*J. Appl. Math. & Informatics Vol.* **31***(2013), No. 3 - 4, pp. 337 - 342*
Website: http://www.kcam.biz

# SKEW CYCLIC CODES OVER $F_p + vF_p$[†]

JIAN GAO

Abstract. In this paper, we study a special class of linear codes, called skew cyclic codes, over the ring $R = F_p + vF_p$, where $p$ is a prime number and $v^2 = v$. We investigate the structural properties of skew polynomial ring $R[x, \theta]$ and the set $R[x, \theta]/(x^n - 1)$. Our results show that these codes are equivalent to either cyclic codes or quasi-cyclic codes. Based on this fact, we give the enumeration of distinct skew cyclic codes over $R$.

AMS Mathematics Subject Classification : 94B05, 94B15.
*Key words and phrases* : Skew polynomial rings, Skew cyclic codes, Quasi-cyclic codes, Enumeration.

## 1. Introduction

Cyclic codes have been investigated and studied by many researchers. These classes of codes are rich of algebraic structure. Based on this fact, cyclic codes have become one of the most important classes in coding theory.

Recently, there are some articles, which illustrate the coding theory using a non-commutative ring, skew polynomial ring[1, 2, 4, 6]. The principle motivation for studying codes in this setting is that polynomials in skew polynomial rings exhibit many factorizations and hence there are many ideals in a skew polynomial ring than in the commutative. The research on codes in this setting has resulted in the discovery of many new codes with better parameters. But all this work is restricted to the condition that the order of the automorphism must be a factor of the length of the code. It is a big impact on the structure of the set $R[x, \theta]/(x^n - 1)$. In [3], I. Siap, etc., removed this condition and they have studied the structural properties of skew cyclic codes of arbitrary length over finite fields.

Received June 14, 2012. Revised Sepetember 10, 2012. Accepted October 10, 2012.

[†]This work was supported by the research grant of National Natural Science Foundation of China (Grant No. 10971160) and Natural Science Foundation of Shandong provence (Grant No. ZR2011AQ004)

In this paper, we are interested in studying skew cyclic codes of arbitrary length over the ring $R = F_p + vF_p$, where $p$ is a prime number and $v^2 = v$. We define an automorphism of $R$. And we will show that the set $R_n = R[x, \theta]/(x^n - 1)$ fails to be a ring anymore unless $|\langle\theta\rangle||n$. But the set $R_n$ is always a left $R[x, \theta]$-submodule. Similar to [3], our results show that skew cyclic code is equivalent to a cyclic or quasi-cyclic code over $R$. And we give the enumeration of distinct skew cyclic codes over $R$.

## 2. Skew polynomial ring

Let $R = F_p + vF_p$, where $p$ is a prime number and $v^2 = v$. The Chinese Remainder Theorem tells us that $R = \langle v-1\rangle \oplus \langle v\rangle$, namely, there exist $c$, $d \in F_p$ such that $a + bv = cv + d(v - 1)$, for all $a$, $b \in F_p$. Define a ring automorphism as follows

$$\theta : R \to R$$

where $\theta(cv+d(v-1)) = c(v-1)+dv$. One can verify that $\theta$ is an automorphism and $\theta^2(e) = e$, for all $e$ in $R$. This implies that $\theta$ is an automorphism with order 2.

For a given automorphism $\theta$ of $R$, the set $R[x, \theta] = \{a_0 + a_1x + \ldots + a_nx^n|a_0 \in R, n \in N_0\}$ of formal polynomials forms a ring under usual addition of polynomial and where multiplication is defined using the rule $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$. The ring $R[x, \theta]$ is called skew polynomial ring over $R$. It is easily seen that the ring $R[x, \theta]$ is non-commutative unless $\theta$ is the identity automorphism on $R$.

**Theorem 2.1.** *The center $Z(R[x, \theta])$ of $R[x, \theta]$ is $F_p[x^2]$.*

*Proof.* The subring of the elements of $R$ that are fixed by $\theta$ is $F_p$. Since 2 is the order of automorphism $\theta$, for any $a \in R$, we have $x^{2i}a = (\theta^2)^i(a)x^{2i} = ax^{2i}$. Therefore, $x^{2i}$ is in the center $Z(R[x, \theta])$ of $R[x, \theta]$. This implies that $f = \varepsilon_0 + \varepsilon_1x^2 + \varepsilon_2x^4 + \ldots + \varepsilon_sx^{2s}$ with $\varepsilon_i \in F_p$ is a center element. Conversely, for any $f \in Z(R[x, \theta])$ and $a \in R$, if $xf = fx$ and $af = fa$, then $f \in F_p[x^2]$. □

**Corollary 2.2.** *$x^n - 1$ is in $Z(R[x, \theta])$ if and only if $n$ is even.*

*Proof.* Suppose $n$ is even, i.e. , $2|n$. Let $f(x) \in R[x, \theta]$ and $f(x) = a_0 + a_1x + \ldots + a_mx^m$. Since $n$ is even, $\theta^n(a) = a$ for any element $a$ in $R$. Hence, $(x^n-1)f(x) = (x^n-1)(a_0+a_1x+\ldots+a_mx^m) = x^na_0+x^na_1x+\ldots+x^na_mx^m - f(x) = \theta^n(a_0)x^n + \theta^n(a_1)x^nx + \ldots + \theta^n(a_m)x^nx^m - f(x) = (a_0 + a_1x + \ldots + a_mx^m)x^n - f(x) = f(x)(x^n - 1)$. Hence, $(x^n - 1) \in Z(R[x, \theta])$. Conversely, let $x^n - 1$ be in $Z(R[x, \theta])$. Then $x^n - 1$ commutes with every element in $R[x, \theta]$. Particularly, $(x^n - 1)a_mx^m = a_mx^m(x^n - 1)$ for some $a_m \in R$. Since $(x^n - 1)a_mx^m = \theta^n(a_m)x^{n+m} - a_mx^m$ and $a_mx^m(x^n - 1) = a_mx^{n+m} - a_mx^m$, $\theta^n(a_m) = a_m$. Thus $n$ is even. □

Note that the ring $R[x, \theta]$ is no longer left or right Euclidean, but left or right division can be defined for some elements.

**Lemma 2.3.** *Let $f, g \in R[x,\theta]$ such that the leading coefficient of $g$ is a unit. Then there exist unique $q, r \in R[x,\theta]$ such that*

$$f = qg + r,\ r = 0 \text{ or } \deg(r) < \deg(g)$$

*Proof.* Let $f = \sum_{i=0}^{m} a_i x^i$ and $g = \sum_{j=o}^{k} b_j x^j$, and $b_k$ is a unit, then the degree of

$$f - \frac{a_m}{\theta^{m-k}(b_k)} x^{m-k} g$$

is less than that of $f$. Iterating the procedure and subsequent such polynomials, we can obtain $q$ and $r$ as defined in Theorem 2.3. Next we will prove $q$ and $r$ are unique. Suppose

$$f = q_1 g + r_1 = q_2 g + r_2,$$

then

$$(q_1 - q_2)g = r_2 - r_1.$$

If $q_1 - q_2$ is not zero, then the right polynomial is of degree at least the degree of $g$, while the right polynomial is of degree at most one less than the degree of $g$. Therefore $q_1 = q_2$ and $r_1 = r_2$. □

## 3. Skew cyclic codes

Let $\theta$ be an automorphism of $R$. Let $n$ be an positive integer. A linear code $\mathcal{C}$ of length $n$ is called skew cyclic code or more precisely $\theta$-cyclic code if

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Rightarrow (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in \mathcal{C}$$

Define a map as follows

$$\rho : R^n \to R[x,\theta]/(x^n - 1)$$

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$$

One can verify that $\rho$ is an $R$-module isomorphism map.

**Case 1 $n$ is even**

Let $n$ be even. Then from Corollary 2.2, $x^n - 1$ is commutative. This implies that $R_n = R[x,\theta]/(x^n - 1)$ is a ring.

**Theorem 3.1.** *Let $n$ be even and $\mathcal{C}$ be a skew cyclic code with length $n$. Then $\mathcal{C}$ is a left ideal in $R_n$.*

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

**Theorem 3.2.** *Let $n$ be even and $\mathcal{C}$ be a skew cyclic code with length $n$ and $f(x)$ be a polynomial in $\mathcal{C}$ with minimal degree. If the leading coefficient of $f(x)$ is a unit in $R$, then $\mathcal{C} = \langle f(x) \rangle$, where $f(x)$ is a right divisor of $x^n - 1$.*

*Proof.* Let $f(x)$ be a polynomial of minimal degree in $\mathcal{C}$. By Lemma 2.3, there are two unique polynomials $q$ and $r$ such that

$$x^n - 1 = qf + r$$

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 $x^n - 1$. □

Let $T$ be a cyclic operate over $R$, i.e., for $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$, $T(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$. Let $\mathcal{C}$ be a linear code of length $n$ over $R$. Then $\mathcal{C}$ is called quasi-cyclic code with index $l$ if and only if $\mathcal{C}$ is invariant under $T^l$, where $l$ is the minimal positive integer satisfies $T^l(\mathcal{C}) = \mathcal{C}$.

**Theorem 3.3.** *Let $n$ be even and $\mathcal{C}$ be a skew cyclic code of length $n$.Then $\mathcal{C}$ is equivalent to a quasi-cyclic code of length $n$ with index 2.*

*Proof.* Let $n = 2N$, $c = (c_{0,0}, c_{0,1}, c_{1,0}, c_{1,1}, \ldots, c_{N-1,0}, c_{N-1,1}) \in \mathcal{C}$. Since $\theta^2(c) \in \mathcal{C}$ and $\theta^2 = 1$, it follows that $\theta^2(c) = (c_{N-1,0}, c_{N-1,1}, c_{0,0}, c_{0,1}, \ldots, c_{N-2,0}, c_{N-2,1}) \in \mathcal{C}$. Therefore from the definition of quasi-cyclic code above, $\mathcal{C}$ is equivalent to a quasi-cyclic code of length $n$ with index 2. □

As in the case of finite fields, it is easy to see that $\mathcal{C}$ is a quasi-cyclic code of length $n$ with index 2 over $R$ if and only if $\mathcal{C}$ is an $R[x]/(x^N - 1)$-submodule of $(R[x]/(x^N - 1))^2$, where $N = n/2$. Therefore from Theorem 3.3, we get the following corollary immediately.

**Corollary 3.4.** *Let $n$ be even. Then the number of distinct skew cyclic codes of length $n$ over $R$ is equal to the number of $R[x]/(x^N - 1)$-submodule of $(R[x]/(x^N - 1))^2$, where $N = n/2$.*

**Case 2 $n$ is odd**

Let $n$ be odd. Then $|\langle\theta\rangle| \nmid n$. This implies that $x^n - 1$ is non-commutative. Therefore the set $R_n = R[x, \theta]/(x^n - 1)$ is not a ring anymore. Define the addition on $R_n$ as usual and multiplication from left as $r(x)(g(x) + (x^n - 1)) = r(x)g(x) + (x^n - 1)$ for any $r(x) \in R[x, \theta]$. We can prove that $R_n$ is a left $R[x, \theta]$-module where multiplication is defined as above.

**Theorem 3.5.** *Let $n$ be odd. Then $\mathcal{C}$ is a skew cyclic code of length $n$ over $R$ if and only if $\mathcal{C}$ is a left $R[x, \theta]$-submodule of $R_n$.*

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

**Theorem 3.6.** *Let $n$ be odd and $\mathcal{C}$ be a skew cyclic code with length $n$ and $f(x)$ be a polynomial in $\mathcal{C}$ with minimal degree. If the leading coefficient of $f(x)$ is a unit in $R$, then $\mathcal{C} = \langle f(x)\rangle$, where $f(x)$ is a right divisor of $x^n - 1$.*

*Proof.* Similar to Theorem 3.2. □

**Theorem 3.7.** *Let $n$ be odd and $\mathcal{C}$ be a skew cyclic code of length $n$. Then $\mathcal{C}$ is equivalent to a cyclic code of length $n$ over $R$.*

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

It is well known that for any linear code $\mathcal{C}$ of length $n$, $\mathcal{C} = (v-1)\mathcal{C}_1 \oplus v\mathcal{C}_2$, where $C_1$ and $C_2$ are linear codes of length $n$ over $F_p$ [5]. Then from Theorem 3.7, we have the following corollary immediately.

**Corollary 3.8.** *Let $n$ be odd. Then the number of distinct skew cyclic codes of length $n$ over $R$ is equal to the number of ideals in $R[x]/(x^n - 1)$. If $x^n - 1 = \prod_{i=1}^{s} p_i^{r_i}(x)$, where $p_i(x)$ are irreducible polynomials over $F_p$, then there are $\prod_{i=1}^{s}(r_i + 1)^2$ distinct skew cyclic codes actually.*

## 4. Examples

**Example 4.1.** Let $R = F_2 + vF_2$, $n = 8$ and $f(x) = x^4 + vx^3 + x^2 + (v+1)x + 1$. Then $f(x)$ generates a skew cyclic code of length 8. And this code equivalent to a quasi-cyclic code of length 8 with index 2.

**Example 4.2.** Let $R = F_2 + vF_2$, $n = 7$ and $f(x) = 1 + x^2 + x^3$. Then $f(x)$ generates a skew cyclic code of length 7. This code is equivalent to a cyclic code of length 7. Since $x^7 - 1 = (x+1)(1+x+x^3)(1+x^2+x^3)$, it follows that there are $2^{2\times 3} = 64$ skew cyclic codes of length 7.

**Example 4.3.** Let $R = F_3 + vF_3$, $n = 3$. Take $f(x) = x^2 + x + 1$. Then $f(x)$ generates a skew cyclic code of length 3. This code is equivalent to a cyclic code of length 3 over $R$. Since $x^3 - 1 = (x+2)^3$, it follows that there are $(3+1)^2 = 16$ distinct skew cyclic codes over $R$.

## 5. Conclusion

In this paper, we mainly investigate the structural properties of skew cyclic codes over $F_p + vF_p$. Our results show that if $n$ is even then skew cyclic code is equivalent to a quasi-cyclic code with index 2 and if $n$ is odd then skew cyclic code is equivalent to a cyclic code. Based on this fact, we discuss the enumeration of distinct skew cyclic codes. But unfortunately, for the case $n$ is even , we have not given the explicit enumeration because of the complex work to compute the number of $R[x]/(x^N - 1)$-submodule of $(R[x]/(x^N - 1))^2$. And this will be worthy of further consideration.

## References

1. D. Boucher and F. Ulmer, *Coding with skew polynoial rings*, J. Symb. Comput **44** (2009),1644-1656.
2. D. Boucher, W. Geiselmann and F. Ulmer, *Skew cyclic codes*, Appl. Algebra Eng. Commun. Comput **18** (2007), 379-389.
3. I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, *Skew cyclic codes of arbitrary length*, Inf. Coding Theory **2** (2011), 10-20.
4. M. Bhaintwal,*Skew quasi-cyclic codes over Galois rings*, Des. Codes Cryptogr (2011), DOI 10.1007/s10623-011-9494-0.
5. S. Zhu and Y. Wang, *A class of constacyclic codes over $F_p + vF_p$ and its Gray image*, Discrete. Math **311** (2011), 2677-2682.
6. T. Abualrub, A. Ghrayeb, N. Aydim and I. Siap, *On the construction of skew quasi-cyclic codes*, IEEE. Trans. Inform. Theory **56**(2010), 2081-2090.

**Jian Gao** received M.Sc. at Shandong University of Technology. And now he is a doctoral student in Chern Institute of Mathematics. His research interests include coding theory and Lattices and codes.

School of Sciense, Shandong University of Technology, Zibo, Shandong, 255091, P. R. China.
e-mail: dezhougaojian@163.com