ORIGINAL PAPER

SKEW CYCLIC CODES OVER $F_q + uF_q + vF_q + uvF_q$

ABDULLAH DERTLI[1], YASEMIN CENGELLENMIS[2]

Manuscript received: 21.11.2016; Accepted paper: 03.04.2017;
Published online: 30.06.2017.

Abstract. *In this paper, the skew cyclic codes over the ring $R = F_q + uF_q + vF_q + uvF_q$, where $u^2 = 1, v^2 = 1, uv = vu, q = p^m, p$ is an odd prime are studied. The structural properties of them are investigated.*

Keywords: *skew cyclic codes; automorphism; Gray map.*

1. INTRODUCTION

As the probability of obtaining the codes which have got big minimum distance are increased, to study about skew codes is vantage.

There are a lot of papers about skew codes such as skew cyclic, skew constacyclic, skew quasicyclic codes, skew generalized quasicyclic codes. At the beginning, these type codes were introduced over finite fields [7, 13, 19]. Later, they were introduced over many finite rings.

The skew cyclic codes are generalization of the notion of cyclic codes. There are also a lot of studies about skew cyclic codes [1-6, 8-12, 14-18]. In these papers, the structural properties of them were investigated. The Gray images of them were determined. The generator polynomials of them and their duals were described. Moreover, in some of these papers, the idempotent generators of them were considered.

In this paper, we study skew cyclic codes over ring the $R = F_q + uF_q + vF_q + uvF_q$, where $u^2 = 1, v^2 = 1, uv = vu$ and $q = p^m, p$ is an odd prime.

The automorphisms θ_t on the ring R are defined as follows,

$$\theta_t : R \to R$$

$$a = a_0 + ua_1 + va_2 + uva_3 \longmapsto \theta_t(a) = a_0^{p^t} + ua_1^{p^t} + va_2^{p^t} + uva_3^{p^t}$$

One can verify that θ_t is an automorphism on R and $\theta_t = \theta_1^t$.

This automorphism acts on F_q as follows

$$\theta_t : F_q \to F_q$$

$$a \longmapsto a^{p^t}$$

[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.

It may be note that the order of this automorphism is $|\langle\theta_t\rangle| = \frac{m}{t}$.

The paper is organized as follows. In section 2, some knowledges about the ring R are given. In section 3, the non trivial automorphism over R is given and we introduce skew cyclic codes over R. It is shown that C is a skew cyclic code over R if and only if C_1, C_2, C_3 and C_4 are all skew cyclic codes over F_q. The structure of skew cyclic codes over R is given.

2. PRELIMINARIES

Let R be denote the commutative ring $F_q + uF_q + vF_q + uvF_q$, where $u^2 = 1, v^2 = 1, uv = vu$ and F_q is a finite field with q elements, $q = p^m, p$ is an odd prime.

Let

$$\lambda_1 = \left(\frac{q^2+1}{4}\right)(1+u+v+uv)$$

$$\lambda_2 = \left(\frac{q^2+1}{4}\right)(1+u) + \left(\frac{q^2-1}{4}\right)(v+uv)$$

$$\lambda_3 = \left(\frac{q^2+1}{4}\right)(1+v) + \left(\frac{q^2-1}{4}\right)(u+uv)$$

$$\lambda_4 = \left(\frac{q^2+1}{4}\right)(1+uv) + \left(\frac{q^2-1}{4}\right)(u+v)$$

It is easy to show that $\lambda_i^2 = \lambda_i$, $\lambda_i\lambda_j = 0$ and $\sum_{k=1}^{4}\lambda_k = 1$ where $i, j = 1,2,3,4$ and $i \neq j$.

This shows that $R = \lambda_1 F_q + \lambda_2 F_q + \lambda_3 F_q + \lambda_4 F_q$. For any $r \in R$, the element r can be expressed uniquely as $r = \sum_{i=1}^{4}\lambda_i a_i$, where $a_i \in F_q$ for $i = 1,2,3,4$.

We define the Gray map as follows,

$$\Phi: R \to F_q^4$$

$$a + ub + vc + uvd \longmapsto \beta$$

where

$$\beta = ((q^2+1)4^{-1}(a+b+c+d), (q^2+1)4^{-1}(a+b) + (q^2-1)4^{-1}(c+d), (q^2+$$
$$14-1a+c+q2-14-1b+d,q2+14-1a+d+q2-14-1(b+c))$$

This can be extended from R^n to F_q^{4n}.

For any element $r = a + ub + vc + uvd \in R$, we define the Lee weight of r as $w_L(r) = w_H(\beta)$, where w_H is the Hamming weight for q-ary codes.

For any element $x, y \in R$, the Lee distance is given by $d_L(x,y) = w_L(x-y)$.

Theorem: The Gray map is an isometry from (R^n, Lee distance) to (F_q^{4n}, Hamming distance).

Proof: For any $x_1, x_2 \in R$ and $\lambda \in F_q$, $\Phi(x_1 + x_2) = \Phi(x_1) + \Phi(x_2)$ and $\Phi(\lambda x_1) = \lambda\Phi(x_1)$. So Φ is linear. From the definition, we have $d_L(x_1, x_2) = w_L(x_1 - x_2) = w_H\big(\Phi(x_1 - x_2)\big) = w_H\big(\Phi(x_1) - \Phi(x_2)\big) = d_H\big(\Phi(x_1), \Phi(x_2)\big)$.

Theorem: If C is a linear code of length n over R with rank k and minimum Lee distance d, then $\Phi(C)$ is $[4n, k, d]$ linear code F_q.

Theorem: If C is self orthogonal, then $\Phi(C)$ is self orthogonal.

Proof: Let C be self orthogonal and $x = a_0 + ua_1 + va_2 + uva_3$, $\acute{x} = b_0 + ub_1 + vb_2 + uvb_3 \in C$ where, $a_0, \dots, a_3, b_0, \dots, b_3 \in F_q^n$.

$$x\acute{x} = a_0b_0 + a_1b_1 + a_2b_2 + a_3b_3 + u(a_0b_1 + a_1b_0 + a_2b_3 + a_3b_2)$$

$$+v(a_0b_2 + a_1b_3 + a_2b_0 + a_3b_1) + uv(a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)$$

Since C is self orthogonal code, we have

$$a_0b_0 + a_1b_1 + a_2b_2 + a_3b_3 = 0$$

$$a_0b_1 + a_1b_0 + a_2b_3 + a_3b_2 = 0$$

$$a_0b_2 + a_1b_3 + a_2b_0 + a_3b_1 = 0$$

$$a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = 0$$

$$\begin{aligned}\Phi(x).\Phi(\acute{x}) = \big(&(q^2+1)4^{-1}(a_0 + a_1 + a_2 + a_3), (q^2+1)4^{-1}(a_0 + a_1) \\ &+ (q^2-1)4^{-1}(a_2 + a_3), (q^2+1)4^{-1}(a_0 + a_2) \\ &+ (q^2-1)4^{-1}(a_1 + a_3), (q^2+1)4^{-1}(a_0 + a_3) \\ &+ (q^2-1)4^{-1}(a_1 + a_2)\big).\big((q^2+1)4^{-1}(b_0 + b_1 + b_2 + b_3), (q^2+1)4^{-1}(b_0 \\ &+ b_1) + (q^2-1)4^{-1}(b_2 + b_3), (q^2+1)4^{-1}(b_0 + b_2) \\ &+ (q^2-1)4^{-1}(b_1 + b_3), (q^2+1)4^{-1}(b_0 + b_3) + (q^2-1)4^{-1}(b_1 + b_2)\big) \\ &= 0\end{aligned}$$

Hence $\Phi(C)$ is self orthogonal.
Let A_1, A_2, A_3, A_4 are linear codes, then we denote that

$$A_1 \oplus A_2 \oplus A_3 \oplus A_4 = \{a_1 + a_2 + a_3 + a_4 : a_i \in A_i, 1 \le i \le 4\}$$

$$A_1 \otimes A_2 \otimes A_3 \otimes A_4 = \{(a_1, a_2, a_3, a_4) : a_i \in A_i, 1 \leq i \leq 4\}$$

Definition: Let C be a linear code of length n over R. Define

$$C_1 = \left\{(q^2+1)4^{-1}(a_0+a_1+a_2+a_3) \in F_q^n : a_0 + ua_1 + va_2 + uva_3 \in C\right\}$$

$$C_2 = \left\{4^{-1}(a_0+a_1) + (q^2-1)4^{-1}(a_2+a_3) \in F_q^n : \ a_0 + ua_1 + va_2 + uva_3 \in C\right\}$$

$$C_3 = \left\{(q^2+1)4^{-1}(a_0+a_2) + (q^2-1)4^{-1}(a_1+a_3) \in F_q^n : \ a_0 + ua_1 + va_2 + uva_3 \in C\right\}$$

$$C_4 = \left\{(q^2+1)4^{-1}(a_0+a_3) + (q^2-1)4^{-1}(a_1+a_2) \in F_q^n : \ a_0 + ua_1 + va_2 + uva_3 \in C\right\}$$

Theorem: Let C be a linear code of length n over R. Then $\Phi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ and $|C| = |C_1||C_2||C_3||C_4|$.

Proof: Let $(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n, t_1, \ldots, t_n) \in \Phi(C)$. Let

$$c_i = (q^2+1)4^{-1}(x_i+y_i+z_i+t_i) + u[4^{-1}(x_i+y_i) + (q^2-1)4^{-1}(z_i+t_i)]$$
$$+ v[(q^2+1)4^{-1}(x_i+z_i) + (q^2-1)4^{-1}(y_i+t_i)]$$
$$+ uv[(q^2+1)4^{-1}(x_i+t_i) + (q^2-1)4^{-1}(y_i+z_i)]$$

where $1 \leq i \leq n$. By using Φ is bijection, we have $c = (c_1, c_2, \ldots, c_n) \in C$. By the definition of C_1, C_2, C_3 and C_4, we get $(x_1, \ldots, x_n) \in C_1$, $(y_1, \ldots, y_n) \in C_2$, $(z_1, \ldots, z_n) \in C_3$ and $(t_1, \ldots, t_n) \in C_4$. Hence $(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n, t_1, \ldots, t_n) \in C_1 \otimes C_2 \otimes C_3 \otimes C_4$. This means that $\Phi(C) \subseteq C_1 \otimes C_2 \otimes C_3 \otimes C_4$.

On the other hand, let $(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n, t_1, \ldots, t_n) \in C_1 \otimes C_2 \otimes C_3 \otimes C_4$, where $x = (x_1, \ldots, x_n) \in C_1$, $y = (y_1, \ldots, y_n) \in C_2$, $z = (z_1, \ldots, z_n) \in C_3$ and $t = (t_1, \ldots, t_n) \in C_4$. There are $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$, $c = (c_1, \ldots, c_n)$, $d = (d_1, \ldots, d_n) \in C$ such that

$$a_i = x_i + \lambda_4 p_i$$

$$b_i = y_i + \lambda_3 q_i$$

$$c_i = z_i + \lambda_2 r_i$$

$$d_i = t_i + \lambda_1 s_i$$

where $p_i, q_i, r_i, s_i \in F_q$. As C is a linear code, then

$$e = a[(q^2+1)4^{-1}(1+u+v+uv)] + b[4^{-1}(1+u) + (q^2-1)4^{-1}(v+uv)]$$
$$+ c[(q^2+1)4^{-1}(1+v) + (q^2-1)4^{-1}(u+uv)]$$
$$+ d[(q^2+1)4^{-1}(1+uv) + (q^2-1)4^{-1}(u+v)]$$

$$= [(q^2+1)4^{-1}(x+y+z+t)] + u[4^{-1}(x+y) + (q^2-1)4^{-1}(z+t)]$$

$$+ v[(q^2+1)4^{-1}(x+z) + (q^2-1)4^{-1}(y+t)]$$

$$+ uv[(q^2+1)4^{-1}(x+t) + (q^2-1)4^{-1}(y+z)]$$

It follows that $\Phi(e) = (x,y,z,t) \in \Phi(C)$. So $C_1 \otimes C_2 \otimes C_3 \otimes C_4 \subseteq \Phi(C)$.
Hence $C_1 \otimes C_2 \otimes C_3 \otimes C_4 = \Phi(C)$. As Φ is bijection, then $|C| = |\Phi(C)| = |C_1 \otimes C_2 \otimes C_3 \otimes C_4| = |C_1||C_2||C_3||C_4|$.

Lemma: If G_i is generator matrix of q-ary linear codes C_i, for $i = 1,2,3,4$, then the generator matrix of C is

$$G = \begin{bmatrix} \lambda_1 G_1 \\ \lambda_2 G_2 \\ \lambda_3 G_3 \\ \lambda_4 G_4 \end{bmatrix}$$

Corollary: If $\Phi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$, then $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4$.

Lemma: Let d_L be minimum Lee weight of linear code C over R. Then

$$d_L = d_H(\Phi(C)) = \min\{d_H(C_1), d_H(C_2), d_H(C_3), d_H(C_4)\}$$

3. SKEW CYCLIC CODES OVER *R*

We are interested in studying skew cyclic codes by using the ring R. By using non trivial ring automorphism θ_t on the ring R, we introduce the skew polynomial ring

$$R[x,\theta_t] = \{a_0 + a_1 x + \cdots . + a_{n-1}x^{n-1} : a_i \in R, n \in N\}$$

This ring is a noncommutative ring. The addition in the ring $R[x,\theta_t]$ is the usual polynomial addition and multiplication is defined using the rule as follows

$$(ax^i)(bx^j) = a\theta_t^i(b)x^{i+j}$$

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

i. C is a submodule of R^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 $R_{t,n} = R[x,\theta_t]/(x^n-1)$ and let $r(x) \in R[x,\theta_t]$. Define multiplication from left as follows,

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

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

Theorem: $R_{t,n}$ is a left $R[x,\theta_t]$-module where multiplication defined as in above.

Theorem: A code C is a skew cyclic code of length n if and only if C is a left $R[x,\theta_t]$-submodule of the left $R[x,\theta_t]$-module $R_{t,n}$.

Theorem: Let C be a linear code of length n over R and $C=\lambda_1C_1\oplus\lambda_2C_2\oplus\lambda_3C_3\oplus\lambda_4C_4$, where C_1,C_2,C_3 and C_4 are linear codes of length n over F_q. Then C is a skew cyclic code with respect to the automorphism θ_t over R if and only if C_1,C_2,C_3 and C_4 are all skew cyclic codes over F_q.

Proof: Let $(c_1^i,\dots,c_n^i)\in C_i$, $i=1,2,3,4$. Assume that $c_j=\lambda_1c_j^1+\lambda_2c_j^2+\lambda_3c_j^3+\lambda_4c_j^4$ for $j=1,2,\dots,n$, then $c=(c_1,\dots,c_n)\in C$. As C is a skew cyclic code in according to the automorphism θ_t, we have $\sigma_{\theta_t}(c)=(\theta_t(c_n),\theta_t(c_1),\dots,\theta_t(c_{n-1}))\in C$. We know that $\sigma_{\theta_t}(c)=\lambda_1\big(\theta_t(c_n^1),\theta_t(c_1^1),\dots,\theta_t(c_{n-1}^1)\big)+\cdots+\lambda_4\big(\theta_t(c_n^4),\theta_t(c_1^4),\dots,\theta_t(c_{n-1}^4)\big)$. Hence $\Big(\theta_t\big(c_n^i\big),\theta_t\big(c_1^i\big),\dots,\theta_t\big(c_{n-1}^i\big)\Big)\in C_i$ for $i=1,2,3,4$. We have C_1,C_2,C_3 and C_4 are skew cyclic codes in according to automorphism θ_t over F_q.

Conversely, assume that C_1,C_2,C_3 and C_4 are skew cyclic codes in according to automorphism θ_t over F_q and $c=(c_1,\dots,c_n)\in C$ where $c_j=\lambda_1c_j^1+\lambda_2c_j^2+\lambda_3c_j^3+\lambda_4c_j^4$ for $j=1,2,\dots,n$, then $(c_1^i,\dots,c_n^i)\in C_i$, $i=1,2,3,4$. Note that

$$\sigma_{\theta_t}(c)=\lambda_1\big(\theta_t(c_n^1),\theta_t(c_1^1),\dots,\theta_t(c_{n-1}^1)\big)+\cdots+\lambda_4\big(\theta_t(c_n^4),\theta_t(c_1^4),\dots,\theta_t(c_{n-1}^4)\big)\in C.$$

Theorem: Let C_1,C_2,C_3 and C_4 are skew cyclic codes over F_q and $g_i(x)$ be the monic generator polynomials of them for $i=1,2,3,4$, respectively. Let $C=\lambda_1C_1\oplus\lambda_2C_2\oplus\lambda_3C_3\oplus\lambda_4C_4$. Then there exist a unique polynomial $g(x)=\lambda_1g_1(x)+\lambda_2g_2(x)+\lambda_3g_3(x)+\lambda_4g_4(x)\in R[x,\theta_t]$ such that $C=<g(x)>$ and $g(x)$ is a right divisor of x^n-1 and $|C|=q^{4n-\sum_{i=1}^{4}degg_i(x)}$.

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

Theorem: Let $(n,\rho)=1$, where ρ is the order of θ_t and C be a skew cyclic code of length n, then C is a cyclic code of length n over R.

Corollary: Let $(n,\rho)=1$, where ρ is the order of θ_t and $x^n-1=\prod_{i=1}^{r}f_i^{p_i}(x)$, where $f_i(x)\in F_q[x,\theta_t]$ is irreducible, then the number of distinct skew cyclic codes of length n over R is equal to the number of ideals in $R[x]/(x^n-1)$, i.e. $\prod_{i=1}^{r}(p_i+1)^3$.

4. CONCLUSION

The skew cyclic codes over the finite ring R are studied. A new Gray map from R to F_q^4 is defined. The non trivial automorphism over R is given and the skew cyclic codes over R are introduced. A linear code over R is represented by means of four q-ary codes. It is shown that C is a skew cyclic code over R if and only if C_1, C_2, C_3 and C_4 are all skew cyclic codes over F_q.

REFERENCES

[1] Abualrub, T., Seneviratne, P., Skew Codes over Rings, *Proceeding of the International Multiconference of Engineers and Computer Scientist 2010*, **II**, 2010.

[2] Abualrub, T., Ghrayeb, A., Aydın, N., Siap, I., *IEEE Transactions on Information Theory*, **56**(5), 2081, 2010.

[3] Ashraf, M., Mohammed, G., *International Journal of Information and Coding Theory*, **2**(4), 218, 2014.

[4] Ashraf, M., Mohammed, G., *Discrete Mathematics, Algorithms and Applications*, **7**(4), 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., *Applicable Algebra in Engineering, Communication and Computing*, **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 Mathematics*, **4**, 540, 2015.

[11] Dertli, A., Cengellenmis, Y., Eren, S., *International Journal of Advanced Computer Science and Applications*, **6**(10), 283, 2015.

[12] Dertli, A., Cengellenmis, Y., *Journal of Science and Arts*, **1**(34), 13, 2016.

[13] Gao, J., Shen, L., Fu, F.W., Skew generalized quasi-cyclic codes over finite fields, *arXiv: 13091621v1*, 2013.

[14] Gao, J., *Journal of Applied Mathematics and Informatics*, **31**(3-4), 337, 2013.

[15] Gursoy, F., Siap, I., Yıldız, B., *Advances in Mathematics of Communications*, **8**, 313, 2014.

[16] Jitman S., Ling, S., Udomkovanich, P., *Advances in Mathematics of Communications*, **6**, 29, 2012.

[17] Shi, M., Yao, T., Alahmadi, A., Sole, P., *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E89-A**, 1845, 2015.

[18] Shi, M., Sole, P., *Journal of Algebra Combinatorics Discrete Structures and Applications*, **2**, 163, 2015.

[19] Siap, I., Abualrub, T., Aydın, N., Seneviratne, P., *International Journal of Information and Coding Theory*, **2**(1), 10, 2011.