ORIGINAL PAPER

CYCLIC AND SKEW CYCLIC CODES OVER THE $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_k\mathbb{F}_q$

ABDULLAH DERTLI[1], YASEMIN CENGELLENMIS[2]

Manuscript received: 15.11.2015; Accepted paper: 10.03.2016;
Published online: 30.03.2016.

Abstract. *In this paper, we study the structure of cyclic and skew cyclic codes over the finite ring* $D_k = \mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_k\mathbb{F}_q$, $v_i^2 = v_i$, $v_iv_j = v_jv_i = 0$, $1 \leq i,j \leq k$, $q = p^m$, p *is a prime for* $k \geq 1$ *which contains the ring* $\mathbb{F}_q + v_1\mathbb{F}_q$, $v_1^2 = v_1$. *We define a new Gray map from* D_k *to* $\mathbb{F}_q^{k+1}$. *The algebraic structures of cyclic codes and duality properties are investigated. A linear code over* D_k *is represented by means of* $k+1$ q*-ary codes. The non trivial automorphism over* D_k *is given and the skew cyclic codes over* D_k *are introduced. The algebraic structure of skew cyclic codes and duality properties are investigated. The Gray images of both cyclic and skew cyclic codes over* D_k *are obtained.*

Keywords: *Cyclic code, skew cyclic code, finite ring.*

1. INTRODUCTION

As cyclic codes have got rich algebraic structure, they are very important class in coding theory. These classes of codes were first discussed by a series of papers and reports by E. Prange in [17] and [18].

Skew cyclic codes are generalization of the notion of cyclic codes. The class of skew cyclic codes are bigger class than the class of cyclic codes. If a trivial automorphism is used, the notion of the cyclic code coincides with the notion of the skew cyclic code. As a similar, the notion of the skew quasi-cyclic codes and skew constacyclic codes are generalizations of the notions of quasi-cyclic codes and constacyclic codes. There are a lot of studies about skew codes.

Firstly, D. Boucher et al. generalized the notion of cyclic codes by using generator polynomials in skew polynomial rings. They introduced skew cyclic codes over finite fields with q elements in [7].

In [8], D. Boucher et al. generalized the construction of linear codes via skew polynomials rings by using Galois ring instead of finite fields. In 2008, D. Boucher and F. Ulmer gave some important result on the duals of skew cyclic codes over $\mathbb{F}_q$ in [9]. T. Abualrub and P. Seneviratne studied skew cyclic codes over the finite ring $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$

[1] Ondokuz Mayıs University, Faculty of Arts and Sciences, Mathematics Department, Samsun, Turkey.
E-mail: abdullah.dertli@gmail.com.
[2] Trakya University, Faculty of Sciences, Mathematics Department, Edirne, Turkey.
E-mail: ycengellenmis@gmail.com.

in [1]. In [2], T. Abualrub et al. studied skew quasi- cyclic codes over $\mathbb{F}_q$. The notion of generator and parity-check polynomials was given. M. Bhaintwal investigated skew quasi-cyclic codes over the Galois ring in [6]. A necessary and sufficient condition for skew cyclic codes over Galois rings to be free and a canonical decomposition of skew quasi-cyclic codes were given. J. Gao et al. studied skew generalized quasi-cyclic codes over finite fields in [12]. In [21], I. Siap et al. investigated the structural properties of skew cyclic codes of arbitrary length over finite fields. In [16], S. Jitman et al. studied the Gray image of three type skew constacyclic codes over finite chain ring. J. Gao studied skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, $v^2 = v$, p is a prime in [13]. He investigated the structural properties of skew poynomial $(\mathbb{F}_p + v\mathbb{F}_p)[x, \theta]$ and $(\mathbb{F}_p + v\mathbb{F}_p)[x, \theta]/\langle x^n - 1\rangle$. F. Gursoy et al. introduced skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, $v^2 = v$, $q = p^m$ in [15]. The idempotent generators of skew cyclic codes over $\mathbb{F}_q$ and $\mathbb{F}_q + v\mathbb{F}_q$ were given, firstly. Both M. Ashraf et al. and M. Shi et al. studied skew cyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, $v^3 = v$, $q = p^m$, p is odd prime at the same time in [5] and [19] , respectively. In [14], J. Gao et al. generalized it to the finite ring $S = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, $v^4 = v$, $q = p^r$, p is odd prime, $3|p-1$. They studied skew cyclic codes over S. In [3], M. Ashraf et al. investigated skew cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$, $v^2 = 1$ by taking the automorphism as $\theta : v \mapsto -v$. Later, M. Ashraf et al. extended this work to the ring $\mathbb{F}_{p^m} + v\mathbb{F}_{p^m}$, $v^2 = 1$, p is odd prime in [4]. In [20], M. Shi et al. interested in skew cyclic codes over $T = \mathbb{F}_q + v\mathbb{F}_q + u\mathbb{F}_q + uv\mathbb{F}_q$, $u^2 = u, v^2 = v, uv = vu$. They gave a formula for the number of skew cyclic codes over length n over T. In [10] and [11], A. Dertli et al. investigated skew cyclic and quasi-cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2, u^3 = 1$ and $\mathbb{Z}_3 + v\mathbb{Z}_3 + v^2\mathbb{Z}_3$, $v^3 = v$, respectively.

This paper is organized as follows. In section 2, some knowledges about linear codes over the finite ring D_k are given. We define a new Gray map from D_k to $\mathbb{F}_q^{k+1}$. It is shown that C is self dual so is $\phi(C)$. The Gray image of cyclic code is obtained. A linear code over D_k is represented by means of $k+1$ q-ary codes. The algebraic structure of cyclic code and its duality properties are investigated. In section 3, the non trivial automorphism over D_k is given and we introduce skew cyclic codes over D_k. It is shown that C is a skew cyclic code over D_k if and only if $C_1, C_2, \ldots, C_{k+1}$ are all skew cyclic codes over $\mathbb{F}_q$. The Gray images of skew cyclic codes are given.

2. LINEAR CODES OVER D_k

Let D_k be the ring $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_k\mathbb{F}_q = \{a_0 + v_1a_1 + \cdots + v_ka_k : a_i \in \mathbb{F}_q, i = 0,\ldots,k$ with $vi2=vi$, $vivj=vjvi=0$, $1\le i,j\le k$, $q=pm$, p is a prime. Dk can be as quotient ring $\mathbb{F}_q[v_1, v_2, \ldots, v_k]/\langle v_i^2 = v_i, v_iv_j = v_jv_i = 0\rangle$, where $1 \le i,j \le k$. D_k is a finite commutative ring with q^{k+1} elements. A linear code C over D_k length n is a D_k-submodule of D_k^n. An element of C is called a codeword. We define the Gray map as follows,

$$\phi : \mathrm{D_k} \to \mathbb{F}_q^{k+1}$$
$$\phi(\mathrm{a_0} + \mathrm{v_1a_1} + \cdots + \mathrm{v_ka_k}) = (\mathrm{a_0}, \mathrm{a_0} + \mathrm{a_1}, \mathrm{a_0} + \mathrm{a_2}, \ldots, \mathrm{a_0} + \mathrm{a_k})$$

It can be extended to D_k^n.

Let C be a code over $\mathbb{F}_q$ of length $(k+1)n$ and $c' = \left(c'_0, c'_1, \dots, c'_{(k+1)n-1}\right)$ be a codeword of C. The Hamming weight of c' is defined as $w_H(c') = \sum_{i=0}^{(k+1)n-1} w_H(c'_i)$, where $w_H(c'_i) = 1$ if $c'_i \neq 0$ and $w_H(c'_i) = 0$ if $c'_i = 0$. The minimum Hamming distance of C is defined as $d_H(C) = \min\{d_H(c, c')\}$, where for any $c' \in C$, $c \neq c'$and $d_H(c, c')$ is Hamming distance between two codewords with $d_H(c, c') = w_H(c - c')$.

Let $r = a_0 + v_1 a_1 + \cdots + v_k a_k$ be an element of D_k, then the Lee weight of r is defined as $w_L(r) = w_H(a_0, a_0 + a_1, a_0 + a_1, \dots, a_0 + a_k)$, where w_H is the Hamming weight.

Define the Lee weight of a vector $c = (c_0, c_1, \dots, c_{n-1}) \in D_k^n$ to be the sum of Lee weights of its components. For any element $c_1, c_2 \in D_k^n$, the Lee distance between c_1 and c_2 is given by $d_L(c_1, c_2) = w_H(c_1 - c_2)$. The minimum Lee distance of C is defined as $d_L(C) = \min\{d_L(c_1, c_2)\}$, where for any $c_1 \in C$, $c_1 \neq c_2$.

For any $x = (x_0, x_1, \dots, x_{n-1})$, $y = (y_0, y_1, \dots, y_{n-1})$ the inner product is defined as

$$xy = \sum_{\mathrm{i}=0}^{\mathrm{n}-1} \mathrm{x_i y_i}$$

If $xy = 0$ then x and y are said to be orthogonal. Let C be a linear code of length n over D_k, the dual code of C

$$\mathrm{C}^{\perp} = \{\mathrm{x} : \forall\, \mathrm{y} \in \mathrm{C}, \mathrm{xy} = 0\}$$

which is also a linear code over D_k of length n. A code C is self orthogonal, if $C \subseteq C^{\perp}$ and self dual, if $C = C^{\perp}$.

A cyclic code C over D_k is a linear code with the property that if $c = (c_0, c_1, \dots, c_{n-1}) \in C$, then $\sigma(C) = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$. A subset C of D_k^n is a linear cyclic code of length n iff its polynomial representation is an ideal of $D_k[x]/\langle x^n - 1\rangle$.

Let $a \in \mathbb{F}_q^{(k+1)n}$ with $a = \left(a_0, a_1, \dots, a_{(k+1)n-1}\right) = \left(a^{(0)} \middle| a^{(1)} \middle| \dots | a^{(k)}\right)$, $a^{(i)} \in \mathbb{F}_q^n$ for $i = 0,1,2, \dots, k$. Let φ be a map from $\mathbb{F}_q^{(k+1)n}$ to $\mathbb{F}_q^{(k+1)n}$ given by $\varphi(a) = \left(\sigma\left(a^{(0)}\right) \middle| \sigma\left(a^{(1)}\right) \middle| \dots | \sigma\left(a^{(k)}\right)\right)$, where σ is a cyclic shift from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ given by

$$\sigma\left(\mathrm{a}^{(\mathrm{i})}\right) = \left(\left(\mathrm{a}^{(\mathrm{i,n-1})}\right), \left(\mathrm{a}^{(\mathrm{i,0})}\right), (\mathrm{a}^{(\mathrm{i,1})}), \dots, \left(\mathrm{a}^{(\mathrm{i,n-2})}\right)\right)$$

for every $a^{(i)} = \left(a^{(i,0)}, a^{(i,1)}, \dots, a^{(i,n-1)}\right)$, where $a^{(i,j)} \in \mathbb{F}_q$, $j = 0, 1, \dots, n-1$.

A code of length $(k+1)n$ over $\mathbb{F}_q$ is said to be quasi-cyclic code of index $k+1$ if $\varphi(C) = C$.

Theorem 1: The Gray map ϕ is distance preserving map from (D_k^n, Lee distance) to ($\mathbb{F}_q^{(k+1)n}$, Hamming distance). Moreover it is $\mathbb{F}_q$-linear.

Proof. For $k_1, k_2 \in \mathbb{F}_q$ and z_1, $z_2 \in D_k^n$, then we have $\phi(k_1 z_1 + k_2 z_2) = k_1 \phi(z_1) + k_2 \phi(z_2)$. So, ϕ is $\mathbb{F}_q$-linear. Let $z_1 = \left(z_{1,0}, z_{1,1}, \dots, z_{1,n-1}\right)$, $z_2 = \left(z_{2,0}, z_{2,1}, \dots, z_{2,n-1}\right)$ be elements D_k^n where $z_{1,i} = a_{1,i}^0 + v_1 a_{1,i}^1 + \cdots + v_k a_{1,i}^k$ and $z_{2,i} = a_{2,i}^0 + v_1 a_{2,i}^1 + \cdots + v_k a_{2,i}^k$, $i = 0,1, \dots, n-1$. Then $z_1 - z_2 = (z_{1,0} - z_{2,0}, \dots, z_{1,n-1} - z_{2,n-1})$ and $\phi(z_1 - z_2) = \phi(z_1) - \phi(z_2)$. So, $d_L(z_1, z_2) = w_L(z_1 - z_2) = w_H\left(\phi(z_1 - z_2)\right) = w_H\left(\phi(z_1) - \phi(z_2)\right) = d_H\left(\phi(z_1), \phi(z_2)\right)$.

Theorem 2: If C is a linear code of length n over D_k with rank r and minimum Lee distance d_L, then $\phi(C)$ is a linear code of length $(k+1)n$ over $\mathbb{F}_q$ with dimension r, $d_H = d_L$.

Proposition 3: Let ϕ be the Gray map from D_k^n to $\mathbb{F}_q^{(k+1)n}$, let σ be the cyclic shift and let φ be a map as in the section 2. Then $\phi\sigma = \varphi\phi$.

Proof. Let $z = (z_0, z_1, \dots, z_{n-1}) \in D_k^n$. Let $z_i = a_i^0 + v_1 a_i^1 + \cdots + v_k a_i^k$, where $a_i^0, a_i^1, \dots, a_i^k \in \mathbb{F}_q$ and $0 \le i \le n-1$. From definition ϕ, we have $\big(a_0^0, \dots, a_{n-1}^0, a_0^0 + a_0^1, \dots, a_{n-1}^0 + a_{n-1}^1, \dots, a_0^0 + a_0^k, \dots, a_{n-1}^0 + a_{n-1}^k\big)$,
$\varphi\big(\phi(z)\big) = \big(a_{n-1}^0, a_0^0, \dots, a_{n-2}^0, a_{n-1}^0 + a_{n-1}^1, \dots, a_{n-2}^0 + a_{n-2}^1, \dots, a_{n-1}^0 + a_{n-1}^k, \dots, a_{n-2}^0 + a_{n-2}^k\big)$ On the other hand, $\sigma(z) = (z_{n-1}, z_0, \dots, z_{n-2})$. If we apply ϕ, we have $\phi\big(\sigma(z)\big) = \big(a_{n-1}^0, a_0^0, \dots, a_{n-2}^0, a_{n-1}^0 + a_{n-1}^1, \dots, a_{n-2}^0 + a_{n-2}^1, \dots, a_{n-1}^0 + a_{n-1}^k, \dots, a_{n-2}^0 + a_{n-2}^k\big)$.

Theorem 4: Let σ and φ be as in section 2. A code C of length n over D_k is a cyclic code iff $\phi(C)$ is a quasi-cyclic code of index $k+1$ over $\mathbb{F}_q$ with length $(k+1)n$.

Proof. Let C be a cyclic code. Then $\sigma(C) = C$. If we apply ϕ, we have $\phi\big(\sigma(C)\big) = \phi(C)$. By using proposition 3, $\phi\big(\sigma(C)\big) = \varphi\big(\phi(C)\big) = \phi(C)$. Hence $\phi(C)$ is a quasi-cyclic code of index $k+1$. For the other part, $\phi(C)$ is a quasi-cyclic code of index $k+1$, then we have $\varphi\big(\phi(C)\big) = \phi(C)$. From proposition 3, we have $\phi\big(\sigma(C)\big) = \varphi\big(\phi(C)\big) = \phi(C)$. Since ϕ is injective, it follows $\sigma(C) = C$.

Definition 5: Let $A_1, A_2, \dots, A_{k+1}$ be linear codes.

$$\mathrm{A}_1 \otimes \mathrm{A}_2 \otimes \dots \otimes \mathrm{A}_{k+1} = \{(\mathrm{a}_1, \mathrm{a}_2, \dots, \mathrm{a}_{k+1}) : \mathrm{a}_1 \in \mathrm{A}_1, \dots, \mathrm{a}_{k+1} \in \mathrm{A}_{k+1}\}$$

and

$$\mathrm{A}_1 \oplus \mathrm{A}_2 \oplus \dots \oplus \mathrm{A}_{k+1} = \{\mathrm{a}_1 + \mathrm{a}_2 + \cdots + \mathrm{a}_{k+1} : \mathrm{a}_1 \in \mathrm{A}_1, \dots, \mathrm{a}_{k+1} \in \mathrm{A}_{k+1}\}$$

Let C be a linear code of length n over D_k. Define

$$\mathrm{C}_1 = \big\{\mathrm{a}_0 \in \mathbb{F}_q^n : \exists\, \mathrm{a}_1, \mathrm{a}_2, \dots, \mathrm{a}_k \in \mathbb{F}_q^n, \mathrm{a}_0 + \mathrm{v}_1\mathrm{a}_1 + \cdots + \mathrm{v}_k\mathrm{a}_k \in \mathrm{C}\big\}$$

$$\mathrm{C}_2 = \big\{\mathrm{a}_0 + \mathrm{a}_1 \in \mathbb{F}_q^n : \mathrm{a}_0 + \mathrm{v}_1\mathrm{a}_1 + \cdots + \mathrm{v}_k\mathrm{a}_k \in \mathrm{C}\big\}$$

$$\vdots$$

$$\mathrm{C}_{k+1} = \big\{\mathrm{a}_0 + \mathrm{a}_k \in \mathbb{F}_q^n : \mathrm{a}_0 + \mathrm{v}_1\mathrm{a}_1 + \cdots + \mathrm{v}_k\mathrm{a}_k \in \mathrm{C}\big\}$$

It is clear that $C_1, C_2, \dots, C_{k+1}$ are q-ary linear codes of length n.

Theorem 6: Let C be a linear code of length n over D_k. Then $\phi(C) = C_1 \otimes C_2 \otimes \dots \otimes C_{k+1}$ and $|C| = |C_1||C_2| \dots |C_{k+1}|$.

Proof. It is proved as in [11].

Corollary 7: If $\phi(C) = C_1 \otimes C_2 \otimes \dots \otimes C_{k+1}$, then

$$\mathrm{C} = (1 - \mathrm{v}_1 - \dots - \mathrm{v}_\mathrm{k})\mathrm{C}_1 \oplus \mathrm{v}_1\mathrm{C}_2 \oplus \mathrm{v}_2\mathrm{C}_3 \oplus \dots \oplus \mathrm{v}_\mathrm{k}\mathrm{C}_{\mathrm{k}+1}.$$

Theorem 8: Let $C = (1 - v_1 - \dots - v_k)C_1 \oplus v_1C_2 \oplus v_2C_3 \oplus \dots \oplus v_kC_{k+1}$ be a linear code of length n over D_k. Then C is a cyclic code over D_k if and only if $C_1, C_2, \dots, C_{k+1}$ are all cyclic codes over $\mathbb{F}_q$.

Proof. Let $(a_0^1, a_1^1, \dots, a_{n-1}^1) \in C_1$, $(a_0^2, a_1^2, \dots, a_{n-1}^2) \in C_2$, ..., $\left(a_0^{k+1}, a_1^{k+1}, \dots, a_{n-1}^{k+1}\right) \in C_{k+1}$. Assume that $z_i = (1 - v_1 - \dots - v_k)a_i^1 + v_1a_i^2 + \dots + v_ka_i^{k+1}$ for $i = 0,1, \dots, n-1$. Then the vector $(z_0, \dots, z_{n-1}) \in C$. As C is a cyclic code, then $(z_{n-1}, z_0, \dots, z_{n-2}) \in C$. Note that $(z_{n-1}, z_0, \dots, z_{n-2})$=$(1 - v_1 - \dots - v_k)(a_{n-1}^1, a_0^1, \dots, a_{n-2}^1) + \dots + v_k\left(a_{n-1}^{k+1}, \dots, a_{n-2}^{k+1}\right)$. Hence $(a_{n-1}^1, a_0^1, \dots, a_{n-2}^1) \in C_1$,..., $\left(a_{n-1}^{k+1}, \dots, a_{n-2}^{k+1}\right) \in C_{k+1}$. So, $C_1, C_2, \dots, C_{k+1}$ are all cyclic codes over $\mathbb{F}_q$.

Conversely, $C_1, C_2, \dots, C_{k+1}$ are all cyclic codes over $\mathbb{F}_q$. Let $(z_0, z_1, \dots, z_{n-1}) \in C$ where $z_i = (1 - v_1 - \dots - v_k)a_i^1 + v_1a_i^2 + \dots + v_ka_i^{k+1}$ for $i = 0,1, \dots, n-1$. Then $(a_0^1, a_1^1, \dots, a_{n-1}^1) \in C_1$, $(a_0^2, a_1^2, \dots, a_{n-1}^2) \in C_2$, ..., $\left(a_0^{k+1}, a_1^{k+1}, \dots, a_{n-1}^{k+1}\right) \in C_{k+1}$. Note that $(z_{n-1}, z_0, \dots, z_{n-2})$=$(1 - v_1 - \dots - v_k)(a_{n-1}^1, a_0^1, \dots, a_{n-2}^1) + \dots + v_k\left(a_{n-1}^{k+1}, \dots, a_{n-2}^{k+1}\right) \in C = (1 - v_1 - \dots - v_k)C_1 \oplus v_1C_2 \oplus v_2C_3 \oplus \dots \oplus v_kC_{k+1}$. Therefore C is a cyclic code over D_k.

Corollary 9: If $G_1, G_2, \dots, G_{k+1}$ are generator matrices of q-ary linear codes $C_1, C_2, \dots, C_{k+1}$ respectively, then the generator matrix of C is

$$G = \begin{bmatrix} (1 - v_1 - \dots - v_k)G_1 \\ v_1G_2 \\ \vdots \\ v_kG_{k+1} \end{bmatrix}$$

We have

$$\phi(G) = \begin{bmatrix} \phi\left((1 - v_1 - \dots - v_k)G_1\right) \\ \phi(v_1G_2) \\ \vdots \\ \phi(v_kG_{k+1}) \end{bmatrix}$$

Let d_L be the minimum Lee weight of a linear code C over D_k. Then,

$$d_L = d_H\left(\phi(C)\right) = \min\{d_H(C_1), \dots, d_H(C_{k+1})\}$$

where $d_H(C_i)$ denotes the minimum Hamming weights of q-ary codes $C_1, \dots, C_{k+1}$, respectively.

Theorem 10: Let C be a linear code over D_k. Then $\phi(C)^\perp = \phi(C^\perp)$. If C is a self dual, so is $\phi(C)$.

Proof. Let $x = a_0 + a_1v_1 + \dots + a_kv_k$, $x^1 = b_0 + b_1v_1 + \dots + b_kv_k \in C$, where $a_0, a_1, \dots, a_k, b_0, b_1, \dots, b_k \in \mathbb{F}_q^n$.

$$xx^1 = a_0b_0 + v_1(a_0b_1 + a_1b_0 + a_1b_1) + \dots + v_k(a_0b_k + a_kb_0 + a_kb_k)$$

Since C is a self dual code, $a_0b_0 = 0, a_0b_1 + a_1b_0 + a_1b_1 = 0, \dots, a_0b_k + a_kb_0 + a_kb_k = 0$. $\phi(x)\phi(x^1) = (a_0, \dots, a_0 + a_k)(b_0, \dots, b_0 + b_k) = 0$. We have $\phi(C)^\perp \subset \phi(C^\perp)$. By using $|\phi(C)^\perp| = |\phi(C^\perp)|$, we have $\phi(C)^\perp = \phi(C^\perp)$.

Proposition 11: Let C be a linear code of length n over D_k and $\phi(C) = C_1 \otimes \dots \otimes C_{k+1}$ then

$$\phi(C^\perp) = C_1^\perp \otimes C_2^\perp \otimes \dots \otimes C_{k+1}^\perp$$

which gives $C^\perp = (1 - v_1 - \cdots - v_k)C_1^\perp \oplus v_1C_2^\perp \oplus \dots \oplus v_kC_{k+1}^\perp$.

Proposition 12: Suppose $C = (1 - v_1 - \cdots - v_k)C_1 \oplus v_1C_2 \oplus \dots \oplus v_kC_{k+1}$ is a cyclic code of length n over D_k. Then

$$C = \langle (1 - v_1 - \cdots - v_k)f_1, v_1f_2, \dots, v_kf_{k+1} \rangle$$

and $|C| = q^{(k+1)n - (deg f_1 + \cdots + deg\, f_{k+1})}$, where $f_1, f_2, \dots, f_{k+1}$ generator polynomials of $C_1, \dots, C_{k+1}$, respectively.

Proposition 13: Suppose C is a cyclic code of length n over D_k, then there is a unique polynomial $f(x)$ such that $C =< f(x) >$ and $f(x) | x^n - 1$, where $f(x) = (1 - v_1 - \cdots -$ *vkf1x+v1f2x+…+vkfk+1(x).*

Proposition 14: If $C = (1 - v_1 - \cdots - v_k)C_1 \oplus v_1C_2 \oplus \dots \oplus v_kC_{k+1}$ is a cyclic code of length n over D_k , then

$$C^\perp = \langle (1 - v_1 - \cdots . -v_k)h_1^* + v_1h_2^* + \cdots + v_kh_{k+1}^* \rangle$$

and $|C^\perp| = q^{(deg f_1 + \cdots + deg\, f_{k+1})}$, where h_i^* are the reciprocal polynomials of h_i for $i = 1,2, \dots, k+1$, i.e., $h_i(x) = x^n - 1/f_i(x)$, $h_i^*(x) = x^{\deg h_i} h_i(x^{-1})$ for $i = 1,2, \dots, k+1$.

3. SKEW CODES OVER D_k

We are interested in studying skew codes over the ring D_k, where $1 \leq k$.

For $k = 1$, $D_1 = \mathbb{F}_q[v_1]/\langle v_1^2 - v_1 \rangle$ where $v_1^2 = v_1$, $q = p^m$ with ring automorphism

$$\theta_i : D_1 \to D_1$$

defined by $\theta_i(a + v_1b) = a^{p^i} + v_1b^{p^i}$. In [15], they studied skew cyclic codes on D_1.

We define non-trivial ring automorphism θ_t on the ring D_k by

$$\theta_t : D_k \to D_k$$
$$\theta_t(a_0 + v_1a_1 + \cdots + v_ka_k) = {a_0}^{p^t} + v_1{a_1}^{p^t} + \cdots . + v_k{a_k}^{p^t}$$

The automorphism θ_1 is Frobenious automorphism of $\mathbb{F}_q$, $q = p^m$ and $\theta_t = \theta_1^t$. The order of the automorphism θ_t is m/t.

The ring $D_k[x, \theta_t] = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_i \in D_k,\ n \in N\}$ is called a skew polynomial ring. This ring is a non-commutative ring. The addition in the ring $D_k[x, \theta_t]$ is the usual polynomial addition and multiplication is defined using the rule, $(ax^i)(bx^j) = a\,\theta_t^i(b) x^{i+j}$.

Definition 15: A subset C of D_k^n is called a skew cyclic code of length n if C satisfies the following conditions,

i. C is a submodule of D_k^n ,

ii. If $c = (c_0, \dots, c_{n-1}) \in C$, then $\sigma_{\theta_t}(c) = (\theta_t(c_{n-1}), \theta_t(c_0), \dots, \theta_t(c_{n-2})) \in C$

Let $f(x) + (x^n - 1)$ be an element in the set $S_{k,n} = D_k[x, \theta_t]/(x^n - 1)$ and let $r(x) \in D_k[x, \theta_t]$. Define multiplication from left as follows,

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

for any $r(x) \in D_k[x, \theta_t]$.

Theorem 16: $S_{k,n}$ is a left $D_k[x, \theta_t]$-module where multiplication defined as in above.

Theorem 17: A code C in $S_{k,n}$ is a skew cyclic code if and only if C is a left $D_k[x, \theta_t]$-submodule of the left $D_k[x, \theta_t]$-module $S_{k,n}$.

Theorem 18: Let C be a linear code of length n over D_k and $C = (1 - v_1 - \cdots - v_k)C_1 \oplus v_1 C_2 \oplus \dots \oplus v_k C_{k+1}$, where $C_1, \dots, C_{k+1}$ are linear codes of length n over $\mathbb{F}_q$. Then C is a skew cyclic code in according to the automorphism θ_t over D_k if and only if $C_1, \dots, C_{k+1}$ are all skew cyclic codes over $\mathbb{F}_q$ in according to the automorphism θ_t.

Proof. Let $(c_0^i, \dots, c_{n-1}^i) \in C_i$, $i = 1,2, \dots, k+1$. Assume that $c_j = (1 - v_1 - \cdots - v_k)c_j^1 + \cdots + v_k c_j^{k+1}$ for $j = 0,1,2, \dots, n-1$, then $c = (c_0, \dots, c_{n-1}) \in C$. As C is a skew cyclic code in according to the automorphism θ_t, we have $\sigma_{\theta_t}(c) = (\theta_t(c_{n-1}), \theta_t(c_0), \dots, \theta_t(c_{n-2})) \in C$. We know that $\sigma_{\theta_t}(c) = (1 - v_1 - \cdots - v_k)(\theta_t(c_{n-1}^1), \theta_t(c_0^1), \dots, \theta_t(c_{n-2}^1)) + \cdots + v_k\left(\theta_t(c_{n-1}^{k+1}), \theta_t(c_0^{k+1}), \dots, \theta_t(c_{n-2}^{k+1})\right)$. So, $\left(\theta_t(c_{n-1}^i), \theta_t(c_0^i), \dots, \theta_t(c_{n-2}^i)\right) \in C_i$ for $i = 1,2, \dots, k+1$. We have $C_1, \dots, C_{k+1}$ are skew cyclic codes in according to automorphism θ_t over $\mathbb{F}_q$.

Conversely, assume that $C_1, \dots, C_{k+1}$ are skew cyclic codes in according to automorphism θ_t over $\mathbb{F}_q$ and $c = (c_0, \dots, c_{n-1}) \in C$ where $c_j = (1 - v_1 - \cdots - v_k)c_j^1 + \cdots + v_k c_j^{k+1}$ for $j = 0,1, \dots, n-1$, then $(c_0^i, \dots, c_{n-1}^i) \in C_i$, $i = 1,2, \dots, k+1$. Note that $\sigma_{\theta_t}(c) = (1 - v_1 - \cdots - v_k)(\theta_t(c_{n-1}^1), \theta_t(c_0^1), \dots, \theta_t(c_{n-2}^1)) + \cdots + v_k\left(\theta_t(c_{n-1}^{k+1}), \dots, \theta_t(c_{n-2}^{k+1})\right) \in C$.

Corollary 19: If C is a skew cyclic code in according to the automorphism θ_t over D_k, then the dual code $C^{\perp}$ is also a skew cyclic code in according to the automorphism θ_t over D_k.

Theorem 20: Let $C_1, \dots, C_{k+1}$ are skew cyclic codes over $\mathbb{F}_q$ and $g_i(x)$ be the monic generator polynomials of them for $i = 1,2, \dots, k+1$, respectively. Let $C = (1 - v_1 - \cdots - v_k)C_1 \oplus v_1 C_2 \oplus \dots \oplus v_k C_{k+1}$. Then there exist a unique polynomial $g(x) = (1 - v_1 - \cdots - v_k)g_1(x) + v_1 g_2(x) + \cdots + v_k g_{k+1}(x) \in D_k[x, \theta_t]$ such that $C =< g(x) >$ and $g(x)$ is a right divisor of $x^n - 1$.

Corollary 21: Every left submodule of $D_k[x, \theta_t]/< x^n - 1 >$ is principally generated.

Definition 22 Let $\mathbb{F}_q$ be a finite field of characteristic p with q elements and θ_t be an automorphism of $\mathbb{F}_q$. A subset C of $\mathbb{F}_q^{(k+1)n}$ is called a skew quasi-cyclic code of length $(k+1)n$ and index n such that $|\theta_t||k+1$ if,

i. C is subspace of $\mathbb{F}_q^{(k+1)n}$
ii. If $c = \left(c_{0,0}, c_{01}, \dots, c_{0,n-1}, c_{1,0}, \dots, c_{1,n-1}, \dots, c_{k,0}, \dots, c_{k,n-1}\right) \in C$, then

$$\tau_{\theta_t,k+1,n}(c) = \begin{pmatrix} \theta_t(c_{k,0}), \dots, \theta_t(c_{k,n-1}), \theta_t(c_{0,0}), \dots, \\ \theta_t(c_{0,n-1}), \dots, \theta_t(c_{k-1,0}), \dots, \theta_t(c_{k-1,n-1}) \end{pmatrix} \in C$$

Proposition 23 Let σ_{θ_t} be the skew cyclic shift on D_k^n, let ϕ be the Gray map from D_k^n to $\mathbb{F}_q^{(k+1)n}$, let φ be as in the section 2 and let $\tau_{\theta_t,k+1,n}$ be the skew quasi-cyclic shift operator. So, $\phi\sigma_{\theta_t} = \nu\varphi\tau_{\theta_t,k+1,n}\phi$ where ν is a map such that $\nu(x_1, \dots, x_{k+1}) = (x_2, \dots, x_{k+1}, x_1)$ for $x_i \in \mathbb{F}_q^n$ with $i = 1,2, \dots, k+1$.

Proof. Let $r_i = \alpha_0^i + v_1\alpha_1^i + \cdots + v_k\alpha_k^i$ be the elements of D_k, for $i = 0,1, \dots, n-1$. We have $\sigma_{\theta_t}(r_0, \dots, r_{n-1}) = (\theta_t(r_{n-1}), \theta_t(r_0), \dots, (\theta_t(r_{n-2}))$. If we apply ϕ, we have $\phi(\sigma_{\theta_t}(r_0, \dots, r_{n-1})) = \phi((\theta_t(r_{n-1}), \theta_t(r_0), \dots., (\theta_t(r_{n-2}))$
$= \left((\alpha_0^{n-1})^{p^t}, (\alpha_0^0)^{p^t}, \dots, (\alpha_0^{n-2})^{p^t}, (\alpha_0^{n-1})^{p^t} + (\alpha_1^{n-1})^{p^t}, \dots, (\alpha_0^{n-2})^{p^t} +\right.$ *(α1n−2)pt,..., (α0n−1)pt+(αkn−1)pt,..., (α0n−2)pt+(αkn−2)pt* .

On the other hand, $\phi(r_0, \dots, r_{n-1}) = (\alpha_0^0, \dots, \alpha_0^{n-1}, \alpha_0^0 + \alpha_1^0, \dots, \alpha_0^{n-1} + \alpha_1^{n-1}, \dots, \alpha_0^0 +$ *αk0,..., α0n−1+αkn−1.* By applying *τθt,k+1,n,* we have $\tau_{\theta_t,k+1,n}\left(\phi(r_0, \dots, r_{n-1})\right) =$
$((\alpha_0^0)^{p^t} + (\alpha_k^0)^{p^t}, \dots, (\alpha_0^{n-1})^{p^t} + (\alpha_k^{n-1})^{p^t}, (\alpha_0^0)^{p^t}, \dots, (\alpha_0^{n-1})^{p^t}, \dots, (\alpha_0^0)^{p^t} +$
$(\alpha_{k-1}^0)^{p^t}, \dots, (\alpha_0^{n-1})^{p^t} + (\alpha_{k-1}^{n-1})^{p^t})$. We have expected result.

Theorem 24: The Gray image a skew cyclic code over D_k of length n is permutation equivalent to a skew quasi-cyclic code of index n over $\mathbb{F}_q$ with length $(k+1)n$.

Proof. Let C be a skew cyclic codes over D_k of length n. So, $\sigma_{\theta_t}(C) = C$. If we apply ϕ, we have $\phi(\sigma_{\theta_t}(C)) = \phi(C)$. From the Proposition 23, $\phi(\sigma_{\theta_t}(C)) = \phi(C) = \nu(\varphi(\tau_{\theta_t,k+1,n}(\phi(C))))$. So, $\phi(C)$ is permutation equivalent to a skew quasi-cyclic code of index n over $\mathbb{F}_q$ with length $(k+1)n$.

4. CONCLUSION

The algebraic structures of cyclic and skew cyclic codes over the finite ring D_k are studied. A new Gray map from D_k to $\mathbb{F}_q^{k+1}$ is defined. The non trivial automorphism over D_k is given and the skew cyclic codes over D_k are introduced. A linear code over D_k is represented by means of $k+1$ q-ary codes. It is shown that C is a (cyclic) skew cyclic code over D_k if and only if $C_1, C_2, \dots, C_{k+1}$ are all (cyclic) skew cyclic codes over $\mathbb{F}_q$. The algebraic structures of (cyclic) skew cyclic codes and its duality properties are investigated. The Gray images of skew cyclic and cyclic codes are obtained.

REFERENCES

[1] Abualrub, T., Seneviratne, P., Skew Codes over Rings, *Proceeding of the International Multiconference of Engineers and Computer Scientist 2010*, **II**, 846, 2010.
[2] Abualrub T., Ghrayeb A., Aydın N., Siap I., *IEEE Transactions on Information Theory*, **56**(5), 2081, 2010.
[3] Ashraf, M., Mohammed, G., *Int. J. Inf. Coding Theory*, **2**(4), 218, 2014.
[4] Ashraf, M., Mohammed, G., *Discrete Math. Algorithm and Appl.*, **7**(3), 1550042, 2015.
[5] Ashraf, M., Mohammed, G., Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, *arXiv:1504.04326v1*, 2015.
[6] Bhaintwal, M., *Designs, Codes and Cryptography*, **62**(1), 85, 2012.
[7] Boucher D., Geiselmann W., Ulmer F., *Appl. Algebra. Eng. Commun Comput.*, **18**(4), 379, 2007.
[8] Boucher, D., Sole, P., Ulmer, F., *Advance of Mathematics of Communications*, **2**(3), 273, 2008.
[9] Boucher, D., Ulmer, F., *Journal of Symbolic Computation*, **44**, 1644, 2009.
[10] Dertli, A., Cengellenmis, Y., Eren, S., *Palestine Journal of Math*, **4**, 540, 2015.
[11] Dertli A., Cengellenmis Y., Eren S., *Int Journal Adv. Comp Science and Appl.*, **6**(10), 283, 2015.
[12] Gao, J., Shen, L., Fu, F. W., Skew generalized quasi-cyclic codes over finite fields, *arXiv: 13091621v1*, 2013.
[13] Gao J., *J. Appl. Math. & Informatics*, **31**(3-4), 337, 2013.
[14] Gao J., Wu L. T., Fu F., Skew Cyclic Codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, *ResearchGate*, 2016.
[15] Gursoy F., Siap I., Yıldız B., *Adv. Math Commun*, **8**, 313, 2014.
[16] Jitman, S., Ling, S., Udomkovanich, P., *Adv. Math Commun.*, **6**, 29, 2012.
[17] Prange, E., *Cyclic error-correcting codes in two symbols*, Air Force Cambridge Research Center-TN-57-103, Cambridge, MA, 1957.

[18] Prange, E., *Some cyclic error-correcting codes with simple decoding algorithm*, Air Force Cambridge Research Center-TN-58-156, Cambridge, MA, 1958.

[19] Shi, M., Yao, T., Alahmadi, A., Sole, P., *IECE Trans. Fundamentals*, **E89-A**, 1845, 2015.

[20] Shi, M., Sole, P., *Journal of Algebra Combinatoric Dis. Struc. and Appl*., **2**, 163, 2015.

[21] Siap I., Abualrub T., Aydın N., Seneviratne P., *Int. J.Information and Coding Theory*, **2**(1), 10, 2010.