Iranian Journal of Mathematical Sciences and Informatics
Vol. 14, No. 1 (2019), pp 135-145
DOI: 10.7508/ijmsi.2019.01.012

On Skew Cyclic Codes over A Finite Ring

Rasul Mohammadi[a], Saeed Rahimi[b], Hamed Mousavi*[,c]

[a] Department of Mathematics, Faculty of Mathematical Sciences
University of Mazandaran, Babolsar, Iran.
[b] Department of Information Technology, Imam Hossein University,
Tehran, Iran.
[c] Department of Mathematics, Tarbiat Modares University, Tehran, Iran.

E-mail: mohamadi.rasul@yahoo.com
E-mail: s.rahimi@sharif.edu
E-mail: h.moosavi@modares.ac.ir

Abstract. In this paper, we classify the skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, where p is a prime number and $v^3 = v$. Each skew cyclic code is a $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$-submodule of the $(\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p)[x;\theta]$, where $v^3 = v$ and $\theta(v) = -v$. Also, we give an explicit forms for the generator of these codes. Moreover, an algorithm of encoding and decoding for these codes is presented.

Keywords: Skew cycilc codes, Skew polynomial rings, Hamming distance.

2000 Mathematics subject classification: 11T71, 16S36, 68P30.

1. Introduction

Recently, there has been a vast interests on the study of cyclic codes. It is mainly due to their applications in power management [21], secret sharing [24, 23], steganography [14], etc. Also, these codes are easy to design considering their high accuracy and performance. In the last decades, the literature was limited to study the cyclic codes over finite fields. But, recently, there are

*Corresponding Author

Received 04 September 2016; Accepted 08 October 2017

a lot of papers which studies the cyclic codes over finite rings like [8, 18, 9]. First, unlike the finite fields, there is not any limitation for the number of input symbols in the cyclic codes over finite rings. Second, the polynomial ring over a finite ring is not necessarily a UFD. Thus, there may be more divisors for x^n-1 which results in more possibilities to choose a generator polynomial. These benefits pays the way to introduce new families of cyclic coding categories like quasi cyclic codes [1], constacyclic codes [27], and double codes [11].

One of the most applicable type of cyclic codes is skew cyclic codes which were introduced by Boucher in [4]. The structure of these codes are based on the skew polynomial rings. The reason of choosing these non commutative rings is the fact that factorization in these rings is even harder than the one in polynomial rings. So the possibilities of choosing a generator polynomial grows. Boucher also introduced different types of skew cyclic codes in [6, 5]. Then in the papers [19, 10, 26, 12], the skew cyclic codes over different rings are proposed. Also the authors in [13] defined the skew cyclic codes over a finite chain rings.

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. Also, an skew cyclic code C over a ring R is an R-submodule of $R[x;\theta]$ such that if $(c_0,c_1,\cdots,c_{n-1})\in C$, then $(\theta(c_{n-1}),\theta(c_0),\cdots,\theta(c_{n-2})\in C$. If $\mathbb{F}$ is a field, it is proved that codes are in fact the submodules of $\frac{\mathbb{F}[x;\theta]}{<x^n-1>}$ (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, $\frac{R[x;\theta]}{<x^n-1>}$ is a ring if and only if $x^n-1\in Center(R[x;\theta])$. 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 $U=(u_0,\cdots u_{n-1}),V=(v_0,\cdots v_{n-1})$ over a ring T, is the cardinality of the set $\{i|v_i\neq u_i\}$. Also the *Lee distance* U,V is:

$$d_L(U,V)=\sum_{i=0}^{n-1}|u_i-v_i|, \tag{1.1}$$

where $|.|$ means a metric over T.

In this paper, we try to classify the skew cyclic codes over the ring $\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$ where $v^3=v$ and $\theta(v)=-v$. We study the construction of $(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)[x;\theta]$. This helps us to classify the skew cyclic codes. Finally, we propose an algorithm to encode and decode the principle codes. For the other types of codes, we give an explicit form of their generators.

2. On the Ring $(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)[x;\theta]$

We study on the ring $R=(\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p)[x;\theta]$ where $\theta(v)=-v$ and $v^3=v$. First, we have to find the properties of $S=\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$.

Now, we try to find the units and nonzero divisors of S.

Proposition 2.1. *Let $u = a + bv + cv^2 \in S$. Then $u \in U(S)$, if and only if $a \neq 0$ and $a - b + c \neq 0$ or $a + b + c \neq 0$.*

Proof. $\Leftarrow$ As $a \neq 0$ it suffices to prove that $u' = 1 + a^{-1}bv + a^{-1}cv^2 \in U(S)$. For, $\Rightarrow$ Let $u = a + bv + cv^2 \in U(S)$. u is unit, if and only if the following matrix equation has a unique solution.

$$\begin{bmatrix} a & 0 & 0 \\ b & a+c & b \\ c & b & a+c \end{bmatrix} [x, y, z]^T = [1, 0, 0]^T. \tag{2.1}$$

This equation has solution, if and only if the determinant of the above matrix is nonzero. This follows the result. □

Proposition 2.2. *Let $z = a + bv + cv^2 \in S$. Then z is a zero divisor in S, if and only if either $a = 0$, or $a + c - b = 0$, or $a + b + c = 0$.*

Proof. Let $z(d + fv + hv^2) = 0$. So the following equations holds.

$$\begin{aligned} &ad = 0 \\ &bd + (a+c)f + bh = 0 \\ &cd + af + h(c+a) = 0 \end{aligned} \tag{2.2}$$

The above equation has a nonzero solution for the vector (d, f, h), if and only if the determinant of the following matrix is zero.

$$\begin{bmatrix} a & 0 & 0 \\ b & a+c & b \\ c & b & a+c \end{bmatrix}. \tag{2.3}$$

It means that $d + fv + hv^2 \neq 0$, if and only $a((a + c)^2 - b^2) = 0$. So either $a = 0$, or $a + c - b = 0$, or $a + b + c = 0$. □

Corollary 2.3. *$u \in S$ is nonzero divisor, if and only if u is unit.*

Proposition 2.4. *The only automorphisms of S are $\theta(a+bv+cv^2) = a-bv+cv^2$ and the identity.*

Proof. Let $a + bv + cv^2, f + gv + hv^2 \in S$. Let $\theta(v) = x + yv + zv^2$. If θ is an automorphism, then

$$\begin{aligned} x + yv + zv^2 =& \theta(v) = \theta(v^3) = (x + yv + zv^2)^3 \\ =& x^3 + v(3yz^2 + 6xyz + y^3 + 3x^2y) \\ &+ v^2(z^3 + 3xz^2 + 3y^2z + 3x^2z + 3xy^2) \end{aligned} \tag{2.4}$$

If $x = 0$, one can find that $b = \pm 1, z = 0$ or $y = 0, z = \pm 1$. But $v \neq v^2$, so $z = \pm 1$ is impossible. So either $\theta(v) = -v$ or θ is identity.

Assume that $x = \pm 1$. Since v is zero divisor and θ is an automorphism,$x + yv + zv^2$ is also a zero divisor. Considering the fact that $x \neq 0$, $y = \pm z$. So

$$y = y^3 \pm 6y^2 + 6y \quad , \quad \pm y = 4 \pm y^3 + 6y^2 \pm 3y \tag{2.5}$$

One can see that these equations do not have any solution except $y = 0$. But $\theta(v) \neq 1$, since θ is surjective. This ends the proof. □

Proposition 2.5. *$Nil(S) = 0$.*

Proof. Let $z^n = 0$. Without loss of generality, suppose that n is even. So $(a + bv + cv^2)^n = 0$ which means that $a^n = 0$. Hence $z = v(b + cv)$. Since $v(b + cv)$ is a zero divisor, $b^2 = c^2$ or $b = 0$ by lemma 2.2. If $b = 0$, $z = 0$. Assume that $b^2 = c^2$. So

$$0 = v^2(b + cv)^n = v^2b^n(1 + v\sum_{i=0}^{\frac{n}{2}} \binom{n}{2i+1} + v^2\sum_{i=0}^{\frac{n}{2}} \binom{n}{2i}) \tag{2.6}$$

This implies $\sum_{i=0}^{\frac{n}{2}} \binom{n}{2i+1} = 0$ and $\sum_{i=1}^{\frac{n}{2}} \binom{n}{2i} = 1$. So $(1 - 1)^n = 2$ which is impossible. Hence $Nil(S) = 0$. □

Now, we try to study the structure of $R = S[x; \theta]$. In the first place, we find the center of R.

Theorem 2.6. *$center(R) = \{\sum_n z_n x^n | \exists a_n, b_n \in \mathbb{F}_p, z_n = a_n + c_n v^2\}$.*

Proof. Let $f(x) = \sum_n z_n x^n \in center(R)$. Let $z_{2k+1} \neq 0$ for some k. So if $f(x) = h(x) + z_{2k+1}x^{2k+1}$, then

$$\begin{aligned} vf(x) = vh(x) + vz_{2k+1}x^{2k+1} \neq h(x)v - vz_{2k+1}x^{2k+1} &= h(x)v + z_{2k+1}x^{2k+1}v \\ &= f(x)v. \end{aligned} \tag{2.7}$$

So $center(R) \subseteq S[x^2; \theta]$. Now assume that $z_n = a_n + vb_n + v^2c_n$. So

$$\begin{aligned} xf(x) = x\sum_n (a_n + vb_n + v^2c_n)x^n &= \sum_n (a_nx + xvb_n + xv^2c_n)x^n \\ &= \sum_n (a_n - vb_n + v^2c_n)x^{n+1}. \end{aligned} \tag{2.8}$$

Also, $f(x)x = \sum_n (a_n + vb_n + v^2c_n)x^{n+1}$. This means that $xf(x) = f(x)x$, if and only if $b_n = 0$ for all n. On the other hand, since $x^2, v^2x^2 \in center(R)$, so $(\mathbb{F}_p + v^2\mathbb{F}_p)[x^2] \subseteq center(R)$. This completes the proof. □

Corollary 2.7. *$x^n - 1 \in center(R)$, if and only if n is even.*

So if n is even, $R_n = \frac{R}{<x^n - 1>}$ is a ring. Otherwise, R_n is just an R-module.

Proposition 2.8. *Let $I \trianglelefteq R_n$ and n is even. If $g \in I$ is the polynomial with the least degree and the leading coefficient of g is a zero divisor, then all of its coefficients are zero divisors.*

Proof. Let $g(x) = \sum_{n=0}^{m} g_n x^n$ be the polynomial with the least degree. Assume that g_m is a zero divisor. So there exists $h \in S$ such that $hg_m = 0$. Since I is an ideal, $hg \in I$ and its degree is less than the degree of g. This contradicts with the definition of g. So $h \in Ann(g_n)$ for $0 \leq n \leq m$. □

The following example shows that R is not an Euclidean ring.

EXAMPLE 2.9. Let $f(x) = vx^2 + 1, g(x) = vx$. Then

$$\begin{aligned} f(x) &= -xg(x) + 1 \\ f(x) &= -v^2xg(x) + 1. \end{aligned} \tag{2.9}$$

It is clear that $-x \neq -vx$ and $\deg(1) < \deg(vx)$. So R is not Euclidean.

We know that being Euclidean is very useful in decoding process. Unfortunately, R is not Euclidean, but we prove the following theorem to address this problem.

Theorem 2.10. *Let $f, g \in R$ and g be a polynomial with unit leading coefficient. Then there exists unique $q, r \in R$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.*

Proof. The proof is similar to the one in [6] for Galois rings. Let $f(x) = \sum_{i=0}^{m} f_i x^i$, $g(x) = \sum_{i=0}^{k} g_i x^i$. We will do it by induction. Let $m = 0$. Since $f(x) = f_0 \in U(R)$, $g(x) = g(x)f_0^{-1}f_0 + 0$. So assume that the result holds for integers less than m. Then if $h = f - \frac{f_m}{\theta^{m-k}(g_k)}x^{m-k}g$, $\deg(h) < \deg(f)$. So there exists $q, r \in S$ such that $h = qg + r$ and $\deg(r) < \deg(g)$. This means that

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

Now let $f = q_1g + r_1 = q_2g + r_2$. So $(r_1 - r_2) = (q_2 - q_1)g$. g is monic, so

$$\deg(r_1 - r_2) = \deg((q_2 - q_1)g) \geq \deg(g) > \deg(r_1) \geq \deg(r_1 - r_2). \tag{2.10}$$

This is impossible and the proof is complete. □

Theorem 2.11. *Let $I \trianglelefteq R$. Suppose that $g \in I$ be the polynomial with the least degree. If g is monic, then $I = Rg$.*

Proof. Let $f \in I$. There exists $q, r \in R$ such that $f = qg + r, \deg(r) < \deg(g)$. Since $f, qg \in I$, $r \in I$. This contradicts by the definition of g. □

Proposition 2.12. *Let $f \in R$. Then there exists $g \in R$ such that $fv = vg$.*

Proof. Let $f(x) = \sum_n f_n x^n$ for some $a, b, c \in \mathbb{F}_p[x]$. Then

$$fv = (\sum_n f_n x^n)v = \sum_{n=2k} vf_n x^n - \sum_{n=2k+1} vf_n x^n. \tag{2.11}$$

So $g(x) = \sum_{n=2k} f_n x^n - \sum_{n=2k+1} f_n x^n$. □

Definition 2.13. The *partaker* of $f \in R$ is the polynomial f' such that $fv = vf'$.

Next theorem gives a condition for the unit elements of R.

Theorem 2.14. *Let $f \in U(R)$. If $f(x) = \sum_n (a_n + vb_n + v^2c_n)x^n$, then $a_0 \neq 0$ and $a_n = 0, n > 0$.*

Proof. Let $f \in U(R)$. If $k(x) = \sum_n a_n x^n, g(x) = \sum_n b_n x^n, h(x) = \sum_n c_n x^n$. If $f^{-1} = u + vw + v^2y$, then

$$\begin{aligned} 1 = (k + vg + v^2h)(u + vw + v^2y) =& ku + v(k'w + gu + gy + h'w) \\ &+ v^2(g'w + hy + gy + h'w). \end{aligned} \tag{2.12}$$

So $k, u \in \mathbb{F}_p$ which follows the result. □

Lemma 2.15. *Let $h \in S$. Then there are three possible cases.*
i) There exists $t, s \in S$ such that $th + s(1 - v^2) = 1$.
ii) $1 - v|h$.
iii) $1 + v|h$.

Proof. Let $h \in S$. If $1 - v \nmid h$ and $1 + v \nmid h$, $h_1 - h_2 + h_3 \neq 0$. One can see

$$\begin{aligned} &\Big(v^2h_2^{-1}(v - (h_1 + h_3)h_2^{-1})(1 - (h_1 + h_3)h_2^{-1})\Big)(h_1 + vh_2 + v_3^h) \\ &+ \Big((1 - (h_1 + h_3)h_2^{-1}) + v^2h_2^{-1}(v - (h_1 + h_3)h_2^{-1})(1 - (h_1 + h_3)h_2^{-1})\Big)(1 - v^2) \\ &= 1. \end{aligned} \tag{2.13}$$

□

Theorem 2.16. *Let I be an R-submodule of R. Suppose that there is no monic polynomial in I of minimal degree and $f(x)$ is a non-monic polynomial in I of minimal degree. Let $f = f_m h$ for some monic polynomial h. Then $I \subseteq Rg + \sum_i Rb_i h$ for some $b_i \in S$.*

Proof. Let $f(x) = f_0 + f_1x + \cdots + f_mx^m \in I$ be a non-monic polynomial in I of minimal degree. Since there is no monic polynomial in I of minimal degree, $f(x) = f_t h$ for some monic polynomial h. If

$$\Gamma = \{k \in I | \deg(f) < \deg(k) < \deg(g)\} \tag{2.14}$$

is empty, there will be nothing to prove. Otherwise, let $w(x)$ be the polynomial with minimal degree k. First, let $k - m$ is even. Then there are four cases.

a) There exists $l, t \in R$ such that $lw_k + tf_m = 1$. Hence $tx^{m-k}f + lw$ is a polynomial in C with degree less than $deg(g)$ and unit leading coefficient, which is impossible.

b) There exists $l, t \in R$ such that $lf_m = tw_k$. So $lx^{k-m}f - tw$ has degree less than $\deg(w)$. Hence, $lx^{k-m}f - tw = rf$ for some $r \in R$. Thus $w = bh$ for some $b \in S$.

Now, assume that $k \in I$. There exists $q, s \in R$ such that $w = qg + s$ and $\deg(s) < \deg g$. So there exists $b \in R$ such that $s = bh$. So $I \subseteq RG + \sum_i Rb_ih$.

Second, assume that $k - m$ is odd. It is enough to discuss the same cases for $\theta(g_m)$ instead of g_m.

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

Corollary 2.17. *Each submodule I of R is in only one of the following forms.*

i) $I = Rg$, where g is the polynomial with the least degree and g is monic.

ii) $I \subseteq Rg + \sum_i Rb_ih$, where $b_i \in S$ and g be the monic polynomial with the least degree.Also, if f is the polynomial with the least degree in I, there exists t sich that $th = f$.

3. Skew Cyclic Codes over S

We know that each skew cyclic code is an R-submodule of R_n. So we try to classify the codes with arbitrary length over S.

Theorem 3.1. *C is an skew cyclic code with length n over S, if and only if C is a submodule of R_n.*

Proof. Let C be an skew cyclic code over S and $c, d \in C$. Let $c(x) = \sum_{i=0}^{n-1} c_ix^i$, $d(x) = \sum_{i=0}^{n-1} d_ix^i$. Since C is a linear code, $c + d \in C$. Also, $xc \in C$, because C is cyclic. This means that $f(x)c \in C$ for some $f \in R_n$. So C is a submodule.

Now assume that C is a submodule of R_n and $c, d \in C$. The definition of submodule causes that $c + d \in C$, $xc \in C$. So C is an skew cyclic code over S. □

Theorem 3.2. *Let C be a code over S. Then C can be as only one of the following form.*

i) $C = R_n\overline{g}$,where $\overline{g} \in R_n$ is the polynomial with the least degree; also it is monic and $x^n - 1 = gl$ for some $l \in R$.

ii) $C \subseteq R_n\overline{g} + \sum_i \frac{Rb_ih + <x^n-1>}{<x^n-1>}$, where $\overline{g} \in R_n$ is the monic polynomial with the least degree; also $\overline{f} = \overline{f_mh}$ is the polynomial with the least degree and $\overline{h}$ is monic.Moreover, $x^n - 1 = gl$ for some $l \in R$.

Proof. This is because of the fact that C is in the form of $\frac{I}{<x^n-1>}$ for some $I \leqslant R$ by correspondence theorem for modules. The rest is followed by theorem 2.17 and $x^n - 1 \in I$. □

The following theorem shows a correspondence between skew cyclic codes and quasi cyclic codes.

Theorem 3.3. *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. It is similar to the proof of theorem 3.7 in [10]. □

Lemma 3.4. *Let $g(x) \in R$ and $g(x)h(x) = x^n - 1$ for some $h \in R$. Then $h(x)g(x) = x^n - 1$.*

Proof. The proof is similar to the one in lemma 2 in [12]. □

Definition 3.5. Let $X = (x_1, x_2, \cdots, x_n)$ and $Y = (y_1, \cdots, y_n)$ be a couple of elements in R^n. The Euclidean and Hermitian inner products of X, Y are defined as

$$< X, Y >_E = \sum_i x_i y_i \tag{3.1}$$

$$< X, Y >_H = \sum_i x_i \theta(y_i). \tag{3.2}$$

Also, the Ecleadian dual code $C^{\perp}(C^{\perp_H})$ of C is

$$\begin{aligned} C^{\perp} &= \{x \in R^n | \forall c \in C, < x, c >_E = 0\} \\ C^{\perp_H} &= \{x \in R^n | \forall c \in C, < x, c >_H = 0\} \end{aligned} \tag{3.3}$$

Now we try to explain the encoding and decoding of principle codes.

Encoding of Principle Codes:

Let $C =< g >$ and $U = (u_0, u_2, \cdots, u_{k-1})$ be the impute of the transmission. Suppose that $u(x) = \sum_i u_i x^i$. To encode, we need to compute $u(x)g(x)$ as follows

$$[u_0, u_2, \cdots, u_{k-1}] \times \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_{n-k-2}) & \theta(g_{n-k-1}) & \cdots & 0 \\ 0 & 0 & \theta^2(g_0) & \cdots & \theta(g_{n-k-3}) & \theta(g_{n-k-2}) & \vdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \theta^{k-1}(g_0) & \cdots & \theta^{k-1}(g_{n-k-2}) & \theta^{k-1}(g_{n-k-1}) \end{bmatrix}_{k \times n}$$
$$= [v_0, v_1, \cdots, v_{n-1}]. \tag{3.4}$$

Decoding of Principle Codes:

Assume that $Y = (y_1, \cdots, y_n)$ is received through the channel. Suppose that $g(x)h(x) = x^n - 1$ and $h(x) = \sum_i h_i x^i$. To decode, first, we should compute

$$\begin{bmatrix} r_0 \\ r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_k & 0 & \cdots & 0 \\ 0 & \theta(h_0) & \theta(h_1) & \cdots & \theta(h_{k-1}) & \theta(h_k) & \cdots & 0 \\ 0 & 0 & h_0 & \cdots & h_{k-2} & h_{k-1} & \vdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \theta^{n-k-1}(h_0) & \cdots & \theta^{n-k-1}(g_{k-2}) & \theta^{n-k-1}(h_k) \end{bmatrix} \times \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix} \tag{3.5}$$

Then, we can check the vector $[r_1, \cdots, r_n]^T$ in the syndrome decoding table and find the codeword.

Theorem 3.6. *The minimum distance of C is equal to the maximum number of dependent columns of the following matrix*

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_k & 0 & \cdots & 0 \\ 0 & \theta(h_0) & \theta(h_1) & \cdots & \theta(h_{k-1}) & \theta(h_k) & \cdots & 0 \\ 0 & 0 & h_0 & \cdots & h_{k-2} & h_{k-1} & \vdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \theta^{n-k-1}(h_0) & \cdots & \theta^{n-k-1}(g_{k-2}) & \theta^{n-k-1}(h_k) \end{bmatrix}_{n-k \times n} \tag{3.6}$$

Proof. Let Y is received. Assume that the error is not detectable. Assume that the real input is L. So $L + E = Y$ where E is the error vector. So the error vector E with minimum weight, which is necessary for occurring a non-detectable error satisfies $(L + E)H = 0$. Also, since L is the codeword, $LH = 0$. This implies $EH = 0$. So if the non zero entries of E are the nonzero coefficients of a linear combination of columns of H, a non detectable error occures. This completes the proof. □

Acknowledgments

The authors would like to thank Mr Farzad Padashnik and Ms Foroogh Mousavi for their insightful comments. Research described in this paper was financed and supported by EXAMIE.

References

1. T. Abuarub, A. Ghrayeb, N. Aydin, I. Siap, On the Construction of Skew Quasi-cyclic Codes, *IEEE Transactions on Information Theory*, **56**(5), (2010), 2081-2090.

2. T. Blackford, Negacyclic Codes over Z_4 of Even Length, *IEEE Transactions on Information Theory*, **49**(6),(2003), 1417-1424.
3. A. Bonnecaze and U. Parampalli, Cyclic Codes and Self-dual Codes over F_2+uF_2, *IEEE Transactions on Information Theory*, **45**(4), (1999), 1250-1255.
4. D. Boucher, W. Geiselmann, F. Ulmer, Skew-cyclic Codes, Applicable Algebra in Engineering, *Communication and Computing*, **18**(4), (2007), 379-389.
5. D. Boucher, F. Ulmer, A Note on the Dual Codes of Module Skew Codes, *Cryptography and Coding Springer Berlin Heidelberg*, (2011), 230-243.
6. D. Boucher, P. Sole, F. Ulmer, Skew Constacyclic Codes over Galois Rings, *Advances in Mathematics of Communications*, **23**(3), (2008), 273292.
7. A. R. Calderbank and J. S. Neil, Modular and p-adic Cyclic Codes, *Designs Codes and Cryptography*, **6**(1), (1995), 21-35.
8. Cengellenmis, Yasemin, On the Cyclic Codes over $F_3 + vF_3$, *International Journal of Algebra*, **4**(6), (2010), 253-259.
9. S. T. Dougherty and H. P Young, On modular cyclic codes, *Finite Fields and Their Applications*, **13**(1), (2007), 31-57.
10. J. Gao, Skew Cyclic Codes over $F_p + vF_p$, *J. Appl. Math. Inform*, **31**(3-4), (2013), 337-342.
11. J. Gao, Sh. Minjia, W. Tingting, F. Fang-Wei, On Double Cyclic Codes over $\mathbb{Z}_4$, *Finite Fields and Their Applications* **39**, (2016), 233-250.
12. L. Jin, Skew Cyclic Codes over Ring $F_p + vF_p$, *Journal of Electronics*(China), **31**(3), (2014), 228-231.
13. S. Jitman, L. San, P. Udomkavanich, Skew Constacyclic Codes over Finite Chain Rings, *arXiv preprint*, 1008.0327(2010).
14. D. Mandelbaum, An Application of Cyclic Coding to Message Identification. *IEEE Transactions on Communication Technology*, **17**(1), (1969), 42–48.
15. C. Pierre-Louis, C. Christophe, N. Abdelkader, Quasi-cyclic Codes as Codes over Rings of Matrices, *Finite Fields and Their Applications*, **16**(2), (2010), 100-115.
16. V. S. Pless, Q. Zhong, Cyclic Codes and Quadratic Residue Codes over Z_4, *IEEE Transactions on Information Theory*, **42**(5), (1996), 1594-1600.
17. K. Pramod, S. R. Lopez-Permouth, Cyclic Codes over the Integers Modulo p^m, *Finite Fields and Their Applications*, **3**(4), (1997), 334-352.
18. Qian, Jianfa, Quantum Codes from Cyclic Codes over $F_2 + vF_2$, *Journal of Inform. and computational Science*, **6**, (2013), 1715-1722.
19. I. Siap, T. Abualrub, N. Aydin, P. Seneviratne, Skew Cyclic Codes of Arbitrary Length, *International Journal of Information and Coding Theory*, **2**(1), (2011), 10-20.
20. S. Irfan, T. Abualrub, N. Aydin, P. Seneviratne, Skew Cyclic Codes of Arbitrary Length, *International Journal of Information and Coding Theory*, **2**(1), (2011), 10-20.
21. T. Kinichiroh, M. Kasahara, T. Namekawa. Burst-error-correction Capability of Cyclic Codes." *Electronics and Communications in Japan (Part I: Communications)* **66**(11), (1983), 60-66.
22. J. Wolfmann, Binary Images of Cyclic Codes over $\mathbb{Z}_4$, *IEEE Transactions on Information Theory*, **47**(5),(2001) 1773.
23. X.-F. Xu, D.-S. Wang, Sh.-D. Li, Ch.-N. Yang, An Anti-cheating Block Secret Sharing Scheme Based on Cyclic Codes, *Intelligent Information Hiding and Multimedia Signal Processing, Ninth International Conference on IEEE*, (2013), 369-372.
24. J. Yuan, and C. Ding, Secret Sharing Schemes from Three Classes of Linear Codes, *IEEE transactions on information theory*, **52**(1), (2006). 206-212.
25. G. Zhang, Ch. Bocong, Constacyclic Codes over $F_p + vF_p$, *arXiv preprint*, 1301.0669, (2013).

26. G. Zhang, B. Chen, Constacyclic Codes over $F_p + vF_p$, *Cornell University, Computer Science*, (2013).
27. Sh. Zhu, L. Wang, A Class of Constacyclic Codes over $F_p + vF_p$ and its Gray Image, *Discrete Mathematics*, **311**(23), (2011), 2677-2682.
28. *http* : *//www.codetables.de*.