第47卷第10期 中国科学技术大学学报 Vol.47,No.10
2017年10月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Oct. 2017

文章编号:0253-2778(2017)10-0862-07

Skew cyclic codes over $\mathbb{F}_q[u,v]/\langle u^2-1,\ v^3-v,\ uv-vu\rangle$

GUAN Yue, LIU Yan, SHI Minjia, LU Zhenyu, WU Bo

(*School of Mathematical Sciences, Anhui University. Hefei 230601, China*)

Abstract: The skew cyclic codes over $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q+v^2\mathbb{F}_q+uv^2\mathbb{F}_q$ were conducted. By defining a gray map from R to $\mathbb{F}_q^6$, the gray image of a linear code of length n over R was considered. Moreover, the generator polynomials of skew cyclic codes over this ring were described and their structural properties by a decomposition theorem investigated. Further, it is shown that the skew cyclic codes over R are principally generated. Finally, the idempotent generators of skew cyclic codes over R were obtained.

Key words: linear codes; dual codes; skew cyclic codes; gray map

CLC number: TN911.22 **Document code**: A doi:10.3969/j.issn.0253-2778.2017.10.009

2010 Mathematics Subject Classification: Primary 94B05; Secondary 94B99

Citation: GUAN Yue, LIU Yan, SHI Minjia, et al. Skew cyclic codes over $\mathbb{F}_q[u,v]/\langle u^2-1,\ v^3-v,\ uv-vu\rangle$ [J]. Journal of University of Science and Technology of China, 2017,47(10):862-868.
管玥,刘艳,施敏加,等. 环 $\mathbb{F}_q[u,v]/\langle u^2-1,v^3-v,uv-vu\rangle$ 上的斜循环码[J]. 中国科学技术大学学报,2017,47(10):862-868.

环 $\mathbb{F}_q[u,v]/\langle u^2-1,v^3-v,uv-vu\rangle$ 上的斜循环码

管玥,刘艳,施敏加,卢振宇,吴波

(安徽大学数学科学学院,安徽合肥 230601)

摘要:研究了环 $R=\mathbb{F}_q[u,v]/\langle u^2-1,v^3-v,uv-vu\rangle$ 上的斜循环码.通过定义从 R 到 $\mathbb{F}_q^6$ 的 Gray 映射,考虑 R 上长度为 n 的线性码的 Gray 像.进一步,利用中国剩余定理定义了该环上的斜循环码并给出了它的生成多项式及结构特性.结果表明,R 上的斜循环码是主理想生成的.最后,给出了 R 上斜循环码的幂等生成元.

关键词:线性码;对偶码;斜循环码;Gray 映射

Received: 2016-06-09; **Revised**: 2017-01-07

Foundation item: Supported by NNSF of China (61672036), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008), Natural Science Research Project of Higher Education of Anhui Province of China (KJ2015JD18).

Biography: GUAN Yue, female, born in 1994, Master candidate. Research field: algebra code. E-mail: guanyueeee@163.com

Corresponding author: SHI Minjia, PhD/Professor. E-mail: smjwcl.good@163.com

0 Introduction

A recent study presented by Boucher et al. introduced a noncommutative ring $\mathbb{F}_q[x,\theta]$, called skew polynomial ring, where $\mathbb{F}_q$ is a finite field with q elements and θ is a field automorphism of $\mathbb{F}_q$. Boucher et al.[1-2] considered the structure of cyclic codes closed under a skew cyclic shift over $\mathbb{F}_q[x,\theta]$, namely, skew cyclic codes, where the generator polynomials of skew cyclic codes come from the ring $\mathbb{F}_q[x,\theta]$. Further, they gave some examples of skew cyclic codes, the Hamming distances of which are larger than the best known linear codes with the same parameters. Based on that, a lot of researchers focused on skew cyclic codes. Recently, Cao[3] investigated the relation between quasi cyclic codes and skew polynomial rings. Boucher and Ulmer[4] introduced the factorization of skew polynomial in skew polynomial rings. These results allowed them to study the skew self-dual cyclic codes with length 2^s.

Later on, Abualrub et al.[5] defined skew quasi cyclic codes over these classes of rings . Jitman et al.[6] defined skew constacyclic codes by defining the skew polynomial ring with coefficients from finite chain rings, especially the ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ where $u^2=0$. Abualrub et al.[7] considered skew cyclic codes over the non chain ring $\mathbb{F}_2+v\,\mathbb{F}_2$ with $v^2=v$ by defining the automorphism $\theta_v : v \mapsto v+1$.However, Gao[8] generalized this result over $\mathbb{F}_p+v\,\mathbb{F}_p$. Gursoy et al.[9] investigated the structural properties of skew cyclic codes through the decomposition method over $\mathbb{F}_q+v\mathbb{F}_q$, where $v^2=v$ and $q=p^m$. In Ref.[10], the authors studied the structural properties of skew cyclic codes over the ring $\mathbb{F}_3+v\mathbb{F}_3$ with $v^2=1$ by considering the automorphism $\theta_v : v \mapsto -v$. They proved that skew cyclic codes over $\mathbb{F}_3+v\mathbb{F}_3$ are equivalent to either cyclic codes or quasi cyclic codes. A lot of work has been done in this direction such as Refs[11-12].

In this paper, we study skew cyclic codes defined by the skew polynomial ring with coefficients over the ring $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q+v^2\mathbb{F}_q+uv^2\mathbb{F}_q$. In our work, we consider the automorphisms $R\rightarrow R$, $a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2 \mapsto a_1^{pi}+a_2^{pi}u+a_3^{pi}v+a_4^{pi}uv+a_5^{pi}v^2+a_6^{pi}uv^2$. The skew polynomial ring in our case is denoted by $R[x,\theta_i]$, where the addition is the usual polynomial addition and the multiplication is defined by the rule $xa=\theta_i(a)x$, $(a\in R)$.

1 Preliminary

Throughout this paper let R be the commutative ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q+v^2\mathbb{F}_q+uv^2\mathbb{F}_q=\{a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2$, where $a_j\in\mathbb{F}_q, 1\leqslant j\leqslant 6\}$ with $u^2=1, v^3=v$ and $uv=vu$. And R_1 denotes the non-chain ring $\mathbb{F}_q+u\mathbb{F}_q$ with $u^2=1$. Then $R=R_1+vR_1+v^2R_1$ can also be thought of as the quotient ring $\mathbb{F}_q[u,v]/\langle u^2-1, v^3-v, uv-vu\rangle$. It is easily checked that R is a Frobenius ring but not local. The definition of the Gray map from R to R_1^3 is defined as $\varphi(a+bv+cv^2)=(a, a+b+c, a-b+c)$, where $a,b,c\in R_1$. The Gray map φ_1 from R_1 to $\mathbb{F}_q^2$ is given by $\varphi_1(a+bu)=(a,b)$, where $a,b\in\mathbb{F}_q$. So we have the following definition.

Definition 1.1 The definition of the Gray map from R to $\mathbb{F}_q^6$ is given by $\Phi(a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2)=(a_1, a_2, a_1+a_3+a_5, a_2+a_4+a_6, a_1-a_3+a_5, a_2-a_4+a_6)$, where $a_j\in\mathbb{F}_q$, $j=1,2,3,4,5,6$.

This map Φ can be extended to R^n in an obvious way. The Hamming distance $d_H(x,y)$ between two vectors x and y over $\mathbb{F}_q$ is the Hamming weight of the vector $x-y$, that is, $d_H(x,y)=w_H(x-y)$. The Lee weight $w_L(x)$ of $x=(x_0, x_1, \cdots, x_{n-1})\in R^n$ is defined as $w_L(x)=w_H(\Phi(x))$. For any $x,y\in R^n$, the Lee distance between x and y is given by $d_L(x,y)=w_L(x-y)$. A linear code C of length n over R is an R-submodule of R^n. It is easy to verify that the Gray image of a linear code over R is a q-ary linear code.

According to the definition of Lee distance, we have the following lemma.

Lemma 1.1 The Gray map Φ is a distance-preserving map from (R^n, Lee distance) to ($\mathbb{F}_q^{6n}$, Hamming distance) and this map is also $\mathbb{F}_q$-linear.

Proof It is clear that $\Phi(x-y)=\Phi(x)-\Phi(y)$ for $x,y\in R^n$. Thus, $d_L(x,y)=w_L(x-y)=w_H(\Phi(x-y))=w_H(\Phi(x)-\Phi(y))=d_H(\Phi(x),\Phi(y))$. Let $x,y\in R^n$, $k_1,k_2\in\mathbb{F}_q$, then from the definition of Gray map, we have $\Phi(k_1x+k_2y)=k_1\Phi(x)+k_2\Phi(y)$. This means that Φ is $\mathbb{F}_q$-linear.

Similar to Lemma 3. 2 in Ref. [11] and combining Lemma 1. 1, we have the following lemma.

Lemma 1.2 Let C be a linear code of length n over R with rank k and minimum Lee distance d, then $\Phi(C)$ is a $[6n,k,d]$ linear code over $\mathbb{F}_q$.

Proof From Lemma 1.1, we see that $\Phi(C)$ is an $\mathbb{F}_q$-linear code. What is more, we can easily obtain that $\Phi(C)$ has dimension k and length $6n$ since Φ is a bijective map from R^n to $\mathbb{F}_q^{6n}$. Note that the Gray map Φ is a distance-preserving map. So $\Phi(C)$ has the same minimum distance d. Let C be a linear code over R. The dual $C^{\perp}$ of C consists of all vectors of R^n which are orthogonal to every codeword in C. A code C is said to be self-dual (resp. self-orthogonal) if $C=C^{\perp}$ (resp. $C\subseteq C^{\perp}$). Let $x=(x_0,x_1,\cdots,x_{n-1})$ and $y=(y_0,y_1,\cdots,y_{n-1})$ be any two vectors over R^n, we define the usual Euclidean inner product by $x\cdot y=\sum_{i=0}^{n-1}x_iy_i$. An important connection that we want to investigate is the relation between the dual and the Gray image of a code. The following theorem resolves this issue.

Theorem 1.1 Let C be a linear code of length n over R. If $C^{\perp}$ is its dual, then $\Phi(C^{\perp})=\Phi(C)^{\perp}$. Moreover, if C is self-dual, so is $\Phi(C)$ over $\mathbb{F}_q$.

Proof Let $c=(c_0,c_1,\cdots,c_{n-1})\in C$, where $c_i=c_{i1}+c_{i2}u+c_{i3}v+c_{i4}uv+c_{i5}v^2+c_{i6}uv^2$. Take $c'=(c'_0,c'_1,\cdots,c'_{n-1})\in C^{\perp}$, where $c'_i=c'_{i1}+c'_{i2}u+c'_{i3}v+c'_{i4}uv+c'_{i5}v^2+c'_{i6}uv^2$. Then we have $c=A_1+A_2u+A_3v+A_4uv+A_5v^2+A_6uv^2$ and $c'=B_1+B_2u+B_3v+B_4uv+B_5v^2+B_6uv^2$, where $A_j=(c_{0j},c_{1j},\cdots,c_{n-1j})$ and $B_j=(c'_{0j},c'_{1j},\cdots,c'_{n-1j})$ for $j=1,2,\cdots,6$. Since $c\cdot c'=0$ in R, then we have

$$A_1B_1+A_2B_2=0,\ A_1B_2+A_2B_1=0,$$

$$A_1B_3+A_2B_4+A_3B_1+A_3B_5+A_4B_2+A_4B_6+A_5B_3+A_6B_4=0,$$

$$A_1B_4+A_2B_3+A_3B_2+A_3B_6+A_4B_1+A_4B_5+A_5B_4+A_6B_3=0,$$

$$A_1B_5+A_2B_6+A_3B_3+A_4B_4+A_5B_1+A_5B_5+A_6B_2+A_6B_6=0,$$

$$A_1B_6+A_2B_5+A_3B_4+A_4B_3+A_5B_2+A_5B_6+A_6B_1+A_6B_5=0.$$

Note that $\Phi(c)\cdot\Phi(c')=0$, which implies $\Phi(C^{\perp})\subseteq\Phi(C)^{\perp}$. Since $|C\|C^{\perp}|=|\Phi(C)||\Phi(C)^{\perp}|=q^{6n}$ and $|\Phi(C^{\perp})|=|C^{\perp}|$, then we get $|\Phi(C^{\perp})|=|\Phi(C)^{\perp}|$. Hence $\Phi(C^{\perp})=\Phi(C)^{\perp}$. If C is self-dual, then $\Phi(C)=\Phi(C^{\perp})=\Phi(C)^{\perp}$.

2 Linear codes over *R*

By the Chinese Remainder Theorem, we have

$$R=(1-v^2)R\oplus(2^{-1}v+2^{-1}v^2)R\oplus(-2^{-1}v+2^{-1}v^2)R=(1-v^2)R_1\oplus(2^{-1}v+2^{-1}v^2)R_1\oplus(-2^{-1}v+2^{-1}v^2)R_1,$$

and $R_1=2^{-1}(1+u)\mathbb{F}_q\oplus2^{-1}(1-u)\mathbb{F}_q$. Hence $R=2^{-1}(1+u)(1-v^2)\mathbb{F}_q\oplus2^{-1}(1-u)(1-v^2)\mathbb{F}_q\oplus4^{-1}(1+u)(v+v^2)\mathbb{F}_q\oplus4^{-1}(1-u)(v+v^2)\mathbb{F}_q\oplus4^{-1}(1+u)(-v+v^2)\mathbb{F}_q\oplus4^{-1}(1-u)(-v+v^2)\mathbb{F}_q$. For the sake of convenience, we denote the elements in R by η_1, η_2, η_3, η_4, η_5, η_6 respectively, i.e., $\eta_1=2^{-1}(1+u)(1-v^2)$, $\eta_2=2^{-1}(1-u)(1-v^2)$, $\eta_3=4^{-1}(1+u)(v+v^2)$, $\eta_4=4^{-1}(1-u)(v+v^2)$, $\eta_5=4^{-1}(1+u)(-v+v^2)$, $\eta_6=4^{-1}(1-u)(-v+v^2)$. Note that η_j ($j=1,2,3,4,5,6$) are mutually orthogonal idempotents over R and $\sum_{j=1}^{6}\eta_j=1$. Let C be a linear code of length n over R. For $1\leqslant i\leqslant6$, define

$$C_i=\dot{x}_i\in\mathbb{F}_q^n\mid\exists\dot{x}_j\in\mathbb{F}_q^n,\ j=\{1,2,\cdots,6\}\backslash\{i\},\quad \text{s.t.}\ \sum_{i=1}^{6}\eta_i\dot{x}_i\in C\}.$$

Then C_i ($i=1,2,\cdots,6$) are all linear codes of length n over $\mathbb{F}_q$. Moreover, the code C of length n over R can be uniquely expressed as

$$C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6 \tag{1}$$

Let C, expressed as Eq.(1), be a linear code of length n with generator matrix G over R. Then, since C is an $\mathbb{F}_q$-module, the generator matrix G can be written as

$$G=\begin{pmatrix}\eta_1G_1\\ \eta_2G_2\\ \vdots\\ \eta_6G_6\end{pmatrix},$$

where G_1, G_2, G_3, G_4, G_5 and G_6 are the generator matrices of C_1, C_2, C_3, C_4, C_5 and C_6, respectively. Now, as an $\mathbb{F}_q$-module, the gray image of C under the Gray map Φ which is a module isomorphism, is an $\mathbb{F}_q$-subspace generated by $\Phi(G)$. So we can easily obtain the following corollary.

Corollary 2.1 Let C, expressed as (1), be a linear code of length n over R, then $d_H(\Phi(C))=\min\{d_H(C_1), d_H(C_2),\cdots, d_H(C_6)\}$.

We will show that the dual code $C^\perp$ of a code C over R is completely characterized by its associated codes $C_j^\perp$ for $j=1,2,3,4,5,6$.

Theorem 2.1 Let C, expressed as Eq.(1), be a linear code of length n over R, then

$$C^\perp=\eta_1C_1^\perp\oplus\eta_2C_2^\perp\oplus\eta_3C_3^\perp\oplus\eta_4C_4^\perp\oplus\eta_5C_5^\perp\oplus\eta_6C_6^\perp.$$

Moreover, C is self-dual if and only if $C_j(j=1,2,\cdots,6)$ are all self-dual over $\mathbb{F}_q$.

Example 2.1 Let C be a linear code of length 6 generated by the matrix G over $R=\mathbb{F}_5+u\mathbb{F}_5+v\mathbb{F}_5+uv\mathbb{F}_5+v^2\mathbb{F}_5+uv^2\mathbb{F}_5$, where

$$G=\begin{pmatrix}\eta_1G_1\\ \eta_2G_2\\ \vdots\\ \eta_6G_6\end{pmatrix},$$

and

$$G_1=\begin{pmatrix}1&2&0&0&0&0\\0&0&1&2&0&0\\0&0&0&0&1&2\end{pmatrix},$$

$$G_2=\begin{pmatrix}1&0&0&2&0&0\\0&1&0&0&2&0\\0&0&1&0&0&3\end{pmatrix},$$

$$G_3=\begin{pmatrix}1&0&0&1&2&2\\0&1&0&2&1&3\\0&0&1&2&3&1\end{pmatrix},$$

$$G_4=\begin{pmatrix}1&3&0&0&0&0\\0&0&1&3&0&0\\0&0&0&0&1&3\end{pmatrix},$$

$$G_5=\begin{pmatrix}1&0&0&1&3&3\\0&1&0&3&1&3\\0&0&1&3&3&1\end{pmatrix},$$

$$G_6=\begin{pmatrix}1&0&0&2&0&0\\0&1&0&0&3&0\\0&0&1&0&0&3\end{pmatrix}.$$

Then C is a self-dual code over R. Moreover, by Theorem 1.1, $\Phi(C)$ is a self-dual code over $\mathbb{F}_5$ with parameters $[36,18,2]$.

3 Skew cyclic codes over R

In the present section, we investigate the structural properties of skew cyclic codes over R with automorphism θ_i. In the commutative case, if $(n,q)=1$, then every cyclic code of length n over $\mathbb{F}_q$ has a unique idempotent generator. However, the skew polynomial ring $\mathbb{F}_q[x,\theta_i]$ does not need to be a unique factorization ring. Note that if $(n,t_i)=1$, then the factorization of x^n-1 in $\mathbb{F}_q[x,\theta_i]$ is unique, where t_i denotes the order of the automorphism θ_i (see Ref.[9]). Now, we give the concept of skew cyclic codes over R.

Definition 3.1 Let R be a ring and θ_i be an automorphism of R. A linear code C of length n over R is a skew cyclic code with the property that

$$c=(c_0,c_1,\cdots,c_{n-1})\in C\Rightarrow$$
$$\sigma(c)=(\theta_i(c_{n-1}),\theta_i(c_0),\cdots,\theta_i(c_{n-2}))\in C,$$

where $\sigma(c)$ is a skew cyclic shift of c.

The skew polynomial representation of a code C is defined to be $\{c_0+c_1x+\cdots+c_{n-1}x^{n-1}\mid(c_0,c_1,\cdots,c_{n-1})\in C\}$. For the sake of convenience, it will be regarded as C itself. The necessary and sufficient conditions for a linear code to be a skew cyclic code are given as follows.

Lemma 3.1[12] A linear code of length n over $\mathbb{F}_q$ is a skew cyclic code with respect to automorphism θ if and only if it is a left $\mathbb{F}_q[x,\theta]$-submodule of $\mathbb{F}_q[x,\theta]/(x^n-1)$. Moreover, if C is a left submodule of $\mathbb{F}_q[x,\theta]/(x^n-1)$, then C is generated by a monic polynomial $g(x)$ which is a right divisor of x^n-1 in $\mathbb{F}_q[x,\theta]$.

We will show that a skew cyclic code over R is completely characterized by its associated codes C_j for $j=1,2,3,4,5,6$, and vice versa.

Theorem 3.1 Let C be a linear code over R of length n and $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$, where C_1, C_2, C_3, C_4, C_5 and C_6 are all linear codes of length n over $\mathbb{F}_q$, then C is a skew cyclic code with respect to the automorphism θ_i if and only if C_1, C_2, C_3, C_4, C_5 and C_6 are skew cyclic codes over $\mathbb{F}_q$ with respect to the automorphism θ_i.

Proof For simplicity, the vector $(x^1, x^2, \cdots, x^n)$ ($(x_v^1, x_v^2, \cdots, x_v^n)$, $\sim v\in\backslash\mathbb{Z}$) denotes the codeword of a code of length n.

Let $(x_j^1, x_j^2, \cdots, x_j^n)\in C_j$ for $j=1,2,3,4,5,6$. Assume that $x^i=\sum_{j=1}^{6}\eta_j x_j{}^i$ for $i=1,2,\cdots,n$, then the vector $x=(x^1,x^2,\cdots,x^n)\in C$. If C is a skew cyclic code, then $(\theta_i(x^n),\theta_i(x^1),\cdots,\theta_i(x^{n-1}))\in C$. Note that $\sigma(x)=(\theta_i(x^n),\theta_i(x^1),\cdots,\theta_i(x^{n-1}))=\sum_{j=1}^{6}\eta_j((x_j^n)^{pi},(x_j^1)^{pi},\cdots,(x_j{}^{n-1})^{pi})$. So $(\theta_i(x_j^n), \theta_i(x_j^1), \cdots, \theta_i(x_j{}^{n-1}))=((x_j^n)^{pi}, (x_j^1)^{pi}, \cdots, (x_j{}^{n-1})^{pi})\in C_j$, which implies that C_j are all skew cyclic codes over $\mathbb{F}_q$ for $j=1,2,3,4,5,6$.

On the other hand, suppose that C_j are all skew cyclic codes over $\mathbb{F}_q$ for $j=1,2,3,4,5,6$, and $y=(y^1,y^2,\cdots,y^n)\in C$, where $y^i=\sum_{j=1}^{6}\eta_j y_j{}^i$ for $i=1,2,\cdots,n$, then $(y_j^1,y_j^2,\cdots,y_j^n)\in C_j$ for $j=1,2,\cdots,6$. Note that $(\theta_i(y_j^n),\theta_i(y_j^1),\cdots,\theta_i(y_j{}^{n-1}))=((y_j^n)^{pi},(y_j^1)^{pi},\cdots,(y_j{}^{n-1})^{pi})\in C_j$ for $j=1,2,\cdots,6$. Thus $\sigma(y)=(\theta_i(y^n),\theta_i(y^1),\cdots,\theta_i(y^{n-1}))=\sum_{j=1}^{6}\eta_j((y_j^n)^{pi},(y_j^1)^{pi},\cdots,(y_j{}^{n-1})^{pi})\in\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6=C$. Therefore C is a skew cyclic code over R.

In view of the previous theorem, the following corollary can be easily obtained.

Corollary 3.1 If C is a skew cyclic code over R, then the dual code $C^\perp$ is also skew cyclic.

Proof By Theorem 2.1, we have $C^\perp=\eta_1C_1^\perp\oplus\eta_2C_2^\perp\oplus\eta_3C_3^\perp\oplus\eta_4C_4^\perp\oplus\eta_5C_5^\perp\oplus\eta_6C_6^\perp$. According to Corollary 18 in Ref.[2], we know that the dual code of every skew cyclic code over $\mathbb{F}_q$ is also skew cyclic. Hence the dual code $C^\perp$ is a skew cyclic code from Theorem 3.1.

Next, we give the definition of skew quasi cyclic codes over R.

Definition 3.2 Let C be a linear code of length n over $\mathbb{F}_q$ and $(c^1|c^2|\cdots|c^l)$ be a codeword in C divided into l equal parts of length s where $n=sl$. If $(\sigma(c^1)|\sigma(c^2)|\cdots|\sigma(c^l))\in C$, then the linear code C which is permutation equivalent to C is called a skew quasi cyclic code of index l or skew l-quasi cyclic code.

Based on the definition of skew quasi cyclic codes, we have the following corollary.

Corollary 3.2 If C is a skew cyclic code of length n over R, then $\Phi(C)$ is a skew 6-quasi cyclic code of length $6n$ over $\mathbb{F}_q$.

Proof The result follows from the Definition 3.2 and the definition of Gray map Φ.

We are now ready to consider the generator polynomial of a skew cyclic code of length n over R.

Theorem 3.2 Let $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_1C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$ be a skew cyclic code of length n over R and assume that $C_j=\langle g_j(x)\rangle$ for $j=1,2,3,4,5,6$, then $C=\langle\eta_1g_1(x),\eta_2g_2(x),\eta_3g_3(x),\eta_4g_4(x),\eta_5g_5(x),\eta_6g_6(x)\rangle$ and $|C|=q^{6n-\sum_{j=1}^{6}\deg(g_j(x))}$.

Proof For the sake of convenience, we denote the ideal $\langle\eta_1g_1(x),\eta_2g_2(x),\eta_3g_3(x),\eta_4g_4(x),\eta_5g_5(x),\eta_6g_6(x)\rangle$ by I. In the following, we prove $C=I$. Since $C_j=\langle g_j(x)\rangle$, $|C_j|=q^{n-\deg(g_j(x))}$, $j=1,2,3,4,5,6$, and $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$, then $C=\left\{\sum_{j=1}^{6}\eta_jk_j(x)g_j(x)\mid k_j(x)\in\mathbb{F}_q[x,\theta],1\leqslant j\leqslant 6\right\}$.

So $C\subseteq I$. Conversely, let us take $\sum_{j=1}^{6}\eta_j l_j(x)g_j(x)\in I$, where $l_j(x)\in R[x,\theta_i]/(x^n-1)$ for $j=1,2,3,4,5,6$, then $\eta_j l_j(x)=\eta_j k_j(x)$ for some $k_j(x)\in\mathbb{F}_q[x,\theta_i]$ for $j=1,2,\cdots,6$. Hence $I\subseteq C$. Therefore, $C=I$. Since $|C|=|C_1\|C_2\|C_3\|C_4\|C_5\|C_6|$, then we have $|C|=q^{6n-\sum_{j=1}^{6}deg(g_j(x))}$.

The next theorem shows that the skew cyclic codes over R are principally generated.

Theorem 3.3 Let $C_j=\langle g_j(x)\rangle$, where $g_j(x)$ are monic polynomials over $\mathbb{F}_q$ for $j=1,2,3,4,5,6$. Let C, expressed as (1), be a skew cyclic code over R, then there exists a unique polynomial $g(x)\in R[x,\theta_i]$ such that $C=\langle g(x)\rangle$ and $g(x)$ is a right divisor of x^n-1, where $g(x)=\sum_{j=1}^{6}\eta_j g_j(x)$.

Proof Let $g(x)=\sum_{j=1}^{6}\eta_j g_j(x)$, then it is easy to verify that $\langle g(x)\rangle\subseteq C$. Conversely, $\eta_j g_j(x)=\eta_j g(x)$, where $1\leqslant j\leqslant 6$, which implies that $C\subseteq\langle g(x)\rangle$. Thus $C=\langle g(x)\rangle$. Since $g_j(x)$ are monic right divisors of x^n-1 in $\mathbb{F}_q[x,\theta_i]$, then there are $h_j(x)$ in $\mathbb{F}_q[x,\theta_i]/(x^n-1)$ such that $x^n-1=h_i(x)g_i(x)$, $1\leqslant i\leqslant 6$. Thus $[2^{-1}\theta_i(2)(\eta_1h_1(x)+\eta_2h_2(x))+4^{-1}\theta_i(4)(\eta_3h_3(x)+\eta_4h_4(x)+\eta_5h_5(x)+\eta_6h_6(x))]\cdot g(x)=2^{-1}\theta_i(2)(\eta_1\theta_i(\eta_1)h_1(x)g_1(x)+\eta_2\theta_i(\eta_2)h_2(x)g_2(x))+4^{-1}\theta_i(4)(\eta_3\theta_i(\eta_3)h_3(x)g_3(x)+\eta_4\theta_i(\eta_4)h_4(x)g_4(x)+\eta_5\theta_i(\eta_5)h_5(x)g_5(x)+\eta_6\theta_i(\eta_6)h_6(x)g_6(x))=(\eta_1+\eta_2+\eta_3+\eta_4+\eta_5+\eta_6)(x^n-1)=x^n-1$. Hence $g(x)$ is a right divisor of x^n-1.

The following corollary is an immediate consequence of the above theorem.

Corollary 3.3 Every left submodule of $R[x,\theta_i]/(x^n-1)$ is principally generated.

Let $g(x)=\sum_{i=0}^{r}g_ix^i$ and $h(x)=\sum_{i=0}^{n-r}h_ix^i$ be polynomials in $\mathbb{F}_q[x,\theta_i]$ such that $x^n-1=h(x)g(x)$ and C be the skew cyclic code generated by $g(x)$ in $\mathbb{F}_q[x,\theta_i]/(x^n-1)$. Then the dual code of C is a skew cyclic code generated by the polynomial $\widetilde{H}(x)=h_{n-r}+\theta_i(h_{n-r-1})x+\cdots+\theta_i{}^{n-r}(h_0)x^{n-r}$ (see Ref.[5], Corollary 18). We are now ready to prove the following corollary for the generator polynomial and the cardinality of the dual code of a skew cyclic code over R.

Corollary 3.4 Let $C_j=\langle g_j(x)\rangle$ be skew cyclic codes over $\mathbb{F}_q$, where $x^n-1=h_j(x)g_j(x)$ in $\mathbb{F}_q[x,\theta_i]$ for $j=1,2,\cdots,6$. If $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$, then $C^{\perp}=\langle h(x)\rangle$, where $h(x)=\sum_{j=1}^{6}\eta_j\tilde{h}_j(x)$ and $|C^{\perp}|=q^{\sum_{j=1}^{6}\deg(g_j(x))}$.

Proof By Theorem 2.1, we have $C^{\perp}=\eta_1C_1^{\perp}\oplus\eta_2C_2^{\perp}\oplus\eta_3C_3^{\perp}\oplus\eta_4C_4^{\perp}\oplus\eta_5C_5^{\perp}\oplus\eta_6C_6^{\perp}$. Since $C_j^{\perp}=\langle h_j(x)\rangle$ for $j=1,2,3,4,5,6$, we conclude by Theorem 3.3 that $C^{\perp}=\langle h(x)\rangle$.

In order to study the idempotent generators of skew cyclic codes over R, we need the following two lemmas which can be found in Ref.[9].

Lemma 3.2[9] Let $g(x)\in\mathbb{F}_q[x,\theta_i]$ be a monic right divisor of x^n-1. If $(n,t_i)=1$, then $g(x)\in\mathbb{F}_p[x,\theta_i]$, where $t_i=m/i$ denotes the order of the automorphism θ_i.

Lemma 3.3[9] Let $g(x)\in\mathbb{F}_q[x,\theta_i]$ be a monic right divisor of x^n-1 and $C=\langle g(x)\rangle$. If $(n,q)=1$ and $(n,t_i)=1$, then there exists an idempotent polynomial $e(x)\in\mathbb{F}_q[x,\theta_i]/(x^n-1)$ such that $C=\langle e(x)\rangle$.

Now, we give the idempotent generators of skew cyclic codes over R.

Corollary 3.5 Let $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$ be a skew cyclic code of length n over R and $(n,q)=1$, $(n,t_i)=1$. Then C_i has the idempotent generators $e_i(x)$, $i=1,2,3,4,5,6$. Moreover, $e(x)=\eta_1e_1(x)+\eta_2e_2(x)+\eta_3e_3(x)+\eta_4e_4(x)+\eta_5e_5(x)+\eta_6e_6(x)$ is an idempotent generator of C, that is, $C=\langle e(x)\rangle$.

Proof In the light of Theorem 3.3 and Lemma 3.3, the proof follows.

The following theorem gives the number of skew cyclic codes of length n over R.

Theorem 3.4 Let $(n,t_i)=1$ and $x^n-1=\prod_{i=1}^{r}p_i^{si}(x)$ where $p_i(x)\in\mathbb{F}_q[x,\theta_i]$ is irreducible. Then the number of skew cyclic codes of length n over R is $\prod_{i=1}^{r}(s_i+1)^6$.

Proof In view of Lemma 3.2, if $(n,t_i)=1$, then $p_i(x) \in \mathbb{F}_p[x, \theta_i]$. In this case the number of skew cyclic codes of length n over $\mathbb{F}_q$ is $\prod_{i=1}^{r}(s_i+1)$. Since $C=\eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$, then $\prod_{i=1}^{r}(s_i+1)^6$ is the number of skewcyclic codes of length n over R.

Note that when $(n, t_i) \neq 1$ in Theorem 3.4, the factorization of x^n-1 is not unique in $\mathbb{F}_q[x, \theta_i]$, therefore we can not say anything certain about the number of skew cyclic codes in this case. Now, we conclude this section with the following example.

Example 3.1 Let γ be the generator of the multiplicative group of $\mathbb{F}_9$, where γ is a root of a primitive polynomial x^2+x+2 over $\mathbb{F}_3$. And θ be the Frobenius automorphism over $\mathbb{F}_9$, i.e. $\theta(\Lambda)=\Lambda^3$ for any $\Lambda \in \mathbb{F}_9$. Then $x^6-1=(2+(2+\gamma)x+(1+2\gamma)x^3+x^4)(1+(2+\gamma)x+x^2)=(2+x+(2+2\gamma)x^2+x^3)(1+x+2\gamma x^2+x^3) \in \mathbb{F}_9[x, \theta]$. Let $g_1(x)=g_2(x)=g_3(x)=2+(2+\gamma)x+(1+2\gamma)x^3+x^4$ and $g_4(x)=g_5(x)=g_6(x)=2+x+(2+2\gamma)x^2+x^3$, then $C_1=\langle g_1(x)\rangle$, $C_2=\langle g_2(x)\rangle$ and $C_3=\langle g_3(x)\rangle$ are skew cyclic codes of length 6 over $\mathbb{F}_9$ with dimensions 4; $C_4=\langle g_4(x)\rangle$, $C_5=\langle g_5(x)\rangle$ and $C_6=\langle g_6(x)\rangle$ are skew cyclic codes of length 6 over $\mathbb{F}_9$ with dimensions 3. Also if we take $g(x)=\eta_1 g_1(x)+\eta_2 g_2(x)+\eta_3 g_3(x)+\eta_4 g_4(x)+\eta_5 g_5(x)+\eta_6 g_6(x)$, then C is a skew cyclic code of length 6 over $\mathbb{F}_9+u\mathbb{F}_9+v\mathbb{F}_9+uv\mathbb{F}_9+v^2\mathbb{F}_9+uv^2\mathbb{F}_9$. Thus the Gray image $\Phi(C)$ of C is a $[36, 21, 4]$ code over $\mathbb{F}_9$.

4 Conclusion

In this paper, we studied the structural properties of skew cyclic codes over the ring $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q+v^2\mathbb{F}_q+uv^2\mathbb{F}_q$ by taking the automorphism θ_i. We proved that the gray image of a skew cyclic code of length n over R was a skew 6-quasi cyclic code of length $3n$ over $\mathbb{F}_q$. It was also shown that skew cyclic codes over R were principally generated. Further, we obtained idempotent generators of skew cyclic codes over R. Last, we gave the number of skew cyclic codes of length n over R under certain conditions. Note that this paper included Ref.[10-11] as special cases, because rings in Ref.[10-11] are subrings of the ring R in this paper.

References

[1] BOUCHER D, GEISELMANN W, ULMER F. Skew-cyclic codes [J]. Applicable Algebra Engineering Communication & Computing, 2007, 18(4) 379-389.

[2] BOUCHER D, ULMER F. Coding with skew polynomial ring[J]. Journal of Symbolic Computation, 2009, 44(12): 1644-1656.

[3] CAO Y L. Quasi-cyclic codes of index 2 and skew polynomial rings over finite fields[J]. Finite Fieids and Their Applications, 2014, 27: 143-158.

[4] BOUCHER D, ULMER F. Self-dual skew codes and factorization of skew polynomials [J]. Journal of Symbolic Computation, 2014, 60(1): 47-61.

[5] ABUALRUB T, GHRAYEB A, AYDIN N, et al. On the construction of skew quasi-cyclic codes[J]. IEEE Transactions on Information Theory, 2010, 56(5): 2081-2090.

[6] JITMAN S, LING S, UDOMKAVANICH P. Skew constacyclic codes over finite chain rings[J]. Advances in Mathematics Communications, 2010, 6(1): 39-63.

[7] AYDIN N, ABUALRUB T, SENEVIRATNE P. On θ-cyclic codes over F_2+vF_2[J]. Australian Journal of Combinatorics, 2012, 54: 115-126.

[8] GAO J. Skew cyclic codes over F_p+vF_p[J]. Journal of applied mathematics & informatics, 2013, 31(3-4): 337-342.

[9] GURSOY F, SIAP I, YILDIZ B. Construction of skew cyclic codes over F_q+vF_q[J]. Advances in Mathematics of Communications, 2014, 8(3): 313-322.

[10] ASHRAF M, GHULAM M. On skew cyclic codes over F_3+vF_3[J]. International Journal of Information & Coding Theory, 2014, 2(4): 218-225.

[11] SHI M J, YAO T, ALAHMADI A, et al. Skew cyclic codes over $F_p+vF_p+v^2F_q$[J]. The Institute of Electronics, Information and Communication Engineers, 2015, 98(8): 1845-1848.

[12] YAO T, SHI M J, SOLÉ P. Skew cyclic codes over $F_p+uF_p+vF_q+uvF_q$[J]. Journal of Algebra Combinatorics Discrete Structures & Applications, 2015, 2(3): 163-168.

[13] SIAP I, ABUALRUB T, AYDIN N, et al. Skew cyclic codes of arbitrary length[J]. International Journal of Information & Coding Theory, 2011, 2(1): 10-20.