (1 - v)a + vb \in \mathcal{C}, \text{for some } a \in \mathbb{F}_p^n\}, \tag{3.2}$$

Obviously, $\mathcal{C}_v$ and $\mathcal{C}_{1-v}$ are linear codes over $\mathbb{F}_p$. By the definition of $\mathcal{C}_v$ and $\mathcal{C}_{1-v}$, we have that $\mathcal{C}$ can be uniquely expressed as $\mathcal{C} = (1 - v)\mathcal{C}_{1-v} \oplus v\mathcal{C}_v$ [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 $Z[\mathcal{R}(x,\theta_v)]$ of $\mathcal{R}(x,\theta_v)$ is the set of all elements that commute with all other elements of $\mathcal{R}(x,\theta_v)$. We call call an element $z \in Z[\mathcal{R}(x,\theta_v)]$ central if z commutes with all elements of $\mathcal{R}(x,\theta_v)$.

Case 1: n is even

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

Proof. Suppose n is even, i.e. , $2|n$. Let $f(x) \in \mathcal{R}[x,\theta_v]$ and $f(x) = a_0 + a_1x + ... + a_mx^m$. Since n is even, $\theta_v^n(a) = a$ for any element $a \in \mathcal{R}$. Hence, $(x^n - \lambda)f(x) = (x^n - \lambda)a_0 + a_1x + ... + a_mx^m = x^na_0 + x^na_1x + ... + x^na_mx^m - \lambda f(x) = \theta_v^n(a_0)x^n + \theta_v^n(a_1)x^nx + ... + \theta_v^n(a_m)x^nx^m - \lambda f(x) = (a_0 + a_1x + ... + a_mx^m)x^n - \lambda f(x) = f(x)x^n - \lambda f(x) = f(x)(x^n - \lambda)$. Hence $(x^n - \lambda) \in Z(\mathcal{R}[x,\theta_v])$. Conversely, let $x^n - \lambda$ be in $Z(\mathcal{R}[x,\theta_v])$. Then $x^n - \lambda$ commutes with every element in $\mathcal{R}[x,\theta_v]$. Particularly, $(x^n - \lambda)a_mx^m = a_mx^m(x^n - \lambda)$ for some $a_m \in \mathcal{R}$. Since $(x^n - \lambda)a_mx^m = \theta_v^n(a_m)x^{n+m} - \lambda a_mx^m$ and $a_mx^m(x^n - \lambda) = a_mx^{n+m} - \lambda a_mx^m$, $\theta^n(a_m) = a_m$. Thus n is even. □

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

Proof. Let $f(x)$ be a polynomial of minimal degree in $\mathcal{C}$. There are two unique polynomials q and r such that

$$x^n - \lambda = qf + r$$

where $deg(r) < deg(f)$. Since $r = (x^n - 1) - qf$ and $\mathcal{C}$ is linear, $r \in \mathcal{C}$. 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 $| < \theta > | \nmid n$. This implies that $x^n - \lambda$ is non-commutative. Therefore the set $\mathcal{R}_n = \mathcal{R}[x,\theta_v]/(x^n - \lambda)$ is not a ring anymore. Define the addition on $\mathcal{R}_n$ as usual and multiplication from left as $r(x)(g(x) + (x^n - \lambda)) = r(x)g(x) + (x^n - \lambda)$ for any $r(x) \in \mathcal{R}[x,\theta_v]$. We can prove that $\mathcal{R}_n$ is a left $\mathcal{R}[x,\theta_v]$-module where multiplication is defined as above.

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

Proof. Suppose $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ be any codeword in $\mathcal{C}$. Since $\mathcal{C}$ is a skew constacyclic code, $x^ic(x) \in \mathcal{C}$. Since $\mathcal{C}$ is linear, it follows that $r(x)c(x) \in \mathcal{C}$ for any $r(x) \in \mathcal{R}[x,\theta_v]$. Therefore $\mathcal{C}$ is an $\mathcal{R}[x,\theta_v]$-submodule of $\mathcal{R}_n$. □

Theorem 3.4. Let n be odd and $\mathcal{C}$ be a skew constacyclic code with length n, and $f(x)$ be a polynomial in $\mathcal{C}$ with minimal degree, then $\mathcal{C} =< f(x) >$, 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 $\mathcal{C}$ be a skew λ−constacyclic code of length n. Then $\mathcal{C}$ is equivalent to a λ−constacyclic code of length n over $\mathcal{R}_n$.

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 $c = c_0 + c_1 + ... + c_{n-1}x^{n-1}$ be a codeword in $\mathcal{C}$. Note that $x^{2a}c(x) = \theta^{2a}(\lambda c_0)x^{1+ln} + \theta^{2a}(c_1)x^{2+ln} + ... + \theta^{2a}(c_{n-1})x^{n+ln} = \lambda^{1+ln}c_{n-1} + c_0x + ... + c_{n-2}x^{n-1} \in \mathcal{C}$. Thus $\mathcal{C}$ is a λ−constacyclic code of length n. □

Theorem 3.6. Let $\mathcal{C} = (1-v)\mathcal{C}_{1-v} \oplus v\mathcal{C}_v$ be a linear code of length n over $\mathcal{R}$. Then $\mathcal{C}$ is a θ_v−λ−constacyclic code of length n over $\mathcal{R}$ if and only if $\mathcal{C}_v$ and $\mathcal{C}_{1-v}$ are θ_v−$(\zeta+\mu)$−constacyclic and θ_v−ζ−constacyclic codes of length n over $\mathbb{F}_p$, respectively.

Proof. $\Longrightarrow$ Let $(m_0, m_1, ..., m_{n-1})$ be an arbitrary element in $\mathcal{C}_{1-v}$, and let $(r_0, r_1, ..., r_{n-1})$ be an arbitrary element in $\mathcal{C}_v$. We assume that $c_i = vm_i + (1-v)r_i$, $i = 0, 1, ..., n-1$; hence we get that $(c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$. Since $\mathcal{C}$ is a $\theta_v{-}\lambda{-}$constacyclic code of length n over $\mathcal{R}$, then $\theta_v((\lambda c_{n-1}), (c_0), ..., (c_{n-2})) \in \mathcal{C}$. Note that

$$\begin{aligned}\theta_v(\lambda c_{n-1}) &= \theta_v((\zeta + v\mu)[vm_{n-1} + (1-v)r_{n-1}]) \\ &= \theta_v(v[(\zeta + \mu)m_{n-1}] + (1-v)[\zeta r_{n-1}])\end{aligned}$$

then

$$\begin{aligned}(\theta_v(\lambda c_{n-1}), \theta_v(c_0), ..., \theta_v(c_{n-2})) = \theta_v(v[(\zeta + \mu)m_{n-1}, m_0, ..., m_{n-2})] \\ + (1-v)[(\zeta r_{n-1}, r_0, ..., r_{n-2})]) \in \mathcal{C},\end{aligned}$$

hence $\theta_v((\zeta+\mu)m_{n-1}, m_0, ..., m_{n-2})) \in \mathcal{C}_{1-v}$ and $\theta_v((\zeta r_{n-1}, r_0, ..., r_{n-2})) \in \mathcal{C}_v$, which implies that $\mathcal{C}_v$ and $\mathcal{C}_{1-v}$ are $\theta_v{-}(\zeta+\mu){-}$constacyclic and $\theta_v{-}\zeta{-}$constacyclic codes of length n over $\mathbb{F}_p$, respectively.

$\Longleftarrow$ Suppose that $\mathcal{C}_v$ and $\mathcal{C}_{1-v}$ are $\theta_v{-}(\zeta+\mu){-}$constacyclic and $\theta_v{-}\zeta{-}$constacyclic codes of length n over $\mathbb{F}_p$, respectively. Let $(c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$, where $c_i = vm_i + (1-v)r_i$, $i = 0, 1, ..., n-1$. It follows that $(m_0, m_1, ..., m_{n-1}) \in \mathcal{C}_{1-v}$ and $(r_0, r_1, ..., r_{n-1}) \in \mathcal{C}_v$. Note that

$$\begin{aligned}\theta_v((\lambda c_{n-1}), (c_0), ..., (c_{n-2})) = \theta_v(v[(\zeta + \mu)m_{n-1}, m_0, ..., m_{n-2})] \\ + (1-v)(\zeta + \mu)r_{n-1}, r_0, ..., r_{n-2})]) \in (1-v)\mathcal{C}_{1-v} \oplus v\mathcal{C}_v = \mathcal{C},\end{aligned}$$

hence $\mathcal{C}$ is a $\theta_v{-}\lambda$-constacyclic code of length n over $\mathcal{R}$. □

The next theorem is classical $\lambda{-}$constacyclic codes to determine the generators for codes.

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

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

Let $\mathcal{C}$ be a non-zero left ideal in $\mathbb{F}_p + v\mathbb{F}_p[x]/ < x^n - \lambda >$ and let $f_1(x)$ and $f_2(x)$ denote the set of all non-zero skew polynomials of minimal degree in $\mathbb{F}_p$.

Theorem 3.8. Let $\mathcal{C} = v\mathcal{C}_{1-v} \oplus (1-v)\mathcal{C}_v$ be a $(\zeta + v\mu){-}$constacyclic code of length n over $\mathcal{R}$. If $\mathcal{C} =< vf_1(x), (1-v)f_2(x) >$, where $f_1(x)$ and $f_2(x) \in \mathbb{F}_p$ are monic skew polynomials with $f_1(x) \mid (x^n - (\zeta + \mu))$ and $f_2(x) \mid (x^n - \zeta)$, then $\mathcal{C}_{1-v} = [f_1(x)]$ and $\mathcal{C}_v = [f_2(x)]$, that is, $f_1(x)$ and $f_2(x)$ are the generator polynomials of constacyclic codes $\mathcal{C}_{1-v}$ and $\mathcal{C}_v$, respectively.

Example 3.1. Let $\mathcal{R} = \mathbb{F}_3 + v\mathbb{F}_3[x]$, $n = 10$, and

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

Then the constacyclic code of length 10 over $\mathcal{R} = \mathbb{F}_3 + v\mathbb{F}_3[x]$ with generating polynomial $f_1(x) = (x^4 - x^3 + x + 1)$ and $f_2(x) = (x^4 + x^3 + x - 1)$, is

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

If $\mathcal{R} = \mathbb{F}_3 + v\mathbb{F}_3[x, \theta_v]$ and $n = 10$. Then the skew constacyclic code of lenght 10 over $\mathcal{R} = \mathbb{F}_3 + v\mathbb{F}_3[x, \theta_v]$ with generating polynomial $f_1(x) = (x^4 - x^3 + x + 1)$ and $f_2(x) = (x^4 + x^3 + x - 1)$, is

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

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 $\mathcal{C}$ be a $\theta_v-(\zeta + v\mu)$-constacyclic code of length n over $\mathcal{R}$. Then the dual code $\mathcal{C}^{\perp}$ for $\mathcal{C}$ 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 λ^{-1} in $\mathcal{R}$. Let $u = (u_0, u_1, ..., u_{n-1}) \in \mathcal{C}$ and $v = (v_0, v_1, ..., v_{n-1}) \in \mathcal{C}^{\perp}$.
Since $(\theta_v^{n-1}(\lambda u_1), \theta_v^{n-1}(\lambda u_2), ..., \theta_v^{n-1}(\lambda u_{n-1}), \theta_v^{n-1}(u_0)) = \rho_{\theta_v,\lambda}^{n-1}(u) \in \mathcal{C}$, we have

$$\begin{aligned}
0 &=< \rho_{\theta_v,\lambda}^{n-1}(u), v > \\
&=< (\theta_v^{n-1}(\lambda u_1), \theta_v^{n-1}(\lambda u_2), ..., \theta_v^{n-1}(\lambda u_{n-1}), \theta_v^{n-1}(u_0)), (v_0, v_1, ..., v_{n-1}) > \\
&= \lambda < (\theta_v^{n-1}(u_1), \theta_v^{n-1}(u_2), ..., \theta_v^{n-1}(u_{n-1}), \theta_v^{n-1}(\lambda^{-1}u_0)), (v_0, v_1, ..., v_{n-1}) > \\
&= \lambda(\theta_v^{n-1}(\lambda^{-1}u_0)v_{n-1} + \sum_{i=1}^{n-1} \theta_v^{n-1}(u_i)v_{i-1}).
\end{aligned}$$

As n is a multiple of the order of θ_v and λ^{-1} is fixed by θ_v, it follows that

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

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

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

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

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

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 $\mathcal{C} = (1-v)\mathcal{C}_{1-v} \oplus v\mathcal{C}_v$, then $\mathcal{C}^{\perp} =< (1-v)h_{1-v}^*(x), vh_v^*(x) >$, *and* $\mid \mathcal{C}^{\perp} \mid = p^{deg(g_{1-v}(x))+deg(g_v(x))}$

Proof. Since $\mathcal{C}^{\perp}$ is a $\theta_v - (\zeta + v\mu)^{-1}-$constacyclic code over $\mathcal{R}$, and $\mathcal{C}^{\perp} = (1-v)\mathcal{C}_{1-v}^{\perp} \oplus v\mathcal{C}_v^{\perp}$, where $\mathcal{C}_{1-v}^{\perp}$ and $\mathcal{C}_v^{\perp}$ are two θ_v-constacyclic codes over $\mathbb{F}_p$. Since h_{1-v}^* and h_v^* are generator polynomials for $\mathcal{C}_{v-1}^{\perp}$ and $\mathcal{C}_v^{\perp}$, respectively, we have that $\{(v-1)h_{1-v}^*(x), vh_v^*(x)\}$ is the generating set in $\mathcal{C}^{\perp}$ so $\mathcal{C}^{\perp} =< (1-v)h_{1-v}^*(x), vh_v^*(x) >$. In addition, $\mid \mathcal{C}^{\perp} \mid = \mid \mathcal{C}_{1-v}^{\perp} \mid\mid \mathcal{C}_v^{\perp} \mid = p^{deg(g_{1-v}(x))}p^{deg(g_v(x))} = p^{deg(g_{1-v}(x))+deg(g_v(x))}$ □

Example 4.1. From previous example 3.1 Let $\mathcal{R} = \mathbb{F}_3 + v\mathbb{F}_3$, $n = 10$, 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

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

Hence

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

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 $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ where q is a power of prime number p.

References

[1] D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, Applicable Algebra in Engineering, Communication and Computing, 18 (2007), 379-389

[2] D. Boucher, P. Solt'e and F. Ulmer, Skew constacyclic codes over Galois rings, Advances in Mathematics of Communications, 2 (2008), 273-292.

[3] D. Boucher and F. Ulmer, Codes as modules over skew polynomial rings, Lecture Notes in Computer Science, 5921 (2009), 38-55.

[4] D. Boucher and F. Ulmer, Coding with skew polynomial rings, Journal of Symbolic Computation, 44 (2009), 1644-1656

[5] D. Boucher and F. Ulmer, Codes as modules over skew polynomial rings. In: Cryptography and coding. Springer, Berlin, (2009a), pp. 38-55.

[6] D. Boucher and F. Ulmer, A note on the dual codes of module skew codes. Vol. 7089 of Lecture Notes in Comput. Sci. (2011), pp. 230-243.

[7] D. Boucher and F. Ulmer, Self-dual skew codes and factorization of skew polynomails, Journal of Symbolic Computation, (2013), pp. 47-61

[8] G. Zhang, B. Chen, Constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, cornell university, Computer Science, arXiv:1301.0669, (2013).

[9] H. Q. Dinh, Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Transactions on Information Theory, 55 (2009), pp. 730-1740.

[10] H. Q. Dinh, Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra 324(2010), pp. 940-950.

[11] I.Siap, T.Abualrub, N.Aydin, and P.Seneviratne, Skew Cyclic Codes Of Arbitrary Length, International Journal of Information and Coding Theory (IJICOT), Vol. 2, No. 1, (2011)

[12] Jia, Y., Ling, S., Xing, C., On self-dual cyclic codes over finite fields. IEEE Trans. Inform. Theory 57 (4), (2011), pp. 2243-2251.

[13] J.GAO, Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, J.Appl. Math & information, Vol.31 (2013), No. 3 - 4, pp. 337 -342.

[14] O. Ore, Theory of non-commutative polynomials, Annals of Math. 34 (1933), pp. 480-508

[15] S. Jitman, S. Ling, P. Udomkavanich, Skew constacyclic codes over finite chain ring. Advance in Mathematic of comm. (2012), pp. 39-63.

[16] S. Zhu, L. Wang, A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image, Discrete Math.311(2011), 2677-2682.

[17] W. Cary Huffman, Vera Pless, Fundemantal Of Error Correcting Codes, printed in the United Kingdom Cambridge University Pres (2003).

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.