Bull. Korean Math. Soc. **55** (2018), No. 6, pp. 1627–1638
https://doi.org/10.4134/BKMS.b160535
pISSN: 1015-8634 / eISSN: 2234-3016

SKEW CYCLIC CODES OVER $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$

Hamed Mousavi, Ahmad Moussavi, and Saeed Rahimi

Abstract. In this paper, we study an special type of cyclic codes called skew cyclic codes over the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, where p is a prime number. This set of codes are the result of module (or ring) structure of the skew polynomial ring $(\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)[x;\theta]$ where $v^3 = 1$ and θ is an $\mathbb{F}_p$-automorphism such that $\theta(v) = v^2$. We show that when n is even, these codes are either principal or generated by two elements. The generator and parity check matrix are proposed. Some examples of linear codes with optimum Hamming distance are also provided.

1. Introduction

Cyclic codes are an important class of codes from both a theoretical and practical viewpoint. Traditionally, cyclic codes have been studied over finite fields. Polynomial rings and their ideals are essential to the construction and understanding of cyclic codes. These codes are applicable because they are easy to design and can detect or correct in an efficient index. They are used in a lot of applications like wireless sensor networks, steganography, burst errors, etc., (For example, see [13], [17]).

There are a lot of works about cyclic codes over rings in [2,3,7,14,15,18]. This is because of the fact that polynomials over rings have more divisors and the length of the code has less limitation over the ring. These codes can propose a lot of optimum linear codes. Also, the algebraic structure of these codes are very easy to study, because the cyclic codes over the ring R with length n correspond with the submodules of the module $\frac{R[x]}{\langle x^n-1\rangle}$, which is studied a lot of cases in the literature. These advantages lead the researchers to study different classes of cyclic code category like constacyclic as in [10], negacyclic codes as [2], quasi cyclic codes [8], etc.

One of the interesting types of generalizing of the notion of cyclic codes is skew cyclic codes which were proposed by Boucher in [4]. For the first time in [6] non commutative skew polynomial rings have been used to construct (a generalization of) cyclic codes. These non commutative rings are of the

Received June 25, 2016; Revised November 7, 2017; Accepted February 1, 2018.
2010 *Mathematics Subject Classification.* Primary 11T71, 16S36, 68P30.
Key words and phrases. skew cyclic coding, skew polynomial rings, Hamming distance, quasi cyclic coding.

category of Ore rings. Recall that a *skew cyclic code* over an arbitrary ring S with an endomorphism θ is a linear code C such that, when $(c_0, c_1, c_2, \ldots, c_n) \in C$ it implies that $(\theta(c_n), \theta(c_0), \ldots, \theta(c_{n-1})) \in C$.

For a given automorphism θ of R, the set $R[x;\theta]$ consisting of polynomials $f = a_0 + a_1x + \cdots + a_nx^n$, with $a_i \in R$ forms a ring under usual addition of polynomials and multiplication defined by the rule $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$ for each $a, b \in R$, and is called *the skew polynomial ring* over R.

Boucher also introduced different types of skew cyclic codes in [5,6]. Then in the papers [9], [11], [12], and [16], the skew cyclic codes over different rings are proposed. Skew cyclic codes with length n over the ring R are the submodules of $\frac{R[x;\theta]}{\langle x^n-1\rangle}$. The module $\frac{R[x;\theta]}{\langle x^n-1\rangle}$ is not necessarily a ring, unless $x^n-1 \in \text{Center}(R)$. The main reason of usefulness of these codes is that these codes usually are not unique factorization domains and have even more divisors than their similar cyclic structures. This results in more possibility to define new generator polynomials. This may cause new codes with larger minimum Hamming distance. As an example, in [1] or [5], the authors could introduce some codes over finite fields, which has better performance than the best known linear codes with the same parameters.

In this paper, we study the skew cyclic codes over the ring $R = \mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ where $v^3 = 1$. We propose the center of R to find the cases that this structure of skew cyclic codes is an ideal. Also, we will find the structure of the ideals of $(\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)[x;\theta]$ where θ is an $\mathbb{F}_p$-automorphism such that $\theta(v) = v^2$ (i.e., $\theta^2 = 1$). Then we try to show the cases a skew cyclic code is a quasi cyclic code. We also give some information about the case that the module $\frac{(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)[x;\theta]}{\langle x^n-1\rangle}$ is not a ring. We show that skew cyclic codes are submodules of the mentioned module. Finally, we propose some examples of optimum codes.

If $\mathbb{F}$ is a field, it is proved that codes are in fact the submodules of $\frac{\mathbb{F}[x;\theta]}{\langle x^n-1\rangle}$ (e.g., see [4]). We prove the same result for the skew cyclic codes over $\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$. Also for each ring R, $\frac{R[x;\theta]}{\langle x^n-1\rangle}$ is a ring if and only if $x^n - 1 \in \text{Center}(R[x;\theta])$. So we need to find the center of R, if we want to exploit the ring structure of skew cyclic codes.

The *Hamming distance* of $U = (u_0, \ldots, u_{n-1}), V = (v_0, \ldots, v_{n-1})$ over a ring T, is the cardinality of the set $\{i \mid v_i \neq u_i\}$. Also the *Lee distance* U, V is: $d_L(U, V) = \sum_{i=0}^{n-1} |u_i - v_i|$, where $|\cdot|$ means a metric over T.

2. The structure of ideals of the ring $\frac{(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)[x;\theta]}{\langle x^n-1\rangle}$

Let p be a prime number and $\mathbb{F}_p$ be a finite field. Then the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ where $v^3 = 1$, is in fact the ring $\frac{\mathbb{F}_p[v]}{\langle v^3-1\rangle}$. To produce a skew polynomial version of this ring, we need the following.

Theorem 2.1. *Let $\theta : \mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p \longrightarrow \mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$ with $\theta(a+bv+cv^2) = a + bv^2 + cv$. Then θ is a ring automorphism.*

Proof. First, we prove that θ is linear. To do this, let $a+bv+cv^2, f+gv+hv^2 \in \mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$. Then

$$\begin{aligned}\theta(a + bv + cv^2) + \theta(f + gv + hv^2) &= a + bv^2 + cv + f + gv^2 + hv \\ &= (a + f) + (c + h)v + (b + g)v^2 \\ &= \theta((a + f) + (b + g)v + (c + h)v^2). \qquad (1)\end{aligned}$$

So θ is additive.

One can see that the following equations hold for each $a, b, c, d, f, g, h \in \mathbb{F}_p$:

$$\begin{aligned}&\theta(a + bv + cv^2)\theta(f + gv + hv^2) \\ &= (a + bv^2 + cv)(f + gv^2 + hv) \\ &= (ch + ag + bf)v^2 + (ah + bg + cf)v + af + bh + cg \\ &= \theta((ch + ag + bf)v + (ah + bg + cf)v^2 + af + bh + cg) \\ &= \theta((a + bv + cv^2)(f + gv + hv^2)).\end{aligned}$$

Also, for each $a + bv + cv^2$, we have $\theta(a + cv + bv^2) = a + bv + cv^2$. Moreover, $\theta(a + bv + cv^2) = a + cv + bv^2 = 0$ if and only if $a = b = c = 0$. □

Throughout this paper, R will denote the ring $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ and S the ring $(\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)[x;\theta]$, and S_n will denote $\frac{(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)[x;\theta]}{\langle x^n-1\rangle}$.

Also, let $g \in S$. Then $\mathrm{supp}(g) = \{g_i \,|\, g_i \neq 0, i \in \mathbb{N} \cup \{0\}\}$. Let $U(R)$ be the set of unit elements of R. Now we determine the center of S.

Theorem 2.2. *The center of S is $\mathbb{F}_p[x^2] + A$ where $A = \{g \in S \,|\, g_i = (1 + v + v^2)a_i, a_i \in \mathbb{F}_p[x^2]\}$.*

Proof. Let $g \in \mathbb{F}_p[x^2]$. So $g(x) = \sum_i g_{2i}x^{2i}$ where $g_{2i} \in \mathbb{F}_p$. Assume that $h(x) = \sum_i h_i x^i \in S$ (i.e., $h_i \in R$). So

$$(hg)(x) = \sum_{i,j} h_i\theta^i(g_{2j})x^{i+2j} = \sum_{i,j} h_i g_{2j} x^{i+2j}.$$

The last equality is rooted from the fact that θ fixes $\mathbb{F}_p$. Also,

$$(gh)(x) = \sum_{i,j} g_{2j}\theta^{2j}(h_i)x^{2j+i} = \sum_{i,j} g_{2j}h_i x^{2j+i}.$$

So $\mathbb{F}_p[x^2] \subseteq \mathrm{Center}(S)$. Now, let $g \in A$ and $h \in S$. So $g(x) = \sum_i a_i(1 + v + v^2)x^{2i}$ and $h(x) = \sum_i h_i x^i$. Thus

$$\begin{aligned}h(x)g(x) &= \sum_{i,j} h_i\theta^i(a_j(1 + v + v^2))x^{i+2j} \\ &= \sum_{i,j}(h_{i,1} + vh_{i,2} + v^2h_{i,3})a_j(1 + v + v^2)x^{i+2j}.\end{aligned}$$

Since $v(1+v+v^2)=1+v+v^2$,

$$h(x)g(x)=\sum_{i,j}(h_{i,1}+h_{i,2}+h_{i,3})a_j(1+v+v^2)x^{i+2j}.$$

Also

$$\begin{aligned}g(x)h(x)&=\sum_{i,j}a_j(1+v+v^2)\theta^j(h_i)x^{i+2j}\\&=\sum_{i,j}a_j(1+v+v^2)\theta^j(h_{i,1}+vh_{i,2}+v^2h_{i,3})x^{i+2j}\\&=\sum_{i,j}a_j(1+v+v^2)(h_{i,1}+h_{i,2}+h_{i,3})x^{i+2j}.\end{aligned}$$

So $A\subseteq \mathrm{Center}(S)$.

Let $g\notin \mathbb{F}_p[x^2]+A$. Then we have a couple of cases:

Case (1): There exists $g_{2i+1}\in \mathrm{supp}(g)$ such that $g_{2i+1}\neq 0$, and $g_{2i+1}\neq a_{2i+1}(1+v+v^2)$. Assume that $g(x)=g_{2i+1}x^{2i+1}+h(x)$, $h(x)\in S$ and $h_{2i+1}=0$.

If $g\in \mathrm{Center}(S)$, then $g(x)v=vg(x)$. This means that

$$g_{2i+1}\theta(v)x^{2i+1}+h(x)v=(g_{2i+1}x^{2i+1}+h(x))v=v(g_{2i+1}x^{2i+1}+h(x)).$$

So $\theta(v)g_{2i+1}=v^2g_{2i+1}=vg_{2i+1}$. This solution has an answer, if $g_{2i+1}=a_{2i+1}(1+v+v^2)$ or $g_{2i+1}=0$. So there is no $g_{2j+1}\in \mathrm{supp}(g)$ such that $g_{2j+1}\neq a_{2j+1}(1+v+v^2)$.

Case (2): There exists $g_{2i}\in \mathrm{supp}(f)$ such that $g_{2i}\notin \mathbb{F}_p$ and $g_{2i}\neq a_{2i}(1+v+v^2)$. Since $xg=gx$, one can see that

$$x\sum_i g_ix^i=\sum_i g_ix^{i+1}.$$

So $\theta(g_{2i})=g_{2i}$. If $g_{2i}=a+bv+cv^2$, then $a+bv^2+cv=a+bv+cv^2$. Hence, $b=c$. Thus $g_{2i}=a+b(1+v)v$. Also $vxg=gvx$. So

$$vx\sum_i g_ix^i=\sum_i g_ix^ivx=\sum_i g_i\theta^i(v)x^{i+1}.$$

This means that $v\theta(g_{2i})=g_{2i}\theta^{2i}(v)=g_{2i}v$. So $v(a+bv^2+bv)=a+bv+bv^2$. Thus $a=b$ and $g_{2i}=a_{2i}(1+v+v^2)$ which is a contradiction. Hence $\mathrm{Center}(S)=\mathbb{F}_p[x^2]+A$. □

Next corollary describes the cases that $\frac{R[x;\theta]}{x^n-1}$ is a ring.

Corollary 2.3. *We have $x^n-1\in \mathrm{Center}(S)$ if and only if $2|n$. Hence $\frac{R[x;\theta]}{x^n-1}$ is a ring if and only if $2|n$. Otherwise, it is just an R-module. In particular, the skew cyclic codes over R are the ideals of S_n if and only if n is even.*

Theorem 2.4. *Let $f,g\in S$. If the leading coefficient of g is unit, then there exist unique $q,r\in S$ such that $f=qg+r$, $\deg(g)>\deg(r)$.*

Proof. The proof is similar to the one in [5] for Galois rings. Let $f(x) = \sum_{i=0}^{m} f_i x^i$, $g(x) = \sum_{i=0}^{k} g_i x^i$. If $m = 0$, then it remains nothing to prove. So assume inductively that the result holds for integers less than m. Then the degree of $h = f - \frac{f_m}{\theta^{m-k}(g_k)} x^{m-k} g$ is less than the degree of f. So there exist $q, r \in S$ such that $h = qg + r$ and $\deg(r) < \deg(g)$. So

$$f = \left(\frac{f_m}{\theta^{m-k}(g_k)} x^{m-k} + q \right) g + r.$$

Now let $f = q_1 g + r_1 = q_2 g + r_2$. So $(r_1 - r_2) = (q_2 - q_1)g$. Since g_k is unit, if $q_1 \neq q_2$, $\deg(r_1 - r_2) = \deg((q_1 - q_2)g) \leq \deg(g)$. This is impossible and the proof is complete. □

Definition. A subset C of R^n is called a skew cyclic code of length n if C satisfies the following conditions:

(1) C is a submodule of R^n.
(2) If $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, then the skew cyclic shift $(\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C$.

The next theorem gives a characterization of those codes which are skew cyclic:

Theorem 2.5. *The code C is a skew cyclic code with length n over R if and only if C is a S_n-submodule of $S_n = \frac{S}{\langle x^n - 1 \rangle}$.*

Proof. Let C be a skew cyclic code over R. Let $h(x) = \sum_i h_i x^i \in C$ and $g(x) = \sum_i g_i x^i \in S_n$. Then

$$(gh)(x) = \sum_i g_i x^i h(x).$$

Since C is cyclic, $x^i h(x) \in C$, and as C is linear we get $\sum_i g_i x^i h(x) \in C$. So $gh \in C$. Also since C is linear, if $h_1, h_2 \in C$ we have $h_1 - h_2 \in C$.

Now assume that C is a submodule of S_n. Then C is closed under addition (i.e., C is a linear code). Also since C is an ideal, $xC \subseteq C$. So C is a skew cyclic code. □

Corollary 2.6. *If n is even, then every skew cyclic code of length n over R is an ideal of S_n.*

Proof. Since n is even, S_n will be a ring and its submodules are ideals. □

Theorem 2.7. *Let C be a skew cyclic code over R with length n and n is even. If f is the polynomial with the least degree in C and its leading coefficient is unit, then $C = S_n f$.*

Proof. Let $h \in C$. Since the leading coefficient of f is a unit, there exist $q, r \in S_n$ such that $h = qf + r$ and $\deg(r) < \deg(f)$. The facts that $r = h - qf \in C$ and f is the least degree of the polynomials, it yields that $r = 0$. So $h = qf$. □

Theorem 2.8. *The element $a+bv+cv^2$ is a zero divisor of $\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$, if and only if a,b,c satisfy in the equation $a^3+b^3+c^3-3abc=0$.*

Proof. Let $(a+bv+cv^2)(f+vg+v^2h)=0$. So

$$\begin{cases} af+cg+bh=0 \\ ag+bf+ch=0 \\ cf+bg+ah=0. \end{cases}$$

Hence, they satisfy the following matrix equation

$$\begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix} \begin{bmatrix} f \\ g \\ h \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

If this system of equations has a nonzero solution, then the determinant

$$\det\left(\begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix}\right)=0.$$

□

Now we can deduce the following result which shows that every non zero divisor of R is a unit in R.

Theorem 2.9. *Every non zero divisor of R is a unit in R (i.e., $U(R)$ is the set of nonzerodivisors).*

Proof. If the equation

$$\begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix} \begin{bmatrix} f \\ g \\ h \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

has a unique solution $f=g=h=0$, then

$$\det\left(\begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix}\right)\neq 0.$$

So the following matrix equation has a unique solution

$$\begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix} \begin{bmatrix} f \\ g \\ h \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Hence, $a+bv+cv^2$ has an inverse which means that $a+bv+cv^2$ is a unit. □

Lemma 2.10. *Let C be a skew cyclic code and n be even. If g is the polynomial with the smallest degree in C and its leading coefficient is not a unit, then the coefficients of g are zero divisors in R.*

Proof. Let $g(x)=\sum_{i=0}^{m} g_i x^i$ and g_m a nonunit. Then g_m is a zero divisor. So there exists $h\in R$ such that $hg_m=0$. Since $hg\in C$ and $\deg(hg)<m$, $hg=0$, $hg_i=0$ for each $0\leq i<m$. Hence g_i is a zero divisor for each i and $hg=0$. □

Note (1): Finding a zero divisor of an element $l \in R$ is easy. It is enough to solve the following matrix equation. Suppose that $l = a + bv + cv^2$. Then

$$\begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix} \begin{bmatrix} f \\ g \\ h \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix},$$

gives $l(f + vg + v^2h) = 0$.

Note (2): The ring R is principal. So depending the irreducibility of $v^2 + v + 1$, this ring has 4 or 8 ideals. Also, it is easy to see that in each case, all of the ideals are annihilator ideals.

For example, $\langle 1 - v \rangle = \mathrm{Ann}(1 + v + v^2)$. Since an annihilator is a Galois connection, the equation $\mathrm{Ann}(\mathrm{Ann}(I)) = I$ holds for all the ideals of R.

Theorem 2.11. *Let f be the polynomial with the least degree in C and its leading coefficient a nonunit. If $f(x) = \sum_{i=0}^{m} f_i x^i$, then $f = f_m \widehat{f}$ and $\widehat{f} = \sum_{i=0}^{m} \widehat{f}_i x^i$ and $\widehat{f_m}$ is a unit.*

Proof. Let f_m be not unit. So it has a zero divisor like $w \in R$ such that $\langle f_m \rangle \subseteq \mathrm{Ann}(w)$. By Note 2, we also know that every ideals of R are annihilator ideal. So there exists $h \in R$ such that $\langle f_m \rangle = \mathrm{Ann}(h)$. Since $f_i h = 0$ by Lemma 2.10, $f_i \in \mathrm{Ann}(h)$. So $f_i \in \langle f_m \rangle$. Thus, $f_i = f_m \widehat{f_i}$. This completes the proof. □

We now demonstrate our main theorem.

Theorem 2.12. *Let C be a skew cyclic code with length n. Suppose that the leading coefficient of the polynomial f, with the least degree in C, is not a unit. Assume that $g \in C$ be the polynomial with least degree from the following set B :*

$$B = \{k \in C \mid \textit{The leading coefficient of } k \textit{ is unit}\}. \tag{2}$$

If l_i is a divisor of f_m, the leading coefficient of f, then $C = \sum_i S_n \hat{f}_i + S_n g$ where $\hat{f}_i$ is taken to be $l_i \hat{f}$.

Proof. Consider the following set.

$$\Gamma = \{h \in C \mid \deg(f) \leq \deg(h) < \deg(g)\}. \tag{3}$$

For each $h \in C$, there exist q, r such that $h = qg + r$ and $\deg(r) < \deg(g)$. Since $r = h - qg \in C$, $r \in \Gamma$. So we have to find a polynomial with degree less than $\deg(g)$. Assume that f_m is not a unit where $f = \sum_{i=0}^{k} f_i x^i$.

If $\Gamma = \emptyset$, then there is nothing to proof. So let w be the polynomial in Γ with the least degree. Then there are two possibilities:

1) $k - m$ is even. In this case, there are four possibilities. Assume that w_k is the leading coefficient of w.

a) There exist $h, t \in R$ such that $hw_k + lf_m = 1$. Hence $lx^{m-k} f + hw$ is a polynomial in C with degree less than $\deg(g)$ and unit leading coefficient, which is impossible.

b) $f_m = uw_k$ with $u \in U(R)$. If $w_k = f_m h$, then $w - x^{m-k}hf$ has a degree less than w. So $w - x^{m-k}hf = tf$ for some $t \in R$ by definition of w. So $W = (x^{m-k}h + t)f$ which is a contradiction.

c) $f_m h = w_k$. If $f = f_m(ux^m + \cdots)$, then $uw - hx^{m-k}f_m\hat{f}$ has degree less than w. So, $uw - hx^{m-k}f_m\hat{f} = rf$ for some $r \in S$. Hence $w = u^{-1}(hx^{m-k} + r)f$, which is impossible.

d) $f_m = w_k h$. Then w_k is a divisor of f_m. So $w_k = l_i u$ for some i and $u \in U(R)$. Hence $uw - x^{m-k}\hat{f}_i$ has degree less than w. Hence $uw = x^{m-k}\hat{f}_i + rf$ for some $r \in S$. Hence $w = u^{-1}(x^{m-k} + r\sqcap_{i\neq j} l_j)\hat{f}_i$. Thus $w \in R\hat{f}$. So for each $h \in C$ there exist q, r such that $h = qg + r$, $\deg(r) < \deg(g)$. Hence $r = h\hat{f}_i$ for some i and $h \in S$. So $C = \sum_i S\hat{f}_i + Sg$.

2) $k - m$ is odd. The proof is similar to the case (1). It is enough to check the cases of the case (1) for $\theta(g_m)$ instead of g_m.

So if $h \in C$ and $h = qg + r$ where $\deg(r) < \deg(g)$, then $h = qg + \sum_i l_i\widehat{f}_i$. Hence $C = S_n g + \sum_i S_n\widehat{f}_i$. □

Corollary 2.13. *Let C be a skew cyclic code over S_n and n even. Then C is either $\langle\widehat{f}_i\rangle$ or $\langle\widehat{f}_i, g\rangle$, where f are defined as in Theorem 2.12 and g is the polynomial with the least degree and unit leading coefficient.*

Proof. It can be followed by Theorem 2.12 and Theorem 2.7. □

Recall that a set C of n-tuples over a ring R is a *quasi cyclic code* with index d and length n, if C is a linear code and whenever $(c_{0,1}, \ldots, c_{0,d}, c_{1,1}, \ldots, c_{1,d}, \ldots, c_{n-1,1}, \ldots, c_{n-1,d}) \in C$, then $(c_{n-1,1}, \ldots, c_{n-1,d}, c_{0,1}, \ldots, c_{0,d}, \ldots, c_{n-2,1}, \ldots, c_{n-2,d}) \in C$.

This is in fact the submodules of $\left(\frac{R[x]}{x^n-1}\right)^d$.

We also show a relationship between the skew cyclic codes over R and the quasi cyclic codes of R. This is important since we show a relationship between two extensive categories of cyclic codes over R. In this way, we could exploit the properties of quasi cyclic codes in the skew cyclic code.

Theorem 2.14. *Let C be a skew cyclic code with length an even number n. Then C can be considered as a quasi cyclic code of length n with index 2.*

Proof. The proof is similar to the proof of Theorem 3.3 in [11]. Let $n = 2N$ and assume that $c = (c_{0,0}, c_{0,1}, \ldots, c_{N-1,0}, c_{N-1,1}) \in C$. Then by two times shifting we get $(\theta^2(c_{N-1,0}), \theta^2(c_{N-1,1}), \ldots, \theta^2(c_{N-2,0}), \theta^2(c_{N-2,1})) \in C$. Since $\theta^2 = id_R$, we then have $(c_{N-1,0}, c_{N-1,1}, \ldots, c_{N-2,0}, c_{N-2,1}) \in C$. So C is a quasi cyclic code with index 2. □

Since the number of the quasi cyclic codes are the number of submodule of $\left(\frac{R[x]}{\langle x^N-1\rangle}\right)^2$, we can compute the number of skew cyclic codes as follows.

Corollary 2.15. *Let n be even. Then the number of distinct skew cyclic codes of length n over R is equal to the number of $\frac{R[x]}{\langle x^N-1\rangle}$-submodules of $\left(\frac{R[x]}{\langle x^N-1\rangle}\right)^2$, where $N = \frac{n}{2}$.*

Theorem 2.16. *Let n be odd and C be an skew cyclic code of length n. Then C is equivalent to a cyclic code of length n over R.*

Proof. This proof is similar to the proof of Theorem 3.7 [11]. Since n is odd, there exists $k \in \mathbb{Z}, -l\mathbb{N}$ such that $2k + nl = 1$. If $c = (c_0, \ldots, c_{n-1}) \in C$, then $(\theta^{2a}(c_{n-2a+1}), \ldots, \theta^{2a}(c_{n-2a}) \in C$. So $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ which means that C is a cyclic code of length n. □

3. Dual codes and the encoding and decoding description

Let $X = (x_1, x_2, \ldots, x_n)$, $Y = (y_1, y_2, \ldots, y_n)$ be two elements of R^n. Then, the Euclidean and Hermitian inner product of X, Y are as following:

$$\langle X, Y\rangle_E = \sum_i x_i y_i, \quad \langle X, Y\rangle_H = \sum_i x_i \theta(y_i).$$

The Euclidean (respectively Hermitian) dual code $C^\perp$ ($C^{\perp_H}$) of C is defined

$$C^\perp = \{x \in R^n \mid \langle x, c\rangle_E = 0 \text{ for all } c \in C\},$$
$$C^{\perp_H} = \{x \in R^n \mid \langle x, c\rangle_H = 0 \text{ for all } c \in C\}.$$

It can be proved that the dual of a (principal) skew cyclic code is a (principal) skew cyclic code by the following lemmas and the theorem. The proof is similar to the one in [5] or [12]. So we do not prove them here.

Lemma 3.1. *Let n be even and $gh = x^n - 1$. Then $gh = hg$.*

Lemma 3.2. *c is a code word of $C = \langle g\rangle$ if and only if $ch = 0$, where $gh = x^n - 1$.*

Theorem 3.3. *Let n be even, $g \in \text{Center}(S)$ and $hg = x^n - 1$ for some $h \in S$. Then the dual of the code $\frac{\langle g(x)\rangle}{\langle x^n-1\rangle}$ is $\frac{\langle g(x)^\perp\rangle}{\langle x^n-1\rangle}$ where*

$$g(x)^\perp = (h_k + \theta(h_{k-1}) + \cdots + \theta^k(h_0)x^k) + S_n.$$

Definition. A principal code over R is the ideal $\frac{\langle g\rangle}{\langle x^n-1\rangle}$, where n is even and $hg = x^n - 1$ for some $h \in S$.

Note (3): If $g(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_0$, and $g_{n-k} \in U(R)$, then $\frac{\langle g\rangle}{\langle x^n-1\rangle}$ is a skew cyclic code.

Here we explain the process of encoding and decoding. We describe the steps to encode and decode the skew cyclic codes.

Encoding of principal codes:

Let $(u_{k-1},\dots,u_0)$ be the source data. Then $(c_i)_{i=0}^{n-1}$ is the encoded data, where $\sum_{i=0}^{n-1} c_i x^i = (\sum_{i=0}^{n-k} u_i x^i)g(x)$. In matrix equation view, it means that

$$[u_0,\dots,u_{k-1}]\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_{n-k-1}) & \theta(g_{n-k}) & \cdots & 0 \\ 0 & 0 & \theta^2(g_0) & \cdots & \theta(g_{n-k-2}) & \theta(g_{n-k-1}) & \vdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \theta^{k-1}(g_0) & \cdots & \theta^{k-1}(g_{n-k-1}) & \theta^{k-1}(g_{n-k}) \end{bmatrix}_{k\times n}$$

$= (v_0,\dots,v_n)$.

This matrix is called *the generator matrix* of the principal skew cyclic codes.

Decoding of principal codes:

Let $(u_{n-1},\dots,u_0)$ be received. Then, we should compute the reminder of division $\sum_{i=0}^{n-1} u_i x^i$ over $g(x)$ (call it $r(x)$). The decoded word is $(\sum u_i x^i) - r(x)$. So the *parity check matrix* is as follows.

$$\begin{bmatrix} h_k & \theta(h_{k-1}) & \theta^2(h_{k-2}) & \cdots & \theta^k(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_k) & \theta^2(h_{k-1}) & \cdots & \theta^k(h_1) & \theta^{k+1}(h_0) & \cdots & 0 \\ 0 & 0 & \theta^2(h_k) & \cdots & \theta^k(h_2) & \theta^{k+1}(h_1) & \vdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \theta^k(h_k) & \cdots & \theta^{n-2}(h_2) & \theta^{n-1}(h_0) \end{bmatrix}_{n-k\times n}$$

Theorem 3.4. *Let n be even. The minimum Hamming distance of $C = \langle g\rangle$ is the number of independent columns of the parity check matrix.*

Proof. One can see by Lemma 3.2, that C is a code word, if and only if $Ch = 0$ in S_n. Let H_i be the ith column of C. Suppose that $\sum jc_{i_j}H_{i_j} = 0$ for some $j \in \{1,2,\dots,n\}$ and some $c_{i_j} \in R$. We cannot detect the error, if the error terms e is the polynomial $\sum_j c_{i_j}x^{i_j}$. So the minimum Hamming distance is the cardinality of the maximal subset of dependent columns. □

If we consider the distance of $a + bv + cv^2$ and $f + vg + v^2h$ as $\sqrt{(a-f)^2 + (b-g)^2 + (c-h)^2}$, we can define the Lee distance of each two n-tuples over R.

Corollary 3.5. *Let n be even. The minimum Lee distance of $C = \langle g\rangle$ is less than the number of independent columns of the following matrix times $\frac{(p-1)\sqrt{3}}{2}$.*

Proof. Let C have maximum error as the maximum number of some dependent columns (call it L). According to 3.4, the Lee distance will be the

$$\sum_{j=0}^{L} |\widehat{v_{i_j}} - C_{ij}| \le \sum_{j=0}^{L} \frac{(p-1)\sqrt{3}}{2} = L\frac{(p-1)\sqrt{3}}{2}.$$

□

Finally we will give some examples of this code as follows.

Example 3.6. Let C be a skew cyclic code with length 4 over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$ and the generator polynomial $x^2 + (1+v)x + v$. So the generator matrix of this code is:

$$\begin{bmatrix} v & 1+v & 1 & 0 \\ 0 & v^2 & 1+v^2 & 1 \end{bmatrix}_{2\times 4}.$$

This code has the following parity check matrix.

$$\begin{bmatrix} 1 & 1+v^2 & v^2 & 0 \\ 0 & 1 & 1+v & v \end{bmatrix}_{2\times 4}.$$

One can see easily that the minimum Hamming distance for this code is 3. Since the number of bits for each symbol in this code is 8, we should compare this code with a linear code over the ring $\mathbb{F}_8$. This means that this is an optimum code $[4, 2, 3]$ according to [19] or the Singleton bound.

Example 3.7. Let C be a skew cyclic code with length 6 over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$ and the generator polynomial $x^3 + (1+v^2)x + (1+v)x + v^2$. So the generator matrix is:

$$\begin{bmatrix} v^2 & 1+v & 1+v^2 & 1 & 0 & 0 \\ 0 & v & 1+v^2 & 1+v & 1 & 0 \\ 0 & 0 & v^2 & 1+v & 1+v^2 & 1 \end{bmatrix}_{3\times 6}.$$

The minimum Hamming distance of this code is 4 which is equal to an optimum code $[3, 4, 6]$ over $\mathbb{F}_8$ with length 6. Please see [19] or use the Singleton bound.

References

[1] T. Abualrub, A. Ghrayeb, N. Aydin, and I. Siap, *On the construction of skew quasi-cyclic codes*, IEEE Trans. Inform. Theory **56** (2010), no. 5, 2081–2090.

[2] T. Blackford, *Negacyclic codes over Z_4 of even length*, IEEE Trans. Inform. Theory **49** (2003), no. 6, 1417–1424.

[3] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over $F_2 + uF_2$*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1250–1255.

[4] D. Boucher, W. Geiselmann, and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 379–389.

[5] D. Boucher, P. Sole, and F. Ulmer, *Skew constacyclic codes over Galois rings*, Adv. Math. Commun. **2** (2008), no. 3, 273–292.

[6] D. Boucher and F. Ulmer, *A note on the dual codes of module skew codes*, in Cryptography and coding, 230–243, Lecture Notes in Comput. Sci., 7089, Springer, Heidelberg, 2011.

[7] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic cyclic codes*, Des. Codes Cryptogr. **6** (1995), no. 1, 21–35.

[8] P.-L. Cayrel, C. Chabot, and A. Necer, *Quasi-cyclic codes as codes over rings of matrices*, Finite Fields Appl. **16** (2010), no. 2, 100–115.

[9] R. Dastbasteh, H. Mousavi, A. Abualrub, N. Aydin, and J. Haghighat, *Skew cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$*, International J. Information and Coding Theory, Accepted, 2018.

[10] S. T. Dougherty and Y. H. Park, *On modular cyclic codes*, Finite Fields Appl. **13** (2007), no. 1, 31–57.

[11] J. Gao, *Skew cyclic codes over $F_p + vF_p$*, J. Appl. Math. Inform. **31** (2013), no. 3-4, 337–342.

[12] L. Jin, *Skew cyclic codes over ring $F_p + vF_p$*, J. Electronics (China) **31** (2014), no. 3, 228–231.
[13] D. Mandelbaum, *An application of cyclic coding to message identification*, IEEE Transactions on Communication Technology **17** (1969), no. 1, 42–48.
[14] P. Kanwar and S. R. Lopez-Permouth, *Cyclic codes over the integers modulo p^m*, Finite Fields Appl. **3** (1997), no. 4, 334–352.
[15] V. S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over Z_4*, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1594–1600.
[16] I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne, *Skew cyclic codes of arbitrary length*, Int. J. Inf. Coding Theory **2** (2011), no. 1, 10–20.
[17] K. Tokiwa, M. Kasahara, and T. Namekawa, *Burst-error-correction capability of cyclic codes*, Electron. Comm. Japan **66** (1983), no. 11, 60–66.
[18] J. Wolfmann, *Binary images of cyclic codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **47** (2001), no. 5, 1773–1779.
[19] http://www.codetables.de.

Hamed Mousavi
Department of Mathematics
Tarbiat Modares University
Tehran, Iran
Email address: h.moosavi@modares.ac.ir

Ahmad Moussavi
Department of Mathematics
Tarbiat Modares University
Tehran, Iran
Email address: moussavi.a@gmail.com and moussavi.a@modares.ac.ir

Saeed Rahimi
Department of Information Technology
Emam Hossein University
Tehran, Iran
Email address: s.rahmi@sharif.edu