On skew cyclic codes over $F_q + vF_q + v^2F_q$

Mohammad Ashraf[1] and Ghulam Mohammad[2]

[1]Department of Mathematics
Aligarh Muslim University
Aligarh -202002, U.P.(India)
[2]Department of Applied Sciences
The NorthCap University
Gurugram-122017, Haryana(India)

E-mail: mashraf80@hotmail.com[1], mohdghulam202@gmail.com[2]

Abstract

In the present paper, we study skew cyclic codes over the ring $F_q + vF_q + v^2F_q$, where $v^3 = v,\ q = p^m$ and p is an odd prime. The structural properties of skew cyclic codes over $F_q + vF_q + v^2F_q$ have been studied by using decomposition method. By defining a Gray map from $F_q+vF_q+v^2F_q$ to F_q^3, it has been proved that the Gray image of a skew cyclic code of length n over $F_q+vF_q+v^2F_q$ is a skew 3-quasi cyclic code of length $3n$ over F_q. Further, it is shown that the skew cyclic codes over $F_q + vF_q + v^2F_q$ are principally generated. Finally, the idempotent generators of skew cyclic codes over $F_q + vF_q + v^2F_q$ have also been studied.

2010 Mathematics Subject Classification. **94B05**. 94B15
Keywords. Dual codes, Quasi cyclic codes, Skew polynomial rings, Skew cyclic codes, Idempotent generators.

1 Introduction

In the last decade of the twentieth century a great deal of attention has been given to the study of linear codes over finite rings because of their new role in algebraic coding theory and their successful applications. The class of cyclic codes is a very important class of linear codes from both theoretical and practical point of view which are easier to implement due to their rich algebraic structure. Cyclic codes have been studied for the last six decades. Based on these facts, cyclic codes have become one of the most important class in coding theory. A landmark paper by Hammons, et al. [12] discovered that some good nonlinear codes over $\mathbb{Z}_2$ can be viewed as binary images under a Gray map of linear cyclic codes over $\mathbb{Z}_4$. But all this work is restricted to codes that are defined in a commutative ring.

Boucher et al. [6], [7] and [8] studied the structure of skew cyclic codes over a non commutative ring $F[x, \theta]$, called skew polynomial ring, where F is a finite field and θ is a field automorphism of F. They generalized the class of linear and cyclic codes to the class of skew cyclic codes by using the ring $F[x, \theta]$, where the generator polynomials of skew cyclic codes come from the ring $F[x, \theta]$. They also gave some examples of skew cyclic codes with Hamming distances larger than the best known linear codes with the same parameters. Later on, Abualrub et al. [1] and Bhaintwal [5], defined skew quasi cyclic codes over these classes of rings. The main motivation of studying codes in this setting is that polynomials in skew polynomial rings exhibit many factorizations and hence there are many ideals in skew polynomial ring than in the commutative ring. But all this work is restricted to the condition that the order of the automorphism must be a factor of the length of

Tbilisi Mathematical Journal 11(2) (2018), pp. 35–45.
Tbilisi Centre for Mathematical Sciences.

Received by the editors: 16 June 2017.
Accepted for publication: 25 January 2018.

the code. In [15], Siap, et al. removed this condition and they studied the structural properties of skew cyclic codes of arbitrary length over finite fields. A lot of work has been done in this direction (see references [2, 3, 9]).

Recently, Jitman et al. [13] defined skew constacyclic codes by defining the skew polynomial ring with coefficients from finite chain rings, especially the ring $F_{p^m} + uF_{p^m}$ where $u^2 = 0$. Gursoy et al. [11] investigated the structural properties of skew cyclic codes through the decomposition method over $F_q + vF_q$, where $v^2 = v$ and $q = p^m$. Very recently, the authors [3] studied the structural properties of skew cyclic codes over the ring $F_3 + vF_3$ with $v^2 = 1$ by considering the automorphism as; $\theta : v \mapsto -v$. They proved that skew cyclic codes over $F_3 + vF_3$ are equivalent to either cyclic codes or quasi cyclic codes. Further, the authors [4] obtained skew quasi cyclic codes over F_q from the skew cyclic codes over the ring $F_q + vF_q$. In the present paper, we study skew cyclic codes over the ring $F_q + vF_q + v^2F_q$, where $v^3 = v,\ q = p^m$ and p is an odd prime. Some skew quasi cyclic codes of index 3 over F_q from skew cyclic codes over $F_q + vF_q + v^2F_q$ have also been obtained.

Throughout the paper R will denote the ring $F_q + vF_q + v^2F_q$ with $v^3 = v,\ q = p^m$ and p is an odd prime. Consider the automorphism $\theta_t : R \longrightarrow R$ such that $\theta_t(a+vb+v^2c) = a^{p^t} + vb^{p^t} + v^2c^{p^t}$. It is to be noted that θ_1 is the Frobenius automorphism of F_q and $\theta_t = \theta_1^t$. In this paper, we will use the automorphism θ_t instead of the automorphism $v \mapsto 1 - v$ which was used by Gao in [9].

2 Preliminaries

Let $R = F_q + vF_q + v^2F_q$, where $q = p^m$ and p is an odd prime. R is a commutative and non-chain ring with characteristic p which contains q^3 elements. The ring is endowed with the natural addition and multiplication with the property $v^3 = v$ and it can be viewed as the quotient ring $F_q[v]/\langle v^3 - v\rangle$. The elements of R can be uniquely written as $a + vb + v^2c$, where $a,\ b,\ c \in F_q$. It is a semi-local ring having three maximal ideals $\langle v\rangle,\ \langle v-1\rangle$ and $\langle v+1\rangle$. It is easy to see that each ideal of this ring is principally generated, therefore, it is a principal ideal ring.

Define a mapping $\theta_t : R \longrightarrow R$ such that $\theta_t(a+vb+v^2c) = a^{p^t} + vb^{p^t} + v^2c^{p^t}$, for all $a,\ b,\ c \in F_q$. 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:

$$\theta_t : F_q \longrightarrow F_q$$

$$a \mapsto a^{p^t}.$$

It may be noted that the order of this automorphism is $|\langle\theta_t\rangle| = m/t$ and the subring $F_{p^t} + vF_{p^t} + v^2F_{p^t}$ of R is invariant under θ_t.

Definition 2.1. For a given automorphism θ_t of R, the set $R[x, \theta_t] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n |\ a_i \in R, n \geq 0\}$ of formal polynomials forms a ring under usual addition of polynomials and multiplication is defined by the rule $(ax^i)(bx^j) = a\theta_t^i(b)x^{i+j}$. The ring $R[x, \theta_t]$ is called skew polynomial ring over R.

It can be easily seen that the ring $R[x, \theta_t]$ is non-commutative unless θ_t is the identity automorphism on R. Therefore, when an ideal of $R[x, \theta_t]$ is considered, one should specify whether it is a right ideal or a left ideal. The skew polynomial ring $R[x, \theta_t]$ is not left or right Euclidean. However, the division algorithm holds for some polynomials whose leading coefficients are invertible (for detail see references [7] and [13]).

3 Gray map and linear codes over R

Gao [10], studied linear codes over the ring $F_p + uF_p + u^2F_p$, where $u^3 = u$ and p is an odd prime. Here, we generalize his study to linear codes over the ring R. Let R^n be the set of all n-tuples over R, then a nonempty subset C of R^n is called a code of length n over R. C is called linear code of length n over R if it is an R-submodule of R^n. Elements of C are called codewords and therefore each codeword c in such a code C is just an n-tuple of the form $x = (x_0, x_1, \cdots, x_{n-1}) \in R^n$.

The Hamming weight $w_H(x)$ of a codeword $x = (x_0, x_1, \cdots, x_{n-1}) \in R^n$ is the number of nonzero components. The minimum weight $w_H(C)$ of a code C is the smallest weight among all its nonzero codewords. For $x = (x_0, x_1, \cdots, x_{n-1}),\ y = (y_0, y_1, \cdots, y_{n-1}) \in R^n$,
$d_H(x, y) = |\{i \mid x_i \neq y_i\}|$ is called the Hamming distance between x and $y \in R^n$ and is denoted by

$$d_H(x, y) = w_H(x - y).$$

The minimum Hamming distance between distinct pairs of codewords of a code C is called the minimum distance of C and is denoted by $d_H(C)$ or shortly d_H.

Now, we define the Lee weight of an element $r = a + vb + v^2c \in R$ as follows:

$$w_L(r) = w_H(a, a + b + c, a - b + c),$$

where w_H denotes the usual Hamming weight on F_q. Let $x = (x_0, x_1, \cdots, x_{n-1})$ be a vector in R^n. Then the Lee weight of x is the rational sum of Lee weights of its components, that is, $w_L(x) = \sum\limits_{i=0}^{n-1} w_L(x_i)$. For any elements $x, y \in R^n$, the Lee distance is given by $d_L(x, y) = w_L(x - y)$. The minimum Lee distance of a code C is the smallest nonzero Lee distance between all pairs of distinct codewords. The minimum Lee weight of C is the smallest nonzero Lee weight among all codewords. If C is linear, then the minimum Lee distance is the same as the minimum Lee weight.

The Gray map φ from R to F_q^3 is defined as $\varphi(a + vb + v^2c) = (a, a + b + c, a - b + c)$. It can be easily seen that φ is linear. The Gray map φ can be extended to R^n in a natural way, that is, $\varphi : R^n \longrightarrow F_q^{3n}$ such that $\varphi(x_0, x_1, \cdots, x_{n-1}) = (a_0, a_0 + b_0 + c_0, a_0 - b_0 + c_0, \cdots, a_{n-1}, a_{n-1}+b_{n-1}+c_{n-1}, a_{n-1}-b_{n-1}+c_{n-1})$, where $x_i = a_i+vb_i+v^2c_i$ for $i = 0, 1, \cdots, n-1$.

The following property is obvious from the definition of the Gray map:

Proposition 3.1. The Gray map φ is a distance-preserving map or isometry from R^n(Lee distance) to F_q^{3n}(Hamming distance) and it is also F_q-linear.

For a code C over R, define

$$C_1 = \{a \in F_q^n \mid a + vb + v^2c \in C \text{ some } b, c \in F_q^n\},$$

$$C_2 = \{a + b + c \in F_q^n \mid a + vb + v^2c \in C\},$$

and

$$C_3 = \{a - b + c \in F_q^n \mid a + vb + v^2c \in C\}.$$

If C is linear code of length n over R, then $C_1,\ C_2$ and C_3 are all linear codes of length n over F_q. Moreover, the linear code C of length n over R can be uniquely expressed as

$$C = (1 - v^2)C_1 \oplus \frac{p+1}{2}(v^2 + v)C_2 \oplus \frac{p+1}{2}(v^2 - v)C_3.$$

A generator matrix of C is a matrix whose rows generate C. Let

$$C = (1 - v^2)C_1 \oplus \frac{p+1}{2}(v^2 + v)C_2 \oplus \frac{p+1}{2}(v^2 - v)C_3$$

be a linear code of length n over R with generator matrix G. Then G can be written as

$$G = \begin{pmatrix} (1 - v^2)G_1 \\ \\ \frac{p+1}{2}(v^2 + v)G_2 \\ \\ \frac{p+1}{2}(v^2 - v)G_3 \end{pmatrix},$$

where $G_1,\ G_2$ and G_3 are the generator matrices of $C_1,\ C_2$ and C_3 respectively.

Let $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$ be two elements of R^n. Then the Euclidean inner product of x and y in R^n is defined as

$$x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}.$$

The dual code $C^\perp$ of C is defined as

$$C^\perp = \{x \in R^n | \ x \cdot y = 0, \text{ for all } y \in C\}.$$

A code C is called self-orthogonal if $C \subseteq C^\perp$ and self dual if $C = C^\perp$.

Now, we give some results on linear codes over R, which are the generalization of results on linear codes over $F_p + vF_p + v^2F_p$. So, we are omitting the proofs of the results.

Theorem 3.2. If $C = (1 - v^2)C_1 \oplus \frac{p+1}{2}(v^2 + v)C_2 \oplus \frac{p+1}{2}(v^2 - v)C_3$ is a linear code of length n over R, then $\varphi(C) = C_1 \otimes C_2 \otimes C_3$ and $|C| = |C_1||C_2||C_3|$.

Corollary 3.3. Let $C = (1-v^2)C_1 \oplus \frac{p+1}{2}(v^2+v)C_2 \oplus \frac{p+1}{2}(v^2-v)C_3$ be a linear code of length n over R, where C_i is a linear code with dimension k_i and minimum Hamming distance $d(C_i)$ for $i = 1,2,3$. Then $\varphi(C)$ is a linear code with parameters $[3n, k_1+k_2+k_3,\ min\{d(C_1), d(C_2), d(C_3)\}]$ over F_q.

One of the properties of the Gray map we defined is that it preserves the duality as given in the following lemma:

Lemma 3.4. Let $C^\perp$ be the dual code of C over R. Then $\varphi(C^\perp) = \varphi(C)^\perp$. In particular, if C is self-dual, then so is $\varphi(C)$.

Proof. Let $x_1 = a_1 + vb_1 + v^2c_1$ and $x_2 = a_2 + vb_2 + v^2c_2 \in C$, where $a_1, b_1, c_1, a_2, b_2, c_2 \in F_q^n$. Now by Euclidean inner product of x_1 and x_2, we have

$$\begin{aligned} x_1 \cdot x_2 &= (a_1 + vb_1 + v^2c_1) \cdot (a_2 + vb_2 + v^2c_2) \\ &= a_1a_2 + v(a_1b_2 + a_2b_1 + b_1c_2 + b_2c_1) + v^2(a_1c_2 + a_2c_1 + b_1b_2 + c_1c_2). \end{aligned}$$

Since C is a self-dual code, $C = C^\perp$, we find that $a_1a_2 = a_1b_2 + a_2b_1 + b_1c_2 + b_2c_1 = a_1c_2 + a_2c_1 + b_1b_2 + c_1c_2 = 0$. Now

$$\varphi(x_1)\varphi(x_2) = (a_1, a_1 + b_1 + c_1, a_1 - b_1 + c_1)(a_2, a_2 + b_2 + c_2, a_2 - b_2 + c_2) = 0.$$

Thus $\varphi(C^\perp) \subseteq \varphi(C)^\perp$. On the other hand let $|C| = (q)^{k_1+k_2+k_3}$ and C is of length n. Then $\varphi(C)$ has the parameters $[3n, k_1 + k_2 + k_3]$. Since $|\varphi(C)| = |C|$, $|\varphi(C)^\perp| = (q)^{3n-(k_1+k_2+k_3)}$. Further $|\varphi(C^\perp)| = |C^\perp| = q^{3n}/|C| = q^{3n-(k_1+k_2+k_3)}$. Hence $\varphi(C^\perp) = \varphi(C)^\perp$.

In view of the previous lemma, the following theorem can be easily obtained:

Theorem 3.5. Let C be a linear code of length n over R and let $\varphi(C) = C_1 \otimes C_2 \otimes C_3$. Then C can be uniquely expressed as $C = (1-v^2)C_1 \oplus \frac{p+1}{2}(v^2+v)C_2 \oplus \frac{p+1}{2}(v^2-v)C_3$. Furthermore, if $\varphi(C^\perp) = C_1^\perp \otimes C_2^\perp \otimes C_3^\perp$, then $C^\perp = (1-v^2)C_1^\perp \oplus \frac{p+1}{2}(v^2+v)C_2^\perp \oplus \frac{p+1}{2}(v^2-v)C_3^\perp$.

4 Skew cyclic codes over R

In the present section, we study skew cyclic codes over R. Let θ_t be an automorphism on R given by $\theta_t(a + vb + v^2c) = a^{p^t} + vb^{p^t} + v^2c^{p^t}$. Then a linear code C of length n over R is called a skew cyclic code or θ_t-cyclic code if it satisfies the property $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ implies $\sigma(c) = (\theta_t(c_{n-1}), \theta_t(c_0), \cdots, \theta_t(c_{n-2})) \in C$, where $\sigma(c)$ denotes the skew cyclic shift of c.

In [15], it was shown that a linear code C of length n over F_q is a skew cyclic code with respect to automorphism θ if and only if it is a left $F_q[x,\theta]$-submodule of $F_q[x,\theta]/\langle x^n - 1\rangle$. Moreover, if C is a left submodule of $F_q[x,\theta]/\langle x^n - 1\rangle$, then C is generated by a monic polynomial $g(x)$ which is a right divisor of $x^n - 1$ in $F_q[x,\theta]$.

The method which we use in this section is same as the method used by Gao in [10] over the ring $F_p + vF_p + v^2F_p$ with $v^3 = v$. The main difference in our case is that the ring $R[x, \theta_t]$ is non-commutative.

Theorem 4.1. Let $C = (1 - v^2)C_1 \oplus \frac{p+1}{2}(v^2 + v)C_2 \oplus \frac{p+1}{2}(v^2 - v)C_3$ be a linear code of length n over R. Then C is a skew cyclic code over R with respect to automorphism θ_t if and only if C_1, C_2 and C_3 are skew cyclic codes of length n over F_q with respect to same automorphism θ_t.

Proof. For any $r = (r_0, r_1, \cdots, r_{n-1}) \in C$, we can write its components as $r_i = (1 - v^2)a_i + \frac{p+1}{2}(v^2 + v)b_i + \frac{p+1}{2}(v^2 - v)c_i$, where $a_i,\ b_i,\ c_i \in F_q,\ 0 \leq i \leq n - 1$. Let $a = (a_0, a_1, \cdots, a_{n-1})$, $b = (b_0, b_1, \cdots, b_{n-1})$ and $c = (c_0, c_1, \cdots, c_{n-1})$. Then $a \in C_1,\ b \in C_2$ and $c \in C_3$. Now, suppose $C_1,\ C_2$ and C_3 are skew cyclic codes over F_q with respect to automorphism θ_t. This means that $\sigma(a) = (\theta_t(a_{n-1}), \theta_t(a_0), \cdots, \theta_t(a_{n-2})) = (a_{n-1}^{p^t}, a_0^{p^t}, \cdots, a_{n-2}^{p^t}) \in C_1$, $\sigma(b) = (\theta_t(b_{n-1}), \theta_t(b_0), \cdots, \theta_t(b_{n-2})) = (b_{n-1}^{p^t}, b_0^{p^t}, \cdots, b_{n-2}^{p^t}) \in C_2$ and $\sigma(c) = (\theta_t(c_{n-1}), \theta_t(c_0), \cdots, \theta_t(c_{n-2})) = (c_{n-1}^{p^t}, c_0^{p^t}, \cdots, c_{n-2}^{p^t}) \in C_3$. Thus $(1 - v^2)\sigma(a) + (v^2 + v)\frac{p+1}{2}\sigma(b) + (v^2 - v)\frac{p+1}{2}\sigma(c) \in C$. It can be easily seen that $(1 - v^2)\sigma(a) + (v^2 + v)\frac{p+1}{2}\sigma(b) + (v^2 - v)\frac{p+1}{2}\sigma(c) = \sigma(r)$. Hence $\sigma(r) \in C$, which means that C is a skew cyclic code over R with respect to automorphism θ_t.

Conversely, suppose C is a skew cyclic code over R with respect to automorphism θ_t. Let $r_i = (1-v^2)a_i + \frac{p+1}{2}(v^2+v)b_i + \frac{p+1}{2}(v^2-v)c_i$, for any $a = (a_0, a_1, \cdots, a_{n-1}) \in C_1,\ b = (b_0, b_1, \cdots, b_{n-1}) \in C_2$ and $c = (c_0, c_1, \cdots, c_{n-1}) \in C_3$. Then $r = (r_0, r_1, ..., r_{n-1}) \in C$. By the hypothesis $\sigma(r) \in C$. Since $(1 - v^2)\sigma(a) + (v^2 + v)\frac{p+1}{2}\sigma(b) + (v^2 - v)\frac{p+1}{2}\sigma(c) = \sigma(r)$, $(1 - v^2)\sigma(a) + (v^2 + v)\frac{p+1}{2}\sigma(b) + (v^2 - v)\frac{p+1}{2}\sigma(c) \in C$. Thus $\sigma(a) \in C_1,\ \sigma(b) \in C_2$ and $\sigma(c) \in C_3$, which implies that $C_1,\ C_2$ and C_3 are skew cyclic codes of length n over F_q with respect to automorphism θ_t.

Corollary 4.2. Let C be a skew cyclic code of length n over R. Then the dual code $C^\perp$ is also a skew cyclic code of length n over R.

Proof. In view of Theorem 3.5, we know that $C^\perp = (1-v^2)C_1^\perp \oplus \frac{p+1}{2}(v^2+v)C_2^\perp \oplus \frac{p+1}{2}(v^2-v)C_3^\perp$. Since the dual code of every skew cyclic code over F_q is also skew cyclic ([8], Corollary 18), by Theorem 4.1, $C^\perp$ is a skew cyclic code over R.

Corollary 4.3. A code $C = (1 - v^2)C_1 \oplus \frac{p+1}{2}(v^2 + v)C_2 \oplus \frac{p+1}{2}(v^2 - v)C_3$ of length n over R is a self-dual skew cyclic if and only if $C_1,\ C_2$ and C_3 are self-dual skew cyclic codes of length n over F_q.

Let C' be a linear code of length n over F_q and $c = (c^1|c^2|\cdots|c^s)$ be a codeword in C' into s equal parts of length r where $n = rs$. If $(\sigma(c^1)|\sigma(c^2)|\cdots|\sigma(c^s)) \in C'$, then the linear code C which is permutation equivalent to C' is called a skew quasi-cyclic code of index s or skew s-quasi cyclic code. (for detail see reference [1])

Theorem 4.4. Let C be a skew cyclic code of length n over R. Then $\varphi(C)$ is a skew 3-quasi cyclic code of length $3n$ over F_q.

Proof. In view of Theorem 3.2 and the definition of skew quasi-cyclic codes, we can obtain the required result.

Theorem 4.5. Let $C = (1-v^2)C_1 \oplus \frac{p+1}{2}(v^2+v)C_2 \oplus \frac{p+1}{2}(v^2-v)C_3$ be skew cyclic code of length n over R. Then $C = \langle (1-v^2)g_1(x), \frac{p+1}{2}(v^2+v)g_2(x), \frac{p+1}{2}(v^2-v)g_3(x)\rangle$ and $|C| = q^{3n-deg(g_1(x))-deg(g_2(x))-deg(g_3(x))}$, where $g_1(x),\ g_2(x)$ and $g_3(x)$ are the generator polynomials of $C_1,\ C_2$ and C_3 respectively.

Proof. Since $C_1 = \langle g_1(x)\rangle \subseteq F_q[x,\theta_t]/\langle x^n-1\rangle,\ C_2 = \langle g_2(x)\rangle \subseteq F_q[x,\theta_t]/\langle x^n-1\rangle,\ C_3 = \langle g_3(x)\rangle \subseteq F_q[x,\theta_t]/\langle x^n-1\rangle$ and $C = (1-v^2)C_1 \oplus \frac{p+1}{2}(v^2+v)C_2 \oplus \frac{p+1}{2}(v^2-v)C_3$, we find that $C = \{c(x) \mid c(x) = (1-v^2)f_1(x) + \frac{p+1}{2}(v^2+v)f_2(x) + \frac{p+1}{2}(v^2-v)f_3(x),\ f_1(x) \in C_1,\ f_2(x) \in C_2,\ f_3(x) \in C_3\}$. Therefore

$$C \subseteq \langle (1-v^2)g_1(x), \frac{p+1}{2}(v^2+v)g_2(x), \frac{p+1}{2}(v^2-v)g_3(x)\rangle \subseteq R[x,\theta_t]/\langle x^n-1\rangle.$$

For any $(1-v^2)k_1(x)g_1(x) + \frac{p+1}{2}(v^2+v)k_2(x)g_2(x) + \frac{p+1}{2}(v^2-v)k_3(x)g_3(x) \in \langle (1-v^2)g_1(x), \frac{p+1}{2}(v^2+v)g_2(x), \frac{p+1}{2}(v^2-v)g_3(x)\rangle \subseteq R[x,\theta_t]/\langle x^n-1\rangle$, where $k_1(x), k_2(x), k_3(x) \in R[x,\theta_t]/\langle x^n-1\rangle$, there are $r_1(x), r_2(x), r_3(x) \in F_q[x,\theta_t]$ such that

$$(1-v^2)k_1(x) = (1-v^2)r_1(x),$$

$$\frac{p+1}{2}(v^2+v)k_2(x) = \frac{p+1}{2}(v^2+v)r_2(x)$$

and

$$\frac{p+1}{2}(v^2-v)k_3(x) = \frac{p+1}{2}(v^2-v)r_3(x).$$

This means that

$$\langle (1-v^2)g_1(x), \frac{p+1}{2}(v^2+v)g_2(x), \frac{p+1}{2}(v^2-v)g_3(x)\rangle \subseteq C.$$

Hence $\langle (1-v^2)g_1(x), \frac{p+1}{2}(v^2+v)g_2(x), \frac{p+1}{2}(v^2-v)g_3(x)\rangle = C$. Since $|C| = |C_1||C_2||C_3|$, $|C| = q^{3n-deg(g_1(x))-deg(g_2(x))-deg(g_3(x))}$.

Theorem 4.6. Let $C_1,\ C_2$ and C_3 be skew cyclic codes over F_q with monic generator polynomials $g_1(x),\ g_2(x)$ and $g_3(x)$ respectively. If $C = (1-v^2)C_1 \oplus \frac{p+1}{2}(v^2+v)C_2 \oplus \frac{p+1}{2}(v^2-v)C_3$ is a skew cyclic code of length n over R, then there is a unique polynomial $g(x) \in R[x,\theta_t]$ such that $C = \langle g(x)\rangle$ and $g(x)$ is a right divisor of x^n-1, where $g(x) = (1-v^2)g_1(x) + \frac{p+1}{2}(v^2+v)g_2(x) + \frac{p+1}{2}(v^2-v)g_3(x)$.

Proof. By Theorem 4.5, we may assume that $C = \langle (1-v^2)g_1(x), \frac{p+1}{2}(v^2+v)g_2(x), \frac{p+1}{2}(v^2-v)g_3(x)\rangle$, where $g_1(x),\ g_2(x)$ and $g_3(x)$ are the monic generator polynomials of $C_1,\ C_2$ and C_3 respectively. Let $g(x) = (1-v^2)g_1(x) + \frac{p+1}{2}(v^2+v)g_2(x) + \frac{p+1}{2}(v^2-v)g_3(x)$. Clearly, $\langle g(x)\rangle \subseteq C$. Note that

$$(1-v^2)g_1(x) = (1-v^2)g(x),$$

$$\frac{p+1}{2}(v^2+v)g_2(x) = \frac{p+1}{2}(v^2+v)g(x)$$

and

$$\frac{p+1}{2}(v^2-v)g_3(x) = \frac{p+1}{2}(v^2-v)g(x),$$

so $C \subseteq \langle g(x)\rangle$. Hence $C = \langle g(x)\rangle$. Since $g_1(x),\ g_2(x)$ and $g_3(x)$ are monic right divisors of $x^n - 1$, there are $r_1(x), r_2(x), r_3(x) \in F_q[x, \theta_t]/\langle x^n - 1\rangle$ such that

$$x^n - 1 = r_1(x)g_1(x) = r_2(x)g_2(x) = r_3(x)g_3(x).$$

This implies that

$$x^n - 1 = [(1 - v^2)r_1(x) + \frac{p+1}{2}(v^2 + v)r_2(x) + \frac{p+1}{2}(v^2 - v)r_3(x)]g(x).$$

Hence, $g(x)|x^n - 1$. The uniqueness of $g(x)$ can be followed from that of $g_1(x), g_2(x)$ and $g_3(x)$.

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

Corollary 4.7. Every left submodule of $R[x, \theta_t]/\langle x^n - 1\rangle$ is principally generated.

In order to study the generator polynomials of the dual code of a skew cyclic code over R, we need the following definition which can be found in [8].

Let $g(x) = g_0 + g_1x + \cdots + g_rx^r$ and $h(x) = h_0 + h_1x + \cdots + h_{n-r}x^{n-r}$ be polynomials in $F_q[x, \theta_t]$ such that $x^n - 1 = h(x)g(x)$ and C' be the skew cyclic code generated by $g(x)$ in $F_q[x, \theta_t]/\langle x^n - 1\rangle$. Then the dual code of C' is a skew cyclic code generated by the polynomial $\bar{h}(x) = h_{n-r} + \theta_t(h_{n-r-1})x + \cdots + \theta_t^{n-r}(h_0)x^{n-r}$.

In view of Theorems 3.5 & 4.6, we have the following corollary:

Corollary 4.8. Let $C_1,\ C_2$ and C_3 be skew cyclic codes over F_q and $g_1(x),\ g_2(x)$ and $g_3(x)$ be their generator polynomials such that

$$x^n - 1 = h_1(x)g_1(x) = h_2(x)g_2(x) = h_3(x)g_3(x) \in F_q[x, \theta_t].$$

If $C = (1 - v^2)C_1 \oplus \frac{p+1}{2}(v^2 + v)C_2 \oplus \frac{p+1}{2}(v^2 - v)C_3$, then

$$C^{\perp} = \langle (1 - v^2)\bar{h}_1(x) + \frac{p+1}{2}(v^2 + v)\bar{h}_2(x) + \frac{p+1}{2}(v^2 - v)\bar{h}_3(x)\rangle$$

and $|C^{\perp}| = q^{deg(g_1(x))+deg(g_2(x))+deg(g_3(x))}$.

5 Idempotent generators of skew cyclic codes over R

The idempotent generators of skew cyclic codes over F_q studied by Gursoy et al. [11] under some restrictions. In fact, they proved the following results:

Lemma 5.1. [11, Lemma 2] Let $g(x) \in F_q[x, \theta_t]$ be a monic right divisor of $x^n - 1$. If $g.c.d.(n, m_t) = 1$, then $g(x) \in F_{p^t}[x]$, where $m_t = m/t$ denotes the order of the automorphism θ_t.

Lemma 5.2. [11, Theorem 6] Let $g(x) \in F_q[x, \theta_t]$ be a monic right divisor of $x^n - 1$ and $C = \langle g(x)\rangle$. If $g.c.d.(n, m_t) = 1$ and $g.c.d.(n, q) = 1$, then there exists an idempotent polynomial $e(x) \in F_q[x, \theta_t]/\langle x^n - 1\rangle$ such that $C = \langle e(x)\rangle$.

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

Theorem 5.3. Let $C = (1-v^2)C_1 \oplus \frac{p+1}{2}(v^2+v)C_2 \oplus \frac{p+1}{2}(v^2-v)C_3$ be skew cyclic code of length n over R and $g.c.d.(n, m_t) = 1,\ g.c.d.(n, q) = 1$. Then C_i has idempotent generator, say $e_i(x)$ for $i = 1, 2, 3$. Moreover $e(x) = (1-v^2)e_1(x) + \frac{p+1}{2}(v^2+v)e_2(x) + \frac{p+1}{2}(v^2-v)e_3(x)$ is an idempotent generator of C, that is, $C = \langle e(x)\rangle$.

Proof. In the light of Theorem 4.6 and Lemma 5.2 , the proof follows.

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

Theorem 5.4. Let $g.c.d.(n, m_t) = 1$ and $x^n - 1 = \prod_{i=1}^{r} g_i^{s_i}(x)$, where $g_i(x) \in F_q[x, \theta_t]$ is irreducible. Then the number of skew cyclic codes of length n over R is $\prod_{i=1}^{r} (s_i + 1)^3$.

Proof. In view of Lemma 5.1 if $g.c.d.(n, m_t) = 1$, then $g_i(x) \in F_{p^t}[x]$. In this case the number of skew cyclic codes of length n over F_q is $\prod_{i=1}^{r}(s_i + 1)$. Since $C = (1-v^2)C_1 \oplus \frac{p+1}{2}(v^2+v)C_2 \oplus \frac{p+1}{2}(v^2-v)C_3$, $\prod_{i=1}^{r} (s_i+1)^3$ is the number of skew cyclic codes of length n over R. When $g.c.d.(n, m_t) \neq 1$, the factorization of $x^n - 1$ is not unique in $F_q[x, \theta_t]$, therefore we can not say anything certain about the number of skew cyclic codes in this case.

Now, we close our discussion with the following examples:

Example 4.11 Let $R = F_9 + vF_9 + v^2F_9$ be the ring with $v^3 = v$ and θ be the Frobenius automorphism over F_9, that is, $\theta(r) = r^3$ for any $r \in F_9$, where $F_9 = F_3[\alpha],\ \alpha^2 + 1 = 0$. Then

$$x^4 - 1 = (x+1)(x+2)(x+\alpha)(x+2\alpha) \in F_9[x, \theta].$$

If $g_1(x) = g_2(x) = g_3(x) = x + 2\alpha$, then $C_1 = \langle g_1(x)\rangle$, $C_2 = \langle g_2(x)\rangle$ and $C_3 = \langle g_3(x)\rangle$ are the skew cyclic codes over F_9 with parameters $[4, 3, 2]$. Therefore, the code $C = \langle (1-v^2)g_1(x) + \frac{p+1}{2}(v^2+v)g_2(x) + \frac{p+1}{2}(v^2-v)g_3(x)\rangle = \langle x + 2\alpha\rangle$ is a skew cyclic code of length 4 over R. Further, the Gray image $\varphi(C)$ of C is a skew 3-quasi cyclic code over F_9 with parameters $[12, 9, 2]$, which is an optimal code.

Example 4.12 Let $R = F_9 + vF_9 + v^2F_9$ be the ring with $v^3 = v$ and θ be the Frobenius automorphism over F_9, that is, $\theta(r) = r^3$ for any $r \in F_9$, where $F_9 = F_3[\alpha],\ \alpha^2 + 1 = 0$. Then

$$x^5 - 1 = (x+2)(x^4 + x^3 + x^2 + x + 1) \in F_9[x, \theta].$$

Since $g.c.d.(5, 2) = 1$, there exist 63 nonzero skew cyclic codes of length 5 over R.

Let $g_1(x) = g_2(x) = g_3(x) = x + 2$. Then $C_1 = \langle g_1(x)\rangle$, $C_2 = \langle g_2(x)\rangle$ and $C_3 = \langle g_3(x)\rangle$ are the skew cyclic codes of length 5 over F_9. Therefore, the code $C = \langle (1-v^2)g_1(x) + \frac{p+1}{2}(v^2+v)g_2(x) + \frac{p+1}{2}(v^2-v)g_3(x)\rangle = \langle x + 2\rangle$ is a skew cyclic code of length 5 over R. Also, the Gray image $\varphi(C)$ of C is a skew 3-quasi cyclic code of length 15 over

F_9.

Example 4.13 Let $R = F_9 + vF_9 + v^2F_9$ be the ring with $v^3 = v$ and θ be the Frobenius automorphism over F_9, that is, $\theta(r) = r^3$ for any $r \in F_9$, where $F_9 = F_3[\alpha],\ \alpha^2 + \alpha + 2 = 0$. Then

$$\begin{aligned} x^6 - 1 &= (2 + (2+\alpha)x + (1+2\alpha)x^3 + x^4)(1 + (2+\alpha)x + x^2) \\ &= (2 + x + (2+2\alpha)x^2 + x^3)(1 + x + 2\alpha x^2 + x^3) \\ &\in F_9[x, \theta]. \end{aligned}$$

If $g_1(x) = g_2(x) = 2 + (2+\alpha)x + (1+2\alpha)x^3 + x^4$ and $g_3(x) = 2 + x + (2+2\alpha)x^2 + x^3$, then $C_1 = \langle g_1(x) \rangle,\ C_2 = \langle g_2(x) \rangle$ and $C_3 = \langle g_3(x) \rangle$ are the skew cyclic codes of length 6 over F_9 with dimensions 2, 2 and 3 respectively. Thus the code

$$C = \langle (1 - v^2)g_1(x) + \frac{p+1}{2}(v^2 + v)g_2(x) + \frac{p+1}{2}(v^2 - v)g_3(x) \rangle$$

is a skew cyclic code of length 6 over R. Also, the Gray image $\varphi(C)$ of C is a skew 3-quasi cyclic code over F_9 with parameters $[18, 7, 4]$.

6 Conclusion

In this paper, we have studied the structural properties of skew cyclic codes over the principal ideal ring $F_q + vF_q + v^2F_q$ by taking the automorphism $\theta_t : a + vb + v^2c \mapsto a^{p^t} + vb^{p^t} + v^2c^{p^t}$. We have proved that the Gray image of a skew cyclic code of length n over $F_q + vF_q + v^2F_q$ is a skew 3-quasi cyclic code of length $3n$ over F_q. It has also been shown that skew cyclic codes over $F_q + vF_q + v^2F_q$ are principally generated. Further, we have obtained idempotent generators of skew cyclic codes over $F_q + vF_q + v^2F_q$.

Acknowledgements

The authors are thankful to the anonymous referees for their careful reading of the paper and valuable comments.

References

[1] T. Abualrub, A. Ghrayeb, N. Aydin and I. Siap, *On the construction of skew quasi cyclic codes* , IEEE. Trans. Inform. Theory, **56**(2010), 2081-2090.

[2] T. Abualrub, N. Aydin and P. Seneviratne, *On θ-cyclic codes over $F_2 + vF_2$*, Australas. J. Combin., **54**(2012), 115-126.

[3] M. Ashraf and G. Mohammad, *On skew cyclic codes over $F_3 + vF_3$*, Int. J. Inf. Coding Theory, **2**(4)(2014), 218-225.

[4] M. Ashraf and G. Mohammad, *On skew cyclic codes over a semi-local ring*, Discrete Math. Algorithm. Appl. **7**(4), 1550042 (2015).

[5] M. Bhaintwal, *Skew quasi cyclic codes over Galois rings*, Des. Codes Cryptogr., **62**(1)(2012), 85-101.

[6] D. Boucher, W. Geiselmann and F. Ulmer, *Skew cyclic codes*, Appl. Algebra Eng. Commun. Comput, **18**(4)(2007), 379-389.

[7] D. Boucher, P. Sole and F. Ulmer, *Skew constacyclic codes over Galois ring*, Adv. Math. Commun., **2**(3)(2008), 273-292.

[8] D. Boucher and F. Ulmer, *Coding with skew polynomial rings*, J. Symb. Comput., **44**(2009), 1644-1656.

[9] J. Gao, *Skew cyclic codes over $F_p + vF_p$*, J. Appl. Math. and Informatics **31**(2013), 337-342.

[10] J. Gao, *Some results on linear codes over $F_p+uF_p+u^2F_p$*, J. Appl. Math. Comput., **47** (2015), 473-485.

[11] F. Gursoy, I. Siap and B. Yildiz, *Construction of skew cyclic codes over $F_q + vF_q$*, Adv. Math. Commun., **8** (2014), 313-322.

[12] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, *The $\mathbb{Z}_4$-linearty of Kerdock, Preparata, Goethals and Related codes*, IEEE. Trans. Inform. Theory, **40**(1994), 301-319.

[13] S. Jitman, S. Ling and P. Udomkavanich, *Skew constacyclic codes over finite chain rings*, Adv. Math. Commun., **6**(2012), 29-63.

[14] Z. Odemis Ozger, U. U. Kara and B. Yildiz, *Linear, cyclic and constacyclic codes over $S_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$*, Filomat, **28**(2014), 897-906.

[15] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, *Skew cyclic codes of arbitrary length*, Int. J. Inf. Coding Theory, **2**(2011), 10-20.