

# Skew Cyclic Codes over $F_q + uF_q + \dots + u^{k-1}F_q$

Jing Li, Xiuli Li

**Abstract**—This paper studies a special class of linear codes, called skew cyclic codes, over the ring  $R = F_q + uF_q + \dots + u^{k-1}F_q$ , where  $q$  is a prime power. A Gray map  $\phi$  from  $R$  to  $F_q$  and a Gray map  $\phi'$  from  $R^n$  to  $F_q^n$  are defined, as well as an automorphism  $\Theta$  over  $R$ . It is proved that the images of skew cyclic codes over  $R$  under map  $\phi'$  and  $\Theta$  are cyclic codes over  $F_q$ , and they still keep the dual relation.

**Keywords**—Skew cyclic code, gray map, automorphism, cyclic code.

## I. INTRODUCTION

IN recent years, the study of coding theory on finite chain has attracted the attention of many scholars. Reference [1] shows cyclic codes of odd length and self-dual codes over ring  $F_2 + uF_2$ . The structure and weight of the cyclic code of arbitrary length over  $Z_2 + uZ_2$  and  $Z_2 + uZ_2 + u^2Z_2$  has been given in [2]. Reference [3] shows skew codes over  $F_4 + vF_4$  ( $v^2 = v$ ), and shows the relationship between the cyclic codes and the cyclic codes over the ring  $F_2 + vF_2$  and  $F_4$ , by defining the Gray map.

As a finite ring in more general sense, the research of the structure of cyclic codes, cyclic codes and quasi cyclic codes over the ring  $R = F_q + uF_q + \dots + u^{k-1}F_q$  has aroused the interest of many people. Reference [4] provides the structure and ideal over the ring  $F_q + uF_q + \dots + u^{k-1}F_q$  length  $p^s n$  where  $p, n$  are coprime, and obtains the direct sum and spectral representation (MS polynomial) of the cyclic codes over the ring by using the discrete Fourier transform and inverse isomorphism. According to [5], the structure and the number of codewords of all  $(u\lambda - 1)$ -cyclic codes with length  $p^e$  over finite chain ring  $F_q + uF_q + \dots + u^{k-1}F_q$  are generated by finite ring theory. Reference [6] studies the Gray image of constacyclic codes over finite chain rings; it is proved that the Gray image of arbitrary cyclic codes over finite chain rings is equivalent to quasi cyclic codes over finite fields. Reference [7] shows quasi cyclic codes over the ring  $F_p + uF_p + \dots + u^{k-1}F_p$ , and establishes the relation between cyclic codes over  $F_p + uF_p + \dots + u^{k-1}F_p$  and quasi cyclic codes over  $F_p$ . By using the torsion codes of arbitrary  $(1 + \lambda u)$ -length constacyclic codes over  $R = F_{p^m}[u]/\langle u^k \rangle$ , the bound of homogeneous distance

of these constacyclic codes is obtained in [8], and a new Gray map is defined to establish the relation between the constacyclic codes over  $R$  and the linear codes over  $F_{p^m}$ , then some optimal linear codes are constructed.

This paper will study the properties of skew cyclic codes over  $R = F_q + uF_q + \dots + u^{k-1}F_q$  where  $q$  is prime power.

## II. LARGE BASIC KNOWLEDGE

$R = F_q + uF_q + \dots + u^{k-1}F_q$  is a finite ring where  $q = p^m$ ,  $p$  is arbitrary prime, and  $m$  is positive integer. Any element  $c$  in the ring  $R$  can be represented uniquely by  $c = r_0(c) + ur_1(c) + \dots + u^{k-1}r_{k-1}(c)$  where  $r_i(c) \in F_q$ ,  $0 \leq i \leq k-1$ .

A subset  $C$  of the ring  $R$  is called a code over  $R$ , in which the element is called a codeword. And a linear cyclic code length  $n$  over  $R$  can be considered as a  $R$ -submodule of  $R^n$ .

There are two forms to express these elements in  $C$  the first one is  $c = (c_0, c_1, \dots, c_{n-1}) \in C$  in vector form, another one is  $f(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in C$  in functional form.

Define the new Grey map  $\phi$  as follows:

$$\phi: R \rightarrow F_q^k$$

$$\phi(r_0 + ur_1 + \dots + u^{k-1}r_{k-1}) = (r_0, r_0 + r_1, r_0 + r_1 + r_2, \dots, r_0 + r_1 + \dots + r_{k-1})$$

Thus, there is another Grey map  $\phi'$  which is derived as:

$$\phi': R^n \rightarrow F_q^{kn}$$

$$\begin{aligned} \phi'(c_0, c_1, \dots, c_{n-1}) &= (\phi(c_0), \phi(c_1), \dots, \phi(c_{n-1})) \\ &= (r_{0,0}, r_{0,0} + r_{1,0}, r_{0,0} + r_{1,0} + r_{2,0}, \dots, r_{0,0} + r_{1,0} + \dots + r_{k-1,0}, \\ &\quad r_{0,1}, r_{0,1} + r_{1,1}, r_{0,1} + r_{1,1} + r_{2,1}, \dots, r_{0,1} + r_{1,1} + \dots + r_{k-1,1}, \\ &\quad \dots, \\ &\quad r_{0,n-1}, r_{0,n-1} + r_{1,n-1}, r_{0,n-1} + r_{1,n-1} + r_{2,n-1}, \dots, r_{0,n-1} + r_{1,n-1} + \dots + r_{k-1,n-1}) \end{aligned}$$

The Hamming weight of codeword  $c = (c_0, c_1, \dots, c_{n-1})$  in

$R$  is defined as  $w_H(c) = \sum_{i=0}^{n-1} w_H(c_i)$ , where

$$w_H(c_i) = \begin{cases} 1, & c_i \neq 0 \\ 0, & c_i = 0 \end{cases}, \quad 0 \leq i \leq n-1.$$

The Hamming distance of code  $C$  is defined as

Jing Li is with the School of Mathematics and Physics, Qingdao University of Science and Technology, Qingdao, China (corresponding author, phone: 18765279986; e-mail: 672092400@qq.com).

Xiuli Li is with Qingdao University of Science and Technology, Qingdao, China (e-mail: lixiuli2004@tom.com).

$$d_H(C) = \min d_H(c, c'),$$

where  $\forall c, c' \in C, c \neq c', d_H(c, c') = w_H(c - c')$ .

We define the Lee weight of codeword  $c = (c_0, c_1, \dots, c_{n-1})$  in  $R$  as  $w_L(c) = \sum_{i=0}^{n-1} w_H(\phi(c_i))$ , where  $w_H(\phi(c_i))$  is Hamming weight of  $\phi(c_i)$ . We also define the Lee distance between  $c$  and  $c'$  as  $d_L(C) = \min d_L(c, c')$ , where  $\forall c, c' \in C, c \neq c', d_L(c, c') = w_L(c - c')$ .

Obviously, the Gray map  $\phi'$  is an isometric mapping from  $R^n$  (Lee distance) to  $F_q^{kn}$  (Hamming distance).

**Theorem 1.** If  $C$  is  $[n, M]$  linear code over  $R$  and  $d_L(C) = d$ , then  $\phi'(C)$  is  $[nk, M]$  linear code over  $F_q$  and  $d_H(\phi'(C)) = d$ .

**Proof.**  $d_L(C) = d_H(\phi'(C))$  is known. It can be seen easily that the length of  $\phi'(C)$  is  $nk$ . Next, it needs to prove that  $\phi'$  keeps linear operation.

Let  $c = (c_0, c_1, \dots, c_{n-1})$ ,  $e = (e_0, e_1, \dots, e_{n-1}) \in R^n$ , when  $0 \leq i < n-1$ , there are

$$c_i = r_0(c_i) + ur_1(c_i) + \dots + u^{k-1}r_{k-1}(c_i)$$

$$e_i = r_0(e_i) + ur_1(e_i) + \dots + u^{k-1}r_{k-1}(e_i)$$

Thus,

$$\begin{aligned} \phi'(c+e) &= (\phi'(c_0+e_0), \phi'(c_1+e_1), \dots, \phi'(c_{n-1}+e_{n-1})) \\ &= (r_0(c_0+e_0), r_0(c_0+e_0)+r_1(c_0+e_0), \dots, \\ &\quad r_0(c_0+e_0)+r_1(c_0+e_0)+\dots+r_{k-1}(c_0+e_0), \dots, \\ &\quad r_0(c_{n-1}+e_{n-1}), r_0(c_{n-1}+e_{n-1})+r_1(c_{n-1}+e_{n-1}), \dots, \\ &\quad r_0(c_{n-1}+e_{n-1})+r_1(c_{n-1}+e_{n-1})+\dots+r_{k-1}(c_{n-1}+e_{n-1})) \\ &= (r_0(c_0), r_0(c_0)+r_1(c_0), \dots, r_0(c_0)+r_1(c_0)+\dots+r_k(c_0), \dots, \\ &\quad r_0(c_{n-1}), r_0(c_{n-1})+r_1(c_{n-1}), \dots, r_0(c_{n-1})+r_1(c_{n-1})+\dots+r_k(c_{n-1})) \\ &\quad + (r_0(e_0), r_0(e_0)+r_1(e_0), \dots, r_0(e_0)+r_1(e_0)+\dots+r_k(e_0), \dots, \\ &\quad r_0(e_{n-1}), r_0(e_{n-1})+r_1(e_{n-1}), \dots, r_0(e_{n-1})+r_1(e_{n-1})+\dots+r_k(e_{n-1})) \\ &= \phi'(c_0, c_1, \dots, c_{n-1}) + \phi'(e_0, e_1, \dots, e_{n-1}) \\ &= \phi'(c) + \phi'(e) \end{aligned}$$

If  $\lambda \in F_q, c \in R$ , then

$$\phi'(\lambda c) = \phi'(\lambda c_0, \lambda c_1, \dots, \lambda c_{n-1}) = \lambda \phi'(c_0, c_1, \dots, c_{n-1}) = \lambda \phi'(c)$$

So,  $\phi'$  keeps linear operation and  $\phi'$  is a bijection. Thus, the number of codewords in  $C$  and  $\phi'(C)$  is the same. This

gives the proof.

Now, define a ring automorphism  $\theta$  as follows

$$\begin{aligned} \theta(c) &= \theta(r_0 + ur_1 + \dots + u^{k-1}r_{k-1}) \\ &= r_0 + u^{k-1}r_1 + u^{k-2}r_2 + \dots + u^2r_{k-2} + ur_{k-1} \end{aligned}$$

for all  $c = r_0(c) + ur_1(c) + \dots + u^{k-1}r_{k-1}(c)$  in  $R$ . One can verify that  $\theta$  is an automorphism and  $\theta^2(a) = a$  for any  $a \in R$ . This implies that  $\theta$  is an automorphism with order 2.

A ring like

$$R[x, \theta] = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} : a_i \in R, 0 \leq i \leq n-1, n \in \mathbb{N}\}$$

is called skew polynomial ring. For a given automorphism  $\theta$  of  $R$ , the set  $R[x, \theta]$  of formal polynomials forms a ring under usual addition of polynomial and where multiplication is defined using the rule  $(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}$ .

Let  $f(x) = \sum_{i=0}^s f_i x^i$ ,  $g(x) = \sum_{i=0}^t g_i x^i$ , where  $f_i$  and  $g_i$  are units of  $R$ , then there exist unique polynomials  $u(x)$  and  $v(x)$  of  $R[x, \theta]$  which make  $g(x) = u(x) * f(x) + v(x)$  establish where  $v(x) = 0$  or  $\deg(v(x)) < \deg(f(x))$ . When  $v(x) = 0$ ,  $f(x)$  is called the right divisor of  $g(x)$ ; that is,  $f(x)$  right divides  $g(x)$  exactly.

Let  $R_n = R[x, \theta] / (x^n - 1)$ , define multiplication from left as

$$r(x) * (f(x) + (x^n - 1)) = r(x) * f(x) + (x^n - 1),$$

where  $f(x) + (x^n - 1)$  is element of  $R_n$ , and  $r(x) \in R[x, \theta]$ .

For any  $x = (x_1, x_2, \dots, x_n)$ ,  $y = (y_1, y_2, \dots, y_n)$  in  $R^n$ , the inner product is defined as  $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ . Let  $C$  be linear code over  $R$ , the dual code of  $C$  is  $C^\perp = \{x \in R^n \mid \langle x, c \rangle = 0, \forall c \in C\}$ . A code  $C$  is called self-dual code if  $C = C^\perp$ .

**Definition 1.** A subset  $C$  of  $R^n$  is called a quasi-cyclic code of length  $N$  ( $N = ns$ ) if  $C$  satisfies the following conditions:

- (1)  $C$  is a  $R$ -submodule of  $R^n$ ;
- (2) If

$$c = (c_{0,0}, c_{0,1}, \dots, c_{0,n-1}, c_{1,0}, c_{1,1}, \dots, c_{1,n-1}, \dots, c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,n-1}) \in C,$$

then

$$\varphi_n(c) = (c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,n-1}, |c_{0,0}, c_{0,1}, \dots, c_{0,n-1}|, \dots, |c_{s-2,0}, c_{s-2,1}, \dots, c_{s-2,n-1}|) \in C$$

Particularly,  $C$  is cyclic code when  $n=1$ .

**Definition 2.** 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  $R^n$ -submodule of  $R^n$ ;
- (2) If  $c = (c_0, c_1, \dots, c_{n-1}) \in C$ , then

$$\varphi_\theta(c) = (\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C.$$

### III. CONSTRUCTION

**Theorem 1.** The center of  $R[x, \theta]$  is  $F_q[x^2]$ .

**Proof.** The subring of the elements of  $R$  that are fixed by  $\theta$  is  $F_q$ . Since  $\theta$  is an automorphism with order 2, for any  $a \in R$ , there is  $(x^{2i})^* a = \theta^{2i}(a) x^{2i} = (\theta^2)^i(a) x^{2i} = a x^{2i}$ . Thus  $x^{2i}$  is in the center of  $R[x, \theta]$ . This implies that any  $f(x) = \varepsilon_0 + \varepsilon_1 x^2 + \varepsilon_2 x^4 + \dots + \varepsilon_s x^{2s}$  is a center element with  $\varepsilon_i \in F_q$ ,  $0 \leq i \leq s$ .

Conversely, let  $Z(R[x, \theta])$  be the center of  $R$ , so  $f(x) * a = a * f(x)$  for any  $f(x) \in Z(R[x, \theta])$  and any  $a \in R$ . Since  $f(x) = \varepsilon_0 + \varepsilon_1 x + \varepsilon_2 x^2 + \dots + \varepsilon_n x^n$  for  $\varepsilon_i \in F_q$ ,  $0 \leq i \leq n$ , there are

$$\begin{aligned} f(x) * a &= a * f(x), \\ (\varepsilon_0 + \varepsilon_1 x + \varepsilon_2 x^2 + \dots + \varepsilon_n x^n) * a &= a * (\varepsilon_0 + \varepsilon_1 x + \varepsilon_2 x^2 + \dots + \varepsilon_n x^n), \\ a \varepsilon_0 + \varepsilon_1 \theta(a) x + \varepsilon_2 \theta^2(a) x^2 + \dots + \varepsilon_n \theta^n(a) x^n &= a \varepsilon_0 + a \varepsilon_1 x + a \varepsilon_2 x^2 + \dots + a \varepsilon_n x^n. \end{aligned}$$

It is known that  $|\langle \theta \rangle| = 2$ , so there are  $\varepsilon_i x^i * a = a \varepsilon_i x^i$  when  $i$  is even, and  $\varepsilon_i x^i * a \neq a \varepsilon_i x^i$  when  $i$  is odd. Hence, any  $f(x) = \varepsilon_0 + \varepsilon_1 x + \varepsilon_2 x^2 + \dots + \varepsilon_n x^n$  of  $Z(R[x, \theta])$  only exists even power term of  $x$ , that is  $f(x) = \varepsilon_0 + \varepsilon_2 x^2 + \varepsilon_4 x^4 + \dots + \varepsilon_{2s} x^{2s}$ . Thus, any element of center is in  $F_q[x^2]$ . This gives the proof.

**Theorem 2.** Let  $R_n = R[x, \theta] / (x^n - 1)$ , a code  $C$  in  $R_n$  is a skew cyclic code if and only if  $C$  is a left  $R[x, \theta]$ -submodule of the left  $R[x, \theta]$  module  $R_n$ .

**Proof.** Suppose  $C$  is  $\theta$ -cyclic code, so  $(\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$  for  $c = (c_0, c_1, \dots, c_{n-1}) \in C$ , that is for any  $f(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \in C$ , there is  $x * f(x) \in C$ . Next,  $g(x) * f(x) \in C$  for any  $g(x) \in R[x, \theta]$

from linear property, then  $C$  is a left  $R[x, \theta]$ -submodule of the left  $R[x, \theta]$  module  $R_n$ .

Now suppose that  $C$  is a left  $R[x, \theta]$ -submodule of the left  $R[x, \theta]$  module  $R_n$ , so

$$x * f(x) = (\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$$

for any  $f(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \in C$ , this implies that

$$(\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$$

for any  $c = (c_0, c_1, \dots, c_{n-1}) \in C$ . Thus,  $C$  is  $\theta$ -cyclic code. This gives the proof.

**Theorem 3.** Let  $C$  be a  $\theta$ -cyclic code in  $R_n = R[x, \theta] / (x^n - 1)$  and let  $f(x)$  be a polynomial in  $C$  of minimal degree. If  $f(x)$  is monic polynomial, then  $C = \langle f(x) \rangle$  where  $f(x)$  is a right divisor of  $x^n - 1$ .

**Proof.** Suppose  $g(x) = u(x) * f(x) + v(x)$  for any  $g(x) \in C$  where  $v(x) = 0$  or  $\deg(v(x)) < \deg(f(x))$ . Since  $f(x) \in C$ , then  $v(x) = g(x) - u(x) * f(x) \in C$ . Also since  $f(x)$  is polynomial in  $C$  of minimal degree, we have  $v(x) = 0$ , this implies that  $C = \langle f(x) \rangle$ .

Since the  $\theta$ -cyclic codes over  $R_n$  and its left  $R[x, \theta]$ -submodule are corresponding one by one, thus  $f(x)$  is a right divisor of  $x^n - 1$ . This gives the proof.

**Theorem 4.** Let  $n$  be even. If codes  $C$  over  $R$  are  $\theta$ -cyclic codes, so is its dual codes  $C^\perp$ .

**Proof.** Let  $c = (c_0, c_1, \dots, c_{n-1}) \in C^\perp$ ,  $a = (a_0, a_1, \dots, a_{n-1}) \in C$ , so  $\langle c, a \rangle = 0$  for any  $c$  and  $a$ . Since  $C$  is  $\theta$ -cyclic codes, then  $(\theta(a_{n-1}), \theta(a_0), \dots, \theta(a_{n-2})) \in C$ . Thus,

$$(\theta^{n-1}(a_1), \theta^{n-1}(a_2), \dots, \theta^{n-1}(a_0)) \in C.$$

Therefore,

$$\begin{aligned} c_0 \theta^{n-1}(a_1) + c_1 \theta^{n-1}(a_2) + \dots + c_{n-1} \theta^{n-1}(a_0) &= 0 \\ \theta(c_0) \theta^n(a_1) + \theta(c_1) \theta^n(a_2) + \dots + \theta(c_{n-1}) \theta^n(a_0) &= 0 \end{aligned}$$

It is known  $n$  is even, then have  $\theta^n(a_j) = a_j$  for  $a_j \in R$ .

Hence,

$$a_0 \theta(c_{n-1}) + a_1 \theta(c_0) + \dots + a_{n-1} \theta(c_{n-2}) = 0$$

by transforming formulas. Thus

$(\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C^\perp$  and  $C^\perp$  is  $\theta$ -cyclic codes.

This gives the proof.

**Theorem 5.** Let  $n$  be even, then the  $\theta$ -cyclic codes  $C$  generated by a monic right divisor  $g(x)$  over  $R$  are cyclic codes if and only if the coefficients of  $g(x)$  are elements of  $F_q$ .

**Proof.** Let  $g(x) = x^m + \sum_{i=0}^{m-1} g_i x^i$  where  $g_i \in F_q$ . So,  $\theta(g_i) = g_i$ ,  $x * g(x) = g(x) * x$  from definition of  $\theta$ , thus the  $\theta$ -cyclic codes  $C$  generated by a monic right divisor  $g(x)$  over  $R$  are cyclic codes.

Let the  $\theta$ -cyclic codes  $C$  generated by  $g(x)$  over  $R$  be cyclic codes, then  $x * g(x) \in C$ ,  $g(x) * x \in C$ . Hence,

$$\begin{aligned} u(x) &= x * g(x) - g(x) * x \\ &= (\theta(g_0) - g_0)x + (\theta(g_1) - g_1)x^2 + \dots + (\theta(g_{m-1}) - g_{m-1})x^m \in C \end{aligned}$$

Since  $g(x)$  is the right divisor of  $u(x)$ , there exists  $u(x) = t * g(x) = tx^m + tg_{m-1}x^{m-1} + \dots + tg_1x + g_0$  where  $t$  is a constant. Comparing two formulas of  $u(x)$ , then

$$\begin{aligned} \theta(g_{m-1}) - g_{m-1} &= t, \\ \theta(g_{m-2}) - g_{m-2} &= tg_{m-1}, \\ &\vdots \\ \theta(g_1) - g_1 &= tg_2, \\ \theta(g_0) - g_0 &= tg_1, \\ tg_0 &= 0. \end{aligned}$$

If  $t=0$ , then  $u(x)=0$ , this theorem is proved. If  $t \neq 0$ ,  $g_0=0$ , it shows that  $g_i=0$ ,  $1 \leq i \leq m-1$ , hence  $g(x)=x^m$ ,  $\theta(g_i)=g_i$ ,  $0 \leq i \leq m$ . Thus, the coefficients of  $g(x)$  are elements of  $F_q$ . This gives the proof.

**Theorem 6.** Let  $n$  be odd and  $C$  be a skew cyclic code of length  $n$  over  $R$ . Then,  $C$  is equivalent to cyclic code of length  $n$  over  $R$ .

**Proof.** Since  $n$  is odd,  $\gcd(2, n) = 1$ . Hence, there exist integers  $b, c$  such that  $2b + cn = 1$ . Thus,  $2b = 1 - cn = 1 + zn$  where  $z > 0$ .

Let  $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in C$ , we have

$$\begin{aligned} x^{2b} * a(x) &= \theta^{2b}(a_0)x^{1+zn} + \theta^{2b}(a_1)x^{2+zn} + \dots + \theta^{2b}(a_{n-1})x^{n+zn} \\ &= a_{n-1} + a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} \in C \end{aligned}$$

Thus,  $C$  is cyclic code of length  $n$  over  $R$ . This gives the proof.

**Corollary 1.** If  $C$  is a skew cyclic code of length  $n$  over  $R$ , then the Gray image  $\phi'(C)$  of  $C$  is equivalent to quasi-cyclic code of length  $nk$  over  $F_q$ .

**Proof.** Let  $(c_0, c_1, \dots, c_{n-1}) \in C$ , each element  $c$  in  $C$  can be expressed as  $c = r_0(c) + ur_1(c) + \dots + u^{k-1}r_{k-1}(c)$ . It is known that  $\varphi_\theta(c) = (\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$ , that is  $\varphi_\theta(C) = C$ . For  $\phi'$ ,  $\phi'(\varphi_\theta(C)) = \phi'(C)$ . From Theorem 1 in Section II,  $\phi'(C)$  is linear code over  $F_q$  and  $\phi'$  keeps linear operation, so

$$\begin{aligned} &\phi'(\varphi_\theta(c_0, c_1, \dots, c_{n-1})) \\ &= \phi'(\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \\ &= (\phi(r_{n-1,0} + u^{k-1}r_{n-1,1} + u^{k-2}r_{n-1,2} + \dots + ur_{n-1,k-1}), \\ &\quad \phi(r_{0,0} + u^{k-1}r_{0,1} + u^{k-2}r_{0,2} + \dots + ur_{0,k-1}), \dots, \\ &\quad \phi(r_{n-2,0} + u^{k-1}r_{n-2,1} + u^{k-2}r_{n-2,2} + \dots + ur_{n-2,k-1})) \\ &= (r_{n-1,0}, r_{n-1,0} + r_{n-1,1}, r_{n-1,0} + r_{n-1,1} + r_{n-1,2}, \dots, \\ &\quad r_{n-1,0} + r_{n-1,1} + r_{n-1,2} + \dots + r_{n-1,k-1} | r_{0,0}, r_{0,0} + r_{0,1}, r_{0,0} + r_{0,1} + r_{0,2}, \\ &\quad \dots, r_{0,0} + r_{0,1} + r_{0,2} + \dots + r_{0,k-1} | r_{n-2,0}, r_{n-2,0} + r_{n-2,1}, \\ &\quad r_{n-2,0} + r_{n-2,1} + r_{n-2,2}, \dots, r_{n-2,0} + r_{n-2,1} + r_{n-2,2} + \dots + r_{n-2,k-1}) \end{aligned}$$

Now, each section of right side of equation is a cyclic code of length  $nk$ . Thus,  $\phi'(C)$  is quasi-cyclic code of length  $nk$  over  $F_q$ . This gives the proof.

## REFERENCES

- [1] Bonnecaze A, Udaya P. Cyclic codes and self-dual codes over  $F_2 + uF_2$  (J). IEEE Trans Inform Theory, 1999, 45(4):1250-1255.
- [2] Abualr T, Siap T. Cyclic codes over the rings  $Z_2 + uZ_2$  and  $Z_2 + uZ_2 + u^2Z_2$  (J). Designs Codes and Cryptography, 2007, 42(3):273-287.
- [3] Xu Xian-qi, Zhu Shi-xin. Skew cyclic codes over the ring  $F_4 + vF_4$  (J). Journal of Hefei University of Technology, 2011, 34(9):1429-1432.
- [4] Han Mu, Ye You-pei, Zhu Shi-xin. Cyclic codes over  $F_p + uF_p + \dots + u^{k-1}F_p$  with length  $p^n$  (J). Information Sciences, 2011, 181(4):926-934.
- [5] Zhu Shi-xin, Li Ping, Wu Bo. A Class of Repeated-root Constacyclic Codes over the Ring  $F_q + uF_q + \dots + u^{k-1}F_q$  (J). Journal of Electronics & Information Technology, 2008, 30(6):1394-1396.
- [6] Qian Jian-fa, Ma Wen-ping. Constacyclic and cyclic codes over finite chain rings (J). Science Direct, 2009, 16(3):122-125.
- [7] Li Fu-lin, Zhu Shi-xin. Quasi-cyclic codes over  $F_p + uF_p + \dots + u^kF_p$  (J). Journal of Hefei University of Technology, 2009, 32(11):1766-1768.
- [8] Ding Jian, Li Hong-ju. Construction of optimal codes with Homogeneous distance (J). Journal of University of Science and Technology of China, 2015, 45(7): 588-593.