Skew Cyclic Codes Of Arbitrary Length Over $R = \frac{F_p[v]}{v^{2^k}-1}$

Alireza Soleimani*

Faculty of Mathematics, Tarbiat Modares University, Tehran, Iran

Article Info

Keywords
Skew cyclic code,
Ring,
Code over ring

Article history
Received: 25 November 2020
Accepted: 13 February 2021

Abstract

In the current paper, we study an special type of Cyclic Codes called skew Cyclic codes over the ring $R = \frac{F_p[v]}{(v^{2^k}-1)}$, where p is a prime number. This sets of codes are the result of module (or ring) structure of the skew polynomial ring

$R[x,\theta]$ where $v^{2^k} = 1$ and is an F_p -automorphism such that$\theta(v) = v^{2^k-1}$. We show that when n is even these codes are principal and if n is odd these code. Look like a module and proof some properties.

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. 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 $\frac{R[x]}{\langle x^n - 1\rangle}$. These advantages lead the researchers to study different classes of cyclic code category. One of the interesting types of generalizing of the notion

*Corresponding author's E-mail: mr.soleymani25@yahoo.com 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 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 $(c_0,c_1,.........,c_{n-1}) \in C$ it implies that $(\theta(c_{n-1}),\theta(c_0),.........,\theta(c_{n-2})) \in C$.

For a given automorphism θ of R, the set $R[x,\theta]$ consisting of polynomials $f = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$, 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 [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 $\frac{R[x]}{\langle x^n - 1\rangle}$. The module $\frac{R[x]}{\langle x^n - 1\rangle}$ is not necessarily a ring, unless $x^n - 1 \in Center(R)$. 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.

In this paper, we study the skew cyclic codes over the ring $R = \frac{F_p[v]}{(v^{2^k} - 1)}$ where $v^{2^k} = 1$.

we will find the structure of the ideals of $R[x,\theta]$ where θ is an F_p -automorphism such that $\theta(v) = v^{2^k - 1}$,$(i.e., \theta^2 = 1)$. 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 $\frac{R[x,\theta]}{\langle x^n - 1\rangle}$ is not a ring. We show that skew cyclic codes are submodules of the mentioned module. If F is a field, it is proved that codes are in fact the submodules of $\frac{F[x,\theta]}{\langle x^n - 1\rangle}$. We prove the same result for skew cyclic code over $R = \frac{F_p[v]}{\left(v^{2^k} - 1\right)}$. Also for each ring R, $\frac{R[x,\theta]}{\langle x^n - 1\rangle}$ is a ring if and only if $x^n - 1 \in Center\left(R[x,\theta]\right)$

2. The structure of ideals of the ring $\frac{R[x,\theta]}{\langle x^n - 1\rangle}$

Let p be a prime number and F_p be a finite field. Then consider a ring $R = \frac{F_p[v]}{\left(v^{2^k} - 1\right)}$ where . To produce a skew polynomial version of this ring, we need the following.

Theorem 2.1. Let $\theta : R \to R$ with $\theta\left(a_0 + a_1 v + \ldots + a_{2^k-1} v^{2^k-1}\right) = a_0 + a_{2^k-1} v + \ldots a_1 v^{2^k-1}$. Then θ is a ring automorphism.

Proof. First, we prove that θ is linear. To do this, let $a_0 + a_1 v + \ldots + a_{2^k-1} v^{2^k-1}, b_0 + b_1 v + \ldots + b_{2^k-1} v^{2^k-1} \in R$. Then

$$\theta\left(a_0 + a_1 v + \ldots + a_{2^k-1} v^{2^k-1}\right) + \theta\left(b_0 + b_1 v + \ldots + b_{2^k-1} v^{2^k-1}\right) =$$

$$a_0 + a_{2^k-1} v + ..a_1 v^{2^k-1} + b_0 + b_{2^k-1} v + ..b_1 v^{2^k-1} = \left(a_0 + b_0\right) + \left(a_{2^k-1} + b_{2^k-1}\right)v + \ldots + \left(a_1 + b_1\right)v^{2^k-1}$$

$$= \left(\left(a_0 + b_0\right) + \left(a_1 + b_1\right)v + \ldots + \left(a_{2^k-1} + b_{2^k-1}\right)\right) .$$

So θ is additive.

One can see that the following equations hold for each $a_i, b_i \in F_p \left(0 \le i \le 2^k - 1\right)$:

$$\theta\left(a_0 + a_1 v + \ldots + a_{2^k-1} v^{2^k-1}\right)\theta\left(b_0 + b_1 v + \ldots + b_{2^k-1} v^{2^k-1}\right)$$

$$= \left(a_0 + a_1 v^{2^k-1} + \ldots + a_{2^k-1} v\right)\left(b_0 + b_1 v^{2^k-1} + \ldots + b_{2^k-1} v\right)$$

$$=\left(a_0b_0+a_{2^k-1}b_1+a_{2^k-2}b_2+\ldots+a_1b_{2^k-1}\right)+\ldots+\left(a_0b_1+\ldots.+a_1b_0\right)v^{2^k-1}$$

$$=\theta\left(\left(a_0b_0+a_{2^k-1}b_1+a_{2^k-2}b_2+\ldots+a_1b_{2^k-1}\right)+\left(a_0b_1+\ldots+a_1b_0\right)v+\ldots+\left(a_0b_{2^k-1}+\ldots+a_{2^k-1}b_0\right)v^{2^k-1}\right)$$

$$=\theta\left(\left(a_0+a_1v+\ldots+a_{2^k-1}v^{2^k-1}\right)\left(b_0+b_1v+\ldots+b_{2^k-1}v^{2^k-1}\right)\right)$$

Also, for each $a_0+a_1v+\ldots+a_{2^k-1}v^{2^k-1}$, we have $\theta\left(a_0+a_1v+\ldots+a_{2^k-1}v^{2^k-1}\right)=a_0+a_1v^{2^k-1}+\ldots+a_{2^k-1}v$

Moreover, $\theta\left(a_0+a_1v+\ldots+a_{2^k-1}v^{2^k-1}\right)=0$ if and only if $a_i=b_i=0\left(0\le i\le 2^k-1\right)$. □

Throughout this paper, R will denote the ring $\frac{F_p[v]}{\left(v^{2^k}-1\right)}$ and S the ring $R[x,\theta]$, and S_n will denote $\frac{R[x,\theta]}{\langle x^n-1\rangle}$.

Properties of skew cyclic codes are closely related to properties of $R[x,\theta]$. The ring $R[x,\theta]$ is a left and right euclidean ring whose left and right ideals are principal. Here right division means that for $P_1(x),P_2(x)\in R[x,\theta]$ which are non zero, there exist unique polynomials $Q(x),R(x)\in R[x,\theta]$ such that

$$P_1(x)=Q(x).P_2(x)+R(x)$$

If $R(x)=0$ then $P_2(x)$ is a right divisor of $P_1(x)$ in $R[x,\theta]$. The definition of left divisor in $R[x,\theta]$ is similar using the left euclidean division.

In particular central elements of $R[x,\theta]$ are the generators of two-sided ideals in $R[x,\theta]$. Therefore, if $|\langle\theta\rangle|$ divides n, then $\left(x^n-1\right)\subset R[x,\theta]$ is a two-sided ideal.

Lemma 2.1 $\left(x^n-1\right)\in Z\left(R[x,\theta]\right)$ if and only if $m\,|\,n$ where $Z\left(R[x,\theta]\right)$ is the center of $R[x,\theta]$ and m is a order of θ.

Proof. Assume $m\,|\,n$ and let $f(x)\in R[x,\theta]$, say

$$f(x)=a_0+a_1x+\ldots+a_rx^r$$

Since $m\,|\,n$, $\theta^n(a)=a$ gor any $a\in R$. Hence

$$(x^n-1)*f(x)=(x^n-1)*\left(a_0+a_1v+\ldots+a_{2^k-1}v^{2^k-1}\right)$$

$$=x^n*a_0+x^n*a_1x+\ldots.+x^n*a_rx^r-f(x)$$

$$=\theta^n(a_0)x^n+\theta^n(a_1)x^nx+\ldots.+\theta^n(a_r)x^nx^r-f(x)$$

$$=a_0x^n+a_1x\,x^n+\ldots.+a_rx^r\,x^n-f(x)$$

$$=\left(a_0+a_1x+\ldots+a_rx^r\right)*x^n-f(x)$$

$$=f(x)*(x^n-1)$$

Hence $(x^n-1)\in Z(R[x,\theta])$.

Conversely, suppose $(x^n-1)\in Z(R[x,\theta])$. Then x^n-1 commutes with every element of $R[x,\theta]$. In particular, $(x^n-1)*ax^m=ax^m*(x^n-1)$, for any $a\in R$. Now $(x^n-1)*ax^m=\theta^n(a)x^{n+m}-ax^m$, and $ax^m*(x^n-1)=ax^{n+m}-ax^m$, This implies that $\theta^n(a)=a$ for all $a\in R$, hence $m\,|\,n$. □

Lemma 2.2. Let R be a ring θ an automorphism of R and n an integer divisible by the order $|\langle\theta\rangle|$ of θ. The ring $\frac{R[x,\theta]}{\langle x^n-1\rangle}$ is a principal left ideal domain in which left ideals are generated G where G is a right divisor of x^n-1 in $R[x,\theta]$.

Proof. The proof is an exact copy of the commutative case only taking care of left and right. Let I be a left ideal of $\frac{R[x,\theta]}{\langle x^n-1\rangle}$. if $I=\{0\}$ then $I=(0)$ Otherwise denote $G\in I$ a monic non zero polynomial of minimal degree in I. Let $p \in I$ be an arbitrary element of I. Performing a right division of P by G in $R[x,\theta]$ we get

$$P = Q.G + R$$
$$\text{where deg(R)} < \text{deg(G)}$$

from which we get $P - Q.G = R \in I$ By minimality of the degree of G we must have $R = 0$, showing that $P = Q.G$, and thus $I = (G)$.

For a second part let I be a left ideal of $\frac{R[x,\theta]}{\langle x^n - 1\rangle}$ and denote $G \in I$ a monic non zero polynomial of minimal degree in I. we now that $x^n - 1$ is a zero of $\frac{R[x,\theta]}{\langle x^n - 1\rangle}$ now we Performing a right division of $x^n - 1$ by G in $R[x,\theta]$ we get

$$x^n - 1 = P.G + R$$
$$\text{where deg(R)} < \text{deg(G)}$$

from which we get $x^n - 1 - P.G = R \in I$ By minimality of the degree of G we must have $R = 0$, showing that $x^n - 1 = P.G$, and thus G is a right divisor of $x^n - 1$ in $R[x,\theta]$. □

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 $\mathrm{c} = (\mathrm{c}_0, \mathrm{c}_1, \ldots, \mathrm{c}_{\text{n-1}}) \in \mathrm{C}$ then the skew cyclic shift

$(\theta(\mathrm{c}_{\text{n-1}}), \theta(\mathrm{c}_0), \ldots, \theta(\mathrm{c}_{\text{n-2}})) \in \mathrm{C}$

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

Theorem 2.2 Let R be a ring θ an automorphism of R and C be a linear code over R of length n. If $|\langle\theta\rangle|$ the order of θ, divides n, then the code C is skew cyclic code if and only if C is a left ideal of $\frac{R[x,\theta]}{\langle x^n-1\rangle}$.

Above theorem when work $|\langle\theta\rangle|$ the order of θ, divides n, but for the general case the following theorem is presented.

Theorem 2.3 The code C is a skew cyclic code with length n over R if and only if C is a S_n -submodule of $S_n=\frac{R[x,\theta]}{\langle x^n-1\rangle}$.

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 ge $(gh)(x)=\sum_i g_i x^i h(x)\in C$. so $gh\in C$. Also since C is linear, if $\mathrm{h}_1,\mathrm{h}_2\in C$ we have $\mathrm{h}_1-\mathrm{h}_2\in C$.

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, $xC\subset C$. So C is a skew cyclic code. □

Definition. 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 $(\mathrm{c}_{0,1},\dots,\mathrm{c}_{0,\mathrm{d}},\mathrm{c}_{1,1},\dots,\mathrm{c}_{1,\mathrm{d}},\dots,\mathrm{c}_{\mathrm{n-1},1},\dots,\mathrm{c}_{\mathrm{n-1,d}})\in\mathrm{C}$, then $(\mathrm{c}_{\mathrm{n-1},1},\dots,\mathrm{c}_{\mathrm{n-1,d}},\mathrm{c}_{0,1},\dots,\mathrm{c}_{0,\mathrm{d}},\dots,\mathrm{c}_{\mathrm{n-2},1},\dots,\mathrm{c}_{\mathrm{n-2,d}})\in\mathrm{C}$.

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 2.4 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. Let $n=2N$ and assume that $\mathrm{c}=(\mathrm{c}_{0,0},\mathrm{c}_{0,1},\ldots,\mathrm{c}_{\mathrm{N}-1,0},\mathrm{c}_{\mathrm{N}-1,1})\in\mathrm{C}$. Then by two times shifting we get $(\theta^2(\mathrm{c}_{\mathrm{N}-1,0}),\theta^2(\mathrm{c}_{\mathrm{N}-1,1}),\ldots,\theta^2(\mathrm{c}_{\mathrm{N}-2,0}),\theta^2(\mathrm{c}_{\mathrm{N}-2,1}))\in\mathrm{C}$. Since $\theta^2=id_R$ we then have $(\mathrm{c}_{\mathrm{N}-1,0},\mathrm{c}_{\mathrm{N}-1,1},\ldots,\mathrm{c}_{\mathrm{N}-2,0},\mathrm{c}_{\mathrm{N}-2,1})\in\mathrm{C}$. 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 2.1. 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 $N=\frac{n}{2}$

In the proofs of the following theorems, we will use the following fact from elementary number theory. Let d be the greatest common divisors of the integers a and b (denoted by $(a,b)=d$. Then there exist integers x and y such that

$$ax+by=d.$$

This representation is not unique. In fact, if we let $x_0=x+k\frac{b}{(a,b)}$, and $y_0=y-k\frac{a}{(a,b)}$, for some integer k, then

$$ax_0+by_0=ax+k\frac{ab}{(a,b)}+by-\frac{ba}{(a,b)} \qquad (1)$$

$$ax+by=d$$

Theorem 2.5 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. Let $C = (g(x))$ be a skew cyclic code of length n such that $(2, n) = 1$. We know that there exist integers α_1, α_2 such that

$$2\alpha_1 + n\alpha_2 = 1$$

By Equation 1 we may assume that α_2 is a negative integer, so we can write $2\alpha_1 = 1 + Dn$ where $D > 0$. Let $\mathrm{c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}} \in \mathrm{C}$. To show that C is a cyclic code it is suffices to show that $\mathrm{c_{n-1} + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-2}} \in \mathrm{C}$. Consider

$$x^{2\alpha_1} * c(x)$$

$$= \mathrm{x^{1+Dn} * \left(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}\right)}$$

$$= \theta^{1+Dn}(c_0)x^{1+Dn} + \ldots. + \theta^{1+Dn}(c_{n-2})x^{1+Dn+n-2} + \theta^{1+Dn}(c_{n-1})x^{1+Dn+n-1}$$

$$= \theta^{2\alpha_1}(c_0)x^{1+Dn} + \ldots. + \theta^{2\alpha_1}(c_{n-2})x^{Dn+n-1} + \theta^{2\alpha_1}(c_{n-1})x^{Dn+n}$$

Note that in the ring $\dfrac{R[x,\theta]}{\langle x^n - 1\rangle}$, we have $x^n = 1$ and $\theta^2(a) = a$ for any $a \in R$. This implies that $x^{2\alpha_1} * c(x) = \mathrm{c_{n-1} + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-2}} \in \mathrm{C}$. Thus, C is a cyclic code of length n. □

This theorem yields the following corollary.

Corollary 2.2 For $(2, n) = 1$ if f(x) is a factor of $x^n - 1$ in $R[x, \theta]$, then f(x) is also a factor of $x^n - 1$ in the usual polynomial ring $R[x]$.

Theorem 2.6 Let $C = (g(x))$ be a skew cyclic code of length n and let θ be an automorphism of R with $|\langle\theta\rangle| = 2$. If $(2, n) = d$ then C is equivalent to a QC code of length n and index d.

Proof Let n = ds and

$\mathrm{c} = \left(\mathrm{c}_{0,0},\mathrm{c}_{0,1},\ldots,\mathrm{c}_{0,\text{d-1}},\mathrm{c}_{1,0},\mathrm{c}_{1,1},\ldots,\mathrm{c}_{1,\text{d-1}},\ldots,\mathrm{c}_{\text{s-1},0},\mathrm{c}_{\text{s-1},1},\ldots,\mathrm{c}_{\text{s-1,d-1}}\right) \in C$. Since $(2,n) = d$ we may write $2\alpha_1 = d + Jn$ for some nonnegative integer J. Consider

$$\theta^{d+Jn}\left(\mathrm{c}_{0,0},\mathrm{c}_{0,1},\ldots,\mathrm{c}_{0,\text{d-1}},\mathrm{c}_{1,0},\mathrm{c}_{1,1},\ldots,\mathrm{c}_{1,\text{d-1}},\ldots,\mathrm{c}_{\text{s-1},0},\mathrm{c}_{\text{s-1},1},\ldots,\mathrm{c}_{\text{s-1,d-1}}\right)$$

$$= \begin{pmatrix} \theta^{\text{d+Jn}}\ (\mathrm{c}_{\text{s-1},0}), \theta^{\text{d+Jn}}\ (\mathrm{c}_{\text{s-1},1}),\ldots,\theta^{\text{d+Jn}}\ (\mathrm{c}_{\text{s-1,d-1}}),\theta^{\text{d+Jn}}\ (\mathrm{c}_{0,0}),\ldots \\ , \theta^{\text{d+Jn}}\ (\mathrm{c}_{0,\text{d-1}}),\ldots,\theta^{\text{d+Jn}}\ (\mathrm{c}_{\text{s-2},0}),\theta^{\text{d+Jn}}\ (\mathrm{c}_{\text{s-2},1}),\ldots,\theta^{\text{d+Jn}}\ (\mathrm{c}_{\text{s-2,d-1}}) \end{pmatrix}$$

$\theta^{\text{d+Jn}}(a) = \theta^{2\alpha_1}(a) = a$ for any $a \in R$. This implies that

$$\theta^{d+Jn}\left(\mathrm{c}_{0,0},\mathrm{c}_{0,1},\ldots,\mathrm{c}_{0,\text{d-1}},\mathrm{c}_{1,0},\mathrm{c}_{1,1},\ldots,\mathrm{c}_{1,\text{d-1}},\ldots,\mathrm{c}_{\text{s-1},0},\mathrm{c}_{\text{s-1},1},\ldots,\mathrm{c}_{\text{s-1,d-1}}\right)$$

$$= \left(\mathrm{c}_{\text{s-1},0},\mathrm{c}_{\text{s-1},1},\ldots,\mathrm{c}_{\text{s-1,d-1}},\mathrm{c}_{0,0},\ldots,\mathrm{c}_{0,\text{d-1}},\ldots,\mathrm{c}_{\text{s-2},0},\mathrm{c}_{\text{s-2},1},\ldots,\mathrm{c}_{\text{s-2,d-1}}\right) \in C$$

Therefore, C is equivalent to a QC code of length n and index d. □

3. Conclusion

In this paper, we investigated the structure of skew cyclic codes of an arbitrary length n, where the generator polynomial of a skew cyclic code comes from the non-commutative ring $R[x,\theta]$ where θ is an automorphism of R with $|\langle\theta\rangle| = 2$ We have shown that if $(2,n) = 1$ then the polynomial generated by $(x^n - 1)$ is not a two-sided ideal and hence the set $S_n = \frac{R[x,\theta]}{\langle x^n - 1\rangle}$ fails to be a ring. Under this condition skew cyclic codes can not be identified with ideals in S_n. Considering S_n as a left $R[x,\theta]$--module, we have shown that a skew cyclic code is either equivalent to a usual cyclic code (the case (m,n) = 1), or a quasi-cyclic code of index d (case (m,n) = d).

References

[1] Abualrub T., Ghrayeb A., Aidin N., Siap I., *On the construction of skew quasicyclic codes*, IEEE Trans. Inform. Theory, 2010; 56(5): 2081–2090.

[2] Blackford T., *Negacyclic codes over Z4 of even length*, IEEE Trans. Inform. Theory , 2006; 49(6):1417–1424.

[3] Bonnecaze A., Udaya P., *Cyclic codes and self-dual codes over F2 + uF2*, IEEE Trans. Inform. Theory, 1999; 45(4): 1250–1255.

[4] Boucher D., Geiselmann W., Ulmer F., *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput. 2007; 18(4): 379–389.

[5] Boucher D., Sole P., Ulmer F., *Skew constacyclic codes over Galois rings*, Adv. Math. Commun. 2008; 2(3): 273–292.

[6] Boucher D., F. Ulmer F., *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] Calderbank A.R., Sloane N.J.A., *Modular and p-adic cyclic codes*, Des. Codes Cryptogr. ,1995; 6(1): 21–35.

[8] Cayrel P.-L, Chabot C., Necer A., *Quasi-cyclic codes as codes over rings of matrices*, Finite Fields Appl.2010; 16(2): 100–115.

[9] Dastbasteh R., Mousavi H., Abualrub A., Aydin N., Haghighat J., *Skew cyclic codes over Fp + uFp*, International J. Information and Coding Theory, 2018, To Appear.

[10] Dougherty S.T., Park Y.H., *On modular cyclic codes*, Finite Fields Appl., 2007; 13 (1): 31–57.

[11] Gao J., *Skew cyclic codes over Fp + vFp*, J. Appl. Math. Inform., 2013; 31(3-4): 337–342.

[12] Jin L., *Skew cyclic codes over ring Fp + vFp*, J. Electronics (China), 2014; 31(3): 228–231.

[13] Mandelbaum D., *An application of cyclic coding to message identification*, IEEE Transactions on Communication Technology, 1969; 17(1): 42–48.

[14] Kanwar P., Lopez-Permouth S.R., *Cyclic codes over the integers modulo pm*, Finite Fields Appl., 1997; 3(4): 334–352.

[15] Pless V.S., Qian Z.*, Cyclic codes and quadratic residue codes over Z4*, IEEE Trans. Inform. Theory, 1996; 42(5): 1594–1600.

[16] Siap I., Abualrub T., Aydin N., Seneviratne P., *Skew cyclic codes of arbitrary length*, Int. J. Inf. Coding Theory, 2011; 2(1): 10–20.

[17] Tokiwa K., Kasahara M., Namekawa T., *Burst-error-correction capability of cyclic codes*, Electron. Comm. Japan, 1983; 66 (11): 60–66.

[18] Wolfmann J.*, Binary images of cyclic codes over Z4*, IEEE Trans. Inform. Theory, 2001; 47(5): 1773–1779.