On the Codes over a Semilocal Finite Ring

Abdullah Dertli
Department of Mathematics
Ondokuz Mayıs University
Samsun, Turkey

Yasemin Cengellenmis
Department of Mathematics
Trakya University
Edirne, Turkey

Senol Eren
Department of Mathematics
Ondokuz Mayıs University
Samsun, Turkey

***Abstract*—In this paper, we study the structure of cyclic, quasi cyclic, constacyclic codes and their skew codes over the finite ring R. The Gray images of cyclic, quasi cyclic, skew cyclic, skew quasi cyclic and skew constacyclic codes over R are obtained. A necessary and sufficient condition for cyclic (negacyclic) codes over R that contains its dual has been given. The parameters of quantum error correcting codes are obtained from both cyclic and negacyclic codes over R. Some examples are given. Firstly, quasi constacyclic and skew quasi constacyclic codes are introduced. By giving two inner product, it is investigated their duality. A sufficient condition for 1 generator skew quasi constacyclic codes to be free is determined.**

***Keywords*—Cyclic codes; Skew cyclic codes; Quantum codes**

I. Introduction

In the beginning, a lot of research on error-correcting codes are concentrated on codes over finite fields. Since the revelation in 1994 [17], there has been a lot of interest in codes over finite rings. The structure of a certain type of codes over many rings are determined such as negacyclic, cyclic, quasi-cyclic, consta cyclic codes in [6,11,20,21,22,23,26,32]. Many methods and many approaches are applied to produce certain types of codes with good parameters and properties.

Some authors generalized the notion of cyclic, quasi-cyclic and constacyclic codes by using generator polynomials in skew polynomial rings [1,2,5,7,8,9,14,15,18,27,30].

Moreover, in [10] Calderbank et al. gave a way to construct quantum error correcting codes from the classical error-correcting codes, although the theory of quantum error-correcting codes has striking differences from the theory of classical error correcting codes. Many good quantum codes have been constructed by using classical cyclic codes over finite fields or finite rings with self orthogonal (or dual containing) properties in [3,12,13,16,19,24,25,28,29,31].

In [4] they introduced the finite ring $R = Z_3[v]/\left\langle v^3 - v\right\rangle$. They studied the structure of this ring. The algebraic structure of cyclic and dual codes was also studied. A MacWilliams type identity was established.

In this paper, first of all we gave some definitions. By giving the duality of codes via inner product, it is shown that C is self orthogonal code over R, so is $\phi(C)$, where ϕ is a Gray map.

The Gray images of cyclic and quasi-cyclic codes over R are obtained. A linear code over R is represented using three ternary codes and the generator matrix is given.

After a cyclic (negacyclic) code over R is represented via cyclic (negacyclic) codes over Z_3, it is determined the dual of cyclic (negacyclic) code. A necessary and sufficient condition for cyclic (negacyclic) code over R that contains its dual is given. The parameters of quantum error-correcting codes are obtained from both cyclic and negacyclic codes over R. As a last, some examples are given about quantum error-correcting codes.

When n is odd, it is defined the λ-constacyclic codes over R where λ is unit. A constacyclic code is represented using either cyclic codes or negacyclic codes of length n.

It is found the nontrivial automorphism θ on the ring R. By using this automorphism, the skew cyclic, skew quasi-cyclic and skew constacyclic codes over R are introduced. The number of distinct skew cyclic codes over R is given. The Gray images of skew codes are obtained.

Firstly, quasi-constacyclic and skew quasi-constacyclic codes over R are introduced. By using two inner product, it is investigated the duality about quasi-constacyclic and skew quasi-constacyclic codes over R. The Gray image of skew quasi-constacyclic codes over R is determined. A sufficient condition for 1-generator skew quasi-constacyclic code to be free is determined.

II. Preliminaries

Suppose $R = Z_3 + vZ_3 + v^2Z_3$ where $v^3 = v$ and $Z_3 = \{0, 1, 2\}$. R is a finite commutative ring with 27 elements. This ring is a semi local ring with three maximal ideals. R is a principal ideal ring and not finite chain ring. The units of the ring are $1, 2, 1 + v^2, 1 + v + 2v^2, 1 + 2v + 2v^2, 2 + v + v^2, 2 + 2v + v^2, 2 + 2v^2$. The maximal ideals,

$$\begin{aligned}
\langle v\rangle &= \langle 2v\rangle = \left\langle v^2\right\rangle = \left\langle 2v^2\right\rangle \\
&= \{0, v, 2v, v^2, 2v^2, v + v^2, v + 2v^2, 2v + v^2, \\
&\quad 2v + 2v^2\} \\
\langle 1+v\rangle &= \langle 2+2v\rangle = \left\langle 1+2v+v^2\right\rangle = \left\langle 2+v+2v^2\right\rangle \\
&= \{0, 1+v, 2+2v, v+v^2, 2v+2v^2, 1+2v \\
&\quad +v^2, 1+2v^2, 2+v^2, 2+v+2v^2\} \\
\left\langle 1+v+v^2\right\rangle &= \langle 1+2v\rangle = \langle 2+v\rangle = \left\langle 2+2v+2v^2\right\rangle \\
&= \{0, 2+v, 1+2v, 2v+v^2, v+2v^2, 2+v^2, \\
&\quad 1+2v^2, 2+2v+2v^2, 1+v+v^2\}
\end{aligned}$$

The other ideals,

$$\begin{aligned}
\langle 0\rangle &= \{0\}\\
\langle 1\rangle &= \langle 2\rangle = \langle 1+v^2\rangle = \langle 1+v+2v^2\rangle\\
&= \langle 1+2v+2v^2\rangle = \langle 2+v+v^2\rangle\\
&= \langle 2+2v+v^2\rangle = \langle 2+2v^2\rangle = R\\
\langle 1+2v^2\rangle &= \langle 2+v^2\rangle = \{0, 2+v^2, 1+2v^2\}\\
\langle v+v^2\rangle &= \langle 2v+2v^2\rangle = \{0, v+v^2, 2v+2v^2\}\\
\langle v+2v^2\rangle &= \langle 2v+v^2\rangle = \{0, v+2v^2, 2v+v^2\}
\end{aligned}$$

A linear code C over R length n is a $R-$submodule of R^n. An element of C is called a codeword.

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

$$x.y = \sum_{i=0}^{n-1} x_i y_i$$

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

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

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

A constacyclic code C over R is a linear code with the property that if $c = (c_0, c_1, ..., c_{n-1}) \in C$ then $\nu(C) = (\lambda c_{n-1}, c_0, ..., c_{n-2}) \in C$ where λ is a unit element of R. A subset C of R^n is a linear λ-constacyclic code of length n iff it is polynomial representation is an ideal of $R[x] / \langle x^n - \lambda\rangle$.

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

Let C be code over Z_3 of length n and $\acute{c} = (\acute{c}_0, \acute{c}_1, ..., \acute{c}_{n-1})$ be a codeword of C. The Hamming weight of $\acute{c}$ is defined as $w_H(\acute{c}) = \sum_{i=0}^{n-1} w_H(\acute{c}_i)$ where $w_H(\acute{c}_i) = 1$ if $\acute{c}_i \neq 0$ and $w_H(\acute{c}_i) = 0$ if $\acute{c}_i = 0$. Hamming distance of C is defined as $d_H(C) = \min d_H(c, \acute{c})$, where for any $\acute{c} \in C$, $c \neq \acute{c}$ and $d_H(c, \acute{c})$ is Hamming distance between two codewords with $d_H(c, \acute{c}) = w_H(c - \acute{c})$.

Let $a \in Z_3^{3n}$ with $a = (a_0, a_1, ..., a_{3n-1}) = \left(a^{(0)} \left| a^{(1)} \right| a^{(2)}\right)$, $a^{(i)} \in Z_3^n$ for $i = 0, 1, 2$. Let φ be a map from Z_3^{3n} to Z_3^{3n} given by $\varphi(a) = \left(\sigma\left(a^{(0)}\right) \left| \sigma\left(a^{(1)}\right) \right| \sigma\left(a^{(2)}\right)\right)$ where σ is a cyclic shift from Z_3^n to Z_3^n given by $\sigma\left(a^{(i)}\right) = ((a^{(i,n-1)}), (a^{(i,0)}), (a^{(i,1)}), ..., (a^{(i,n-2)}))$ for every $a^{(i)} = (a^{(i,0)}, ..., a^{(i,n-1)})$ where $a^{(i,j)} \in Z_3$, $j = 0, 1, ..., n-1$. A code of length $3n$ over Z_3 is said to be quasi cyclic code of index 3 if $\varphi(C) = C$.

Let $n = sl$. A quasi-cyclic code C over R of length n and index l is a linear code with the property that if

$e = (e_{0,0}, ..., e_{0,l-1}, e_{1,0}, ..., e_{1,l-1}, ..., e_{s-1,0}, ..., e_{s-1,l-1}) \in C$, then $\tau_{s,l}(e) = (e_{s-1,0}, ..., e_{s-1,l-1}, e_{0,0}, ..., e_{0,l-1}, ..., e_{s-2,0}, ..., e_{s-2,l-1}) \in C$.

Let $a \in Z_3^{3n}$ with $a = (a_0, a_1, ..., a_{3n-1}) = \left(a^{(0)} \left| a^{(1)} \right| a^{(2)}\right)$, $a^{(i)} \in Z_3^n$, for $i = 0, 1, 2$. Let Γ be a map from Z_3^{3n} to Z_3^{3n} given by

$$\Gamma(a) = \left(\mu\left(a^{(0)}\right) \left| \mu\left(a^{(1)}\right) \right| \mu\left(a^{(2)}\right)\right)$$

where μ is the map from Z_3^n to Z_3^n given by

$$\mu\left(a^{(i)}\right) = ((a^{(i,s-1)}), (a^{(i,0)}), ..., (a^{(i,s-2)}))$$

for every $a^{(i)} = \left(a^{(i,0)}, ..., a^{(i,s-1)}\right)$ where $a^{(i,j)} \in Z_3^l$, $j = 0, 1, ..., s-1$ and $n = sl$. A code of length $3n$ over Z_3 is said to be $l-$quasi cyclic code of index 3 if $\Gamma(C) = C$.

III. Gray Map and Gray Images of Cyclic and Quasi-cyclic Codes Over R

In [4], the Gray map is defined as follows

$$\begin{aligned}
\phi &: R \to Z_3^3\\
\phi(a + vb + v^2 c) &= (a, a+b+c, a+2b+c)
\end{aligned}$$

Let C be a linear code over R of length n. For any codeword $c = (c_0, ..., c_{n-1})$ the Lee weight of c is defined as $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$ and the Lee distance of C is defined as $d_L(C) = \min d_L(c, \acute{c})$, where for any $\acute{c} \in C$, $c \neq \acute{c}$ and $d_L(c, \acute{c})$ is Lee distance between two codewords with $d_L(c, \acute{c}) = w_L(c - \acute{c})$. Gray map ϕ can be extended to map from R^n to Z_3^{3n}.

Theorem 1: The Gray map ϕ is a weight preserving map from $(R^n, \text{Lee weight})$ to $\left(Z_3^{3n}, \text{Hamming weight}\right)$. Moreover it is an isometry from R^n to Z_3^{3n}.

Theorem 2: If C is an $[n, k, d_L]$ linear codes over R then $\phi(C)$ is a $[3n, k, d_H]$ linear codes over Z_3, where $d_H = d_L$.

Proof: Let $x = a_1 + vb_1 + v^2 c_1$, $y = a_2 + vb_2 + v^2 c_2 \in R, \alpha \in Z_3$ then

$$\phi(x+y) = \phi\left(a_1 + a_2 + v(b_1 + b_2) + v^2(c_1 + c_2)\right)$$

$= (a_1 + a_2, a_1 + a_2 + b_1 + b_2 + c_1 + c_2, a_1 + a_2 + 2(b_1 + b_2) + c_1 + c_2)$

$= (a_1, a_1 + b_1 + c_1, a_1 + 2b_1 + c_1) + (a_2, a_2 + b_2 + c_2, a_2 + 2b_2 + c_2)$

$= \phi(x) + \phi(y)$

$$\begin{aligned}
\phi(\alpha x) &= \phi\left(\alpha a_1 + v\alpha b_1 + v^2 \alpha c_1\right)\\
&= (\alpha a_1, \alpha a_1 + \alpha b_1 + \alpha c_1, \alpha a_1 + 2\alpha b_1 + \alpha c_1)\\
&= \alpha(a_1, a_1 + b_1 + c_1, a_1 + 2b_1 + c_1)\\
&= \alpha\phi(x)
\end{aligned}$$

so ϕ is linear. As ϕ is bijective then $|C| = |\phi(C)|$. From Theorem 1 we have $d_H = d_L$. ■

Theorem 3: If C is self orthogonal, so is $\phi(C)$.

Proof: Let $x = a_1 + vb_1 + v^2c_1,\ y = a_2 + vb_2 + v^2c_2$ where $a_1, b_1, c_1,\ a_2, b_2, c_2 \in Z_3$. From $x.y = a_1a_2 + v(a_1b_2 + b_1a_2 + b_1c_2 + c_1b_2) + v^2(a_1c_2 + b_1b_2 + c_1a_2 + c_1c_2)$ if C is self orthogonal, so we have

$$a_1a_2 = 0,$$
$$a_1b_2 + b_1a_2 + b_1c_2 + c_1b_2 = 0,$$
$$a_1c_2 + b_1b_2 + c_1a_2 + c_1c_2 = 0.$$

From $\phi(x).\phi(y) = (a_1, a_1 + b_1 + c_1, a_1 + 2b_1 + c_1)(a_2, a_2 + b_2 + c_2, a_2 + 2b_2 + c_2) = a_1a_2 + a_1a_2 + a_1b_2 + a_1c_2 + b_1a_2 + b_1b_2 + b_1c_2 + c_1a_2 + c_1b_2 + c_1c_2 + a_1a_2 + 2(a_1b_2 + b_1a_2 + b_1c_2 + c_1b_2) + a_1c_2 + b_1b_2 + c_1a_2 + c_1c_2 = 0$
Therefore, we have $\phi(C)$ is self orthogonal. ■

Note that $\phi(C)^{\perp} = \phi\left(C^{\perp}\right)$. Moreover, if C is self-dual, so is $\phi(C)$.

Proposition 4: Let ϕ the Gray map from R^n to Z_3^{3n}, let σ be cyclic shift and let φ be a map as in the preliminaries. Then $\phi\sigma = \varphi\phi$.

Proof: Let $r_i = a_i + vb_i + v^2c_i$ be the elements of R for $i = 0, 1, ..., n-1$. We have $\sigma(r_0, r_1, ..., r_{n-1}) = (r_{n-1}, r_0, ..., r_{n-2})$. If we apply ϕ, we have

$$\begin{aligned}\phi(\sigma(r_0, ..., r_{n-1})) &= \phi(r_{n-1}, r_0, ..., r_{n-2}) \\ &= (a_{n-1}, ..., a_{n-2}, a_{n-1} + b_{n-1} + c_{n-1} \\ &\quad , ..., a_{n-2} + b_{n-2} + c_{n-2}, a_{n-1} + \\ &\quad 2b_{n-1} + c_{n-1}, ..., a_{n-2} + 2b_{n-2} + \\ &\quad c_{n-2})\end{aligned}$$

On the other hand $\phi(r_0, ..., r_{n-1}) = (a_0, ..., a_{n-1}, a_0 + b_0 + c_0, ..., a_{n-1} + b_{n-1} + c_{n-1}, a_0 + 2b_0 + c_0, ..., a_{n-1} + 2b_{n-1} + c_{n-1})$. If we apply φ, we have $\varphi(\phi(r_0, r_1, ..., r_{n-1})) = (a_{n-1}, ..., a_{n-2}, a_{n-1} + b_{n-1} + c_{n-1}, ..., a_{n-2} + b_{n-2} + c_{n-2}, a_{n-1} + 2b_{n-1} + c_{n-1}, ..., a_{n-2} + 2b_{n-2} + c_{n-2})$. Thus, $\phi\sigma = \varphi\phi$. ■

Proposition 5: Let σ and φ be as in the preliminaries. A code C of length n over R is cyclic code if and only if $\phi(C)$ is quasi cyclic code of index 3 over Z_3 with length $3n$.

Proof: Suppose C is cyclic code. Then $\sigma(C) = C$. If we apply ϕ, we have $\phi(\sigma(C)) = \phi(C)$. From Proposition 4, $\phi(\sigma(C)) = \varphi(\phi(C)) = \phi(C)$. Hence, $\phi(C)$ is a quasi cyclic code of index 3. Conversely, if $\phi(C)$ is a quasi cyclic code of index 3, then $\varphi(\phi(C)) = \phi(C)$. From Proposition 4, we have $\varphi(\phi(C)) = \phi(\sigma(C)) = \phi(C)$. Since ϕ is injective, it follows that $\sigma(C) = C$. ■

Proposition 6: Let $\tau_{s,l}$ be quasi-cyclic shift on R. Let Γ be as in the preliminaries. Then $\phi\tau_{s,l} = \Gamma\phi$.

Proof: Let $e = (e_{0,0}, ..., e_{0,l-1}, e_{1,0}, ..., e_{1,l-1}, ..., e_{s-1,0}, ..., e_{s-1,l-1})$ with $e_{i,j} = a_{i,j} + vb_{i,j} + v^2c_{i,j}$ where $i = 0, 1, ..., s-1$ and $j = 0, 1, ..., l-1$. We have $\tau_{s,l}(e) = (e_{s-1,0}, ..., e_{s-1,l-1}, e_{0,0}, ..., e_{0,l-1}, ..., e_{s-2,0}, ..., e_{s-2,l-1})$. If we apply ϕ, we have

$$\begin{aligned}\phi(\tau_{s,l}(e)) &= (a_{s-1,0}, ..., a_{s-2,l-1}, a_{s-1,0} + b_{s-1,0} + c_{s-1,0} \\ &\quad , ..., a_{s-2,l-1} + b_{s-2,l-1} + c_{s-2,l-1}, a_{s-1,0} + \\ &\quad 2b_{s-1,0} + c_{s-1,0}, ..., a_{s-2,l-1} + 2b_{s-2,l-1} + \\ &\quad c_{s-2,l-1})\end{aligned}$$

On the other hand,

$$\begin{aligned}\phi(e) &= (a_{0,0}, ..., a_{s-1,l-1}, a_{0,0} + b_{0,0} + c_{0,0}, ..., a_{s-1,l-1} + \\ &\quad b_{s-1,l-1} + c_{s-1,l-1}, a_{0,0} + 2b_{0,0} + c_{0,0}, ..., a_{s-1,l-1} \\ &\quad +2b_{s-1,l-1} + c_{s-1,l-1})\end{aligned}$$

$\Gamma(\varphi(e)) = (a_{s-1,0}, ..., a_{s-2,l-1}, a_{s-1,0} + b_{s-1,0} + c_{s-1,0}, ..., a_{s-2,l-1} + b_{s-2,l-1} + c_{s-2,l-1}, a_{s-1,0} + 2b_{s-1,0} + c_{s-1,0}, ..., a_{s-2,l-1} + 2b_{s-2,l-1} + c_{s-2,l-1})$. So, we have $\varphi\tau_{s,l} = \Gamma\varphi$. ■

Theorem 7: The Gray image of a quasi-cyclic code over R of length n with index l is a l-quasi cyclic code of index 3 over Z_3 with length $3n$.

Proof: Let C be a quasi-cyclic code over R of length n with index l. That is $\tau_{s,l}(C) = C$. If we apply ϕ, we have $\phi(\tau_{s,l}(C)) = \phi(C)$. From the Proposition 6, $\phi(\tau_{s,l}(C)) = \phi(C) = \Gamma(\phi(C))$. So, $\phi(C)$ is a l quasi-cyclic code of index 3 over Z_3 with length $3n$. ■

We denote that $A_1 \otimes A_2 \otimes A_3 = \{(a_1, a_2, a_3) : a_1 \in A_1, a_2 \in A_2, a_3 \in A_3\}$ and $A_1 \oplus A_2 \oplus A_3 = \{a_1 + a_2 + a_3 : a_1 \in A_1, a_2 \in A_2, a_3 \in A_3\}$

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

$$\begin{aligned}C_1 &= \left\{a \in Z_3^n : \exists b, c \in Z_3^n, a + vb + v^2c \in C\right\} \\ C_2 &= \left\{a + b + c \in Z_3^n : a + vb + v^2c \in C\right\} \\ C_3 &= \left\{a + 2b + c \in Z_3^n : a + vb + v^2c \in C\right\}\end{aligned}$$

Then C_1, C_2 and C_3 are ternary linear codes of length n. Moreover, the linear code C of length n over R can be uniquely expressed as $C = (1 + 2v^2)C_1 \oplus \left(2v + 2v^2\right)C_2 \oplus \left(v + 2v^2\right)C_3$.

Theorem 8: Let C be a linear code of length n over R. Then $\phi(C) = C_1 \otimes C_2 \otimes C_3$ and $|C| = |C_1||C_2||C_3|$.

Proof: For any $(a_0, a_1, ..., a_{n-1}, a_0 + b_0 + c_0, a_1 + b_1 + c_1, ..., a_{n-1} + b_{n-1} + c_{n-1}, a_0 + 2b_0 + c_0, a_1 + 2b_1 + c_1, ..., a_{n-1} + 2b_{n-1} + c_{n-1}) \in \phi(C)$. Let $m_i = a_i + vb_i + v^2c_i,\ i = 0, 1, ..., n-1$. Since ϕ is a bijection $m = (m_0, m_1, ..., m_{n-1}) \in C$. By definitions of C_1, C_2 and C_3 we have $(a_0, a_1, ..., a_{n-1}) \in C_1, (a_0 + b_0 + c_0, a_1 + b_1 + c_1, ..., a_{n-1} + b_{n-1} + c_{n-1}) \in C_2, (a_0 + 2b_0 + c_0, a_1 + 2b_1 + c_1, ..., a_{n-1} + 2b_{n-1} + c_{n-1}) \in C_3$. So, $(a_0, a_1, ..., a_{n-1}, a_0 + b_0 + c_0, a_1 + b_1 + c_1, ..., a_{n-1} + b_{n-1} + c_{n-1}, a_0 + 2b_0 + c_0, a_1 + 2b_1 + c_1, ..., a_{n-1} + 2b_{n-1} + c_{n-1}) \in C_1 \otimes C_2 \otimes C_3$. That is $\phi(C) \subseteq C_1 \otimes C_2 \otimes C_3$.

On the other hand, for any $(a, b, c) \in C_1 \otimes C_2 \otimes C_3$ where $a = (a_0, a_1, ..., a_{n-1}) \in C_1$, $b = (a_0 + b_0 + c_0, a_1 + b_1 + c_1, ..., a_{n-1} + b_{n-1} + c_{n-1}) \in C_2$, $c = (a_0 + 2b_0 + c_0, a_1 + 2b_1 + c_1, ..., a_{n-1} + 2b_{n-1} + c_{n-1}) \in C_3$. There are $x = (x_0, x_1, ..., x_{n-1})$, $y = (y_0, y_1, ..., y_{n-1})$, $z = (z_0, z_1, ..., z_{n-1}) \in C$ such that $x_i = a_i + (v + 2v^2)p_i$, $y_i = b_i + \left(1 + 2v^2\right)q_i$, $z_i = c_i + \left(2v + 2v^2\right)r_i$ where $p_i,\ q_i, r_i \in Z_3$ and $0 \le i \le n-1$. Since C is linear we have $m = (1 + 2v^2)x + \left(2v + 2v^2\right)y + \left(v + 2v^2\right)z = a + v(2b + c) + v^2(2a + 2b + 2c) \in C$. It follows then $\phi(m) = (a, b, c)$, which gives $C_1 \otimes C_2 \otimes C_3 \subseteq \phi(C)$.

Therefore, $\phi(C) = C_1 \otimes C_2 \otimes C_3$. The second result is easy to verify. ■

Corollary 9: If $\phi(C) = C_1 \otimes C_2 \otimes C_3$, then $C = (1+2v^2)C_1 \oplus \left(2v+2v^2\right) C_2 \oplus \left(v+2v^2\right) C_3$. It is easy to see that

$$|C| = |C_1|\,|C_2|\,|C_3| = 3^{n-\deg(f_1)}3^{n-\deg(f_2)}3^{n-\deg(f_3)}$$
$$= 3^{3n-(\deg(f_1)+\deg(f_2)+\deg(f_3))}$$

where f_1, f_2 and f_3 are the generator polynomials of C_1, C_2 and C_3, respectively.

Corollary 10: If G_1, G_2 and G_3 are generator matrices of ternary linear codes C_1, C_2 and C_3 respectively, then the generator matrix of C is

$$G = \begin{bmatrix} (1+2v^2)G_1 \\ \left(2v+2v^2\right) G_2 \\ \left(v+2v^2\right) G_3 \end{bmatrix}.$$

We have

$$\phi(G) = \begin{bmatrix} \phi((1+2v^2)G_1) \\ \phi(\left(2v+2v^2\right) G_2) \\ \phi(\left(v+2v^2\right) G_3) \end{bmatrix} = \begin{bmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{bmatrix}.$$

Let d_L minimum Lee weight of linear code C over R. Then, $d_L = d_H(\phi(C)) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}$ where $d_H(C_i)$ denotes the minimum Hamming weights of ternary codes C_1, C_2 and C_3, respectively.

As similiar to section 4 in [4] we have the following Lemma and Examples.

Lemma 11: Let $C = \langle f(x)\rangle$ be a negacyclic code of length n over R and $\phi(f(x)) = (f_1, f_2, f_3)$ with $\deg(\gcd(f_1, x^n+1)) = n-k_1, \deg(\gcd(f_2, x^n+1)) = n-k_2, \deg(\gcd(f_3, x^n+1)) = n-k_3$. Then, $|C| = 3^{k_1+k_2+k_3}$.

Example 12: Let $C = \langle f(x)\rangle = \langle (2v+2v^2)x^2 + (1+2v+2v^2)x + 1\rangle$ be a negacyclic code of length 3 over R. Hence, $\phi(f(x)) = (x+1, x^2+2x+1, x+1)$ and

$$\begin{aligned} f_1 &= \gcd(x+1, x^3+1) = x+1 \\ f_2 &= \gcd(x^2+2x+1, x^3+1) = x^2+2x+1 \\ f_3 &= \gcd(x+1, x^3+1) = x+1 \end{aligned}$$

So we have $|C| = 3^{2+1+2} = 3^5$.

Example 13: Let $C = \langle f(x)\rangle = \langle v^2x^4 + vx^3 + (1+2v^2)x^2 + 2vx + 1\rangle$ be a negacyclic code of length 10 over R. Hence, $\phi(f(x)t) = (x^2+1, x^4+x^3+2x+1, x^4+2x^3+x+1)$ and

$$\begin{aligned} f_1 &= \gcd(x^2+1, x^{10}+1) = x^2+1 \\ f_2 &= \gcd(x^4+x^3+2x+1, x^{10}+1) = x^4+x^3+2x+1 \\ f_3 &= \gcd(x^4+2x^3+x+1, x^{10}+1) = x^4+2x^3+x+1 \end{aligned}$$

So we have $|C| = 3^{8+6+6} = 3^{20}$.

Let $h_i(x) = (x^n+1)/(\gcd(x^n+1, f_i))$. Hence, $C^\perp = \left\langle \phi^{-1}\left(h_{1_R}(x), h_{2_R}(x), h_{3_R}(x)\right)\right\rangle$ where $h_{i_R}(x)$ be the reciprocal polynomial of $h_i(x)$ for $i = 1, 2, 3$. By using the previous Example 13,

$$\begin{aligned} C^\perp &= \left\langle \phi^{-1}\left(h_{1_R}(x), h_{2_R}(x), h_{3_R}(x)\right)\right\rangle \\ &= \langle \phi^{-1}(x^8+2x^6+x^4+2x^2+1, x^6+x^5+x^4+x^2 \\ &\quad +2x+1, x^6+2x^5+x^4+x^2+x+1)\rangle \\ &= \langle (1+2v^2)x^8 + (2+2v^2)x^6 + vx^5 + x^4 \\ &\quad +(2+2v^2)x^2 + 2vx + 1\rangle \end{aligned}$$

IV. Quantum Codes From Cyclic (Negacyclic) Codes Over R

Theorem 14: Let $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ be linear codes over GF(q) with $C_2^\perp \subseteq C_1$. Furthermore, let $d = min\{wt(v) : v \in (C_1 \backslash C_2^\perp) \cup (C_2^\perp \backslash C_1)\} \geq \min\{d_1, d_2\}$.Then there exists a quantum error-correcting code $C = [n, k_1+k_2-n, d]_q$.In particular, if $C_1^\perp \subseteq C_1$, then there exists a quantum error-correcting code $C = [n, n-2k_1, d_1]$, where $d_1 = min\{wt(v) : v \in (C_1^\perp \backslash C_1)\}$ [16].

Proposition 15: Let $C = (1+2v^2)C_1 \oplus \left(2v+2v^2\right) C_2 \oplus \left(v+2v^2\right) C_3$ be a linear code over R. Then C is a cyclic code over R iff C_1, C_2 and C_3 are cyclic codes.

Proof: Let $(a_0, a_1, ..., a_{n-1}) \in C_1$, $(b_0, b_1, ..., b_{n-1}) \in C_2$ and $(c_0, c_1, ..., c_{n-1}) \in C_3$. Assume that $m_i = (1+2v^2)a_i + \left(2v+2v^2\right) b_i + \left(v+2v^2\right) c_i$ for $i = 0, 1, ..., n-1$. Then $(m_0, m_1, ..., m_{n-1}) \in C$. Since C is a cyclic code, it follows that $(m_{n-1}, m_0, ..., m_{n-2}) \in C$. Note that $(m_{n-1}, m_0, ..., m_{n-2}) = (1+2v^2)(a_{n-1}, a_0, ..., a_{n-2}) + (2v+2v^2)(b_{n-1}, b_0, ..., b_{n-2}) + (v+2v^2)(c_{n-1}, c_0, ..., c_{n-2})$. Hence $(a_{n-1}, a_0, ..., a_{n-2}) \in C_1, (b_{n-1}, b_0, ..., b_{n-2}) \in C_2$ and $(c_{n-1}, c_0, ..., c_{n-2}) \in C_3$. Therefore,$C_1, C_2$ and C_3 cyclic codes over Z_3.

Conversely, suppose that C_1, C_2 and C_3 cyclic codes over Z_3. Let $(m_0, m_1, ..., m_{n-1}) \in C$ where $m_i = (1+2v^2)a_i + \left(2v+2v^2\right) b_i + \left(v+2v^2\right) c_i$ for $i = 0, 1, ..., n-1$. Then $(a_0, a_1, ..., a_{n-1}) \in C_1, (b_0, b_1, ..., b_{n-1}) \in C_2$ and $(c_0, c_1, ..., c_{n-1}) \in C_3$. Note that $(m_{n-1}, m_0, ..., m_{n-2}) = (1+2v^2)(a_{n-1}, a_0, ..., a_{n-2}) + \left(2v+2v^2\right)(b_{n-1}, b_0, ..., b_{n-2}) + \left(v+2v^2\right)(c_{n-1}, c_0, ..., c_{n-2}) \in C = (1+2v^2)C_1 \oplus \left(2v+2v^2\right) C_2 \oplus \left(v+2v^2\right) C_3$. So, C is cyclic code over R. ■

Proposition 16: Let $C = (1+2v^2)C_1 \oplus \left(2v+2v^2\right) C_2 \oplus \left(v+2v^2\right) C_3$ be a linear code over R. Then C is a negacyclic code over R iff C_1, C_2 and C_3 are negacyclic codes.

Proof: Let $(a_0, a_1, ..., a_{n-1}) \in C_1$, $(b_0, b_1, ..., b_{n-1}) \in C_2$ and $(c_0, c_1, ..., c_{n-1}) \in C_3$. Assume that $m_i = (1+2v^2)a_i + \left(2v+2v^2\right) b_i + \left(v+2v^2\right) c_i$ for $i = 0, 1, ..., n-1$. Then $(m_0, m_1, ..., m_{n-1}) \in C$. Since C is a negacyclic code, it follows that $(-m_{n-1}, m_0, ..., m_{n-2}) \in C$. Note that $(-m_{n-1}, m_0, ..., m_{n-2}) = (1+2v^2)(-a_{n-1}, a_0, ..., a_{n-2}) + (2v+2v^2)(-b_{n-1}, b_0, ..., b_{n-2}) + (v+2v^2)(-c_{n-1}, c_0, ..., c_{n-2})$. Hence $(-a_{n-1}, a_0, ..., a_{n-2}) \in C_1, (-b_{n-1}, b_0, ..., b_{n-2}) \in C_2$ and $(-c_{n-1}, c_0, ..., c_{n-2}) \in C_3$. Therefore, C_1, C_2 and C_3 negacyclic codes over Z_3.

Conversely, suppose that C_1, C_2 and C_3 negacyclic codes over Z_3. Let $(m_0, m_1, ..., m_{n-1}) \in C$ where $m_i = (1+2v^2)a_i + (2v+2v^2)b_i + (v+2v^2)c_i$ for $i = 0, 1, ..., n-1$. Then $(a_0, a_1, ..., a_{n-1}) \in C_1$,

$(b_0, b_1, ..., b_{n-1}) \in C_2$ and $(c_0, c_1, ..., c_{n-1}) \in C_3$. Note that $(-m_{n-1}, m_0, ..., m_{n-2}) = (1 + 2v^2)(-a_{n-1}, a_0, ..., a_{n-2}) + (2v+2v^2)(-b_{n-1}, b_0, ..., b_{n-2}) + (v + 2v^2)(-c_{n-1}, c_0, ..., c_{n-2}) \in C = (1 + 2v^2)C_1 \oplus (2v + 2v^2)C_2 \oplus (v + 2v^2)C_3$. So, C is negacyclic code over R. ■

Proposition 17: Suppose $C = (1 + 2v^2)C_1 \oplus \left(2v + 2v^2\right) C_2 \oplus \left(v + 2v^2\right) C_3$ is a cyclic (negacyclic) code of length n over R. Then

$$C =< (1 + 2v^2)f_1, \left(2v + 2v^2\right) f_2, \left(v + 2v^2\right) f_3 >$$

and $|C| = 3^{3n-(\deg f_1+\deg f_2+\deg f_3)}$ where f_1, f_2 and f_3 generator polynomials of C_1, C_2 and C_3 respectively.

Proposition 18: Suppose C is a cyclic (negacyclic) code of length n over R, then there is a unique polynomial $f(x)$ such that $C = \langle f(x)\rangle$ and $f(x) \mid x^n-1$ ($f(x) \mid x^n+1$) where $f(x) = (1+2v^2)f_1(x)+\left(2v + 2v^2\right) f_2(x)+\left(v + 2v^2\right) f_3(x)$.

Proposition 19: Let C be a linear code of length n over R, then $C^\perp = (1+2v^2)C_1^\perp \oplus \left(2v + 2v^2\right) C_2^\perp \oplus \left(v + 2v^2\right) C_3^\perp$. Furthermore, C is self-dual code iff C_1, C_2 and C_3 are self-dual codes over Z_3.

Proposition 20: If $C = (1 + 2v^2)C_1 \oplus \left(2v + 2v^2\right) C_2 \oplus \left(v + 2v^2\right) C_3$ is a cyclic (negacyclic) code of length n over R. Then

$$C^\perp = \left\langle (1 + 2v^2)h_1^* + \left(2v + 2v^2\right) h_2^* + \left(v + 2v^2\right) h_3^* \right\rangle$$

and $\left|C^\perp\right| = 3^{\deg f_1+\deg f_2+\deg f_3}$ where for $i = 1, 2, 3$, h_i^* are the reciprocal polynomials of h_i i.e., $h_i(x) = (x^n - 1)/f_i(x)$,($h_i(x) = (x^n + 1)/f_i(x)$), $h_i^*(x) = x^{\deg h_i} h_i\left(x^{-1}\right)$ for $i = 1, 2, 3$.

Lemma 21: A ternary linear cyclic (negacyclic) code C with generator polynomial $f(x)$ contains its dual code iff

$$x^n - 1 \equiv 0\,(mod f f^*)\,, \qquad (x^n + 1 \equiv 0\,(mod f f^*)\,)$$

where f^* is the reciprocal polynomial of f.

Theorem 22: Let $C = \langle (1 + 2v^2)f_1, (2v + 2v^2)f_2, (v + 2v^2)f_3\rangle$ be a cyclic (negacyclic) code of length n over R. Then $C^\perp \subseteq C$ iff $x^n - 1 \equiv 0\,(mod f_i f_i^*)$ $(x^n + 1 \equiv 0\,(mod f_i f_i^*))$ for $i = 1, 2, 3$.

Proof: Let $x^n - 1 \equiv 0\,(mod f_i f_i^*)$ $(x^n + 1 \equiv 0\,(mod f_i f_i^*))$ for $i = 1, 2, 3$. Then $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2, C_3^\perp \subseteq C_3$. By using $(1 + 2v^2)C_1^\perp \subseteq (1 + 2v^2)C_1$, $\left(2v + 2v^2\right) C_2^\perp \subseteq \left(2v + 2v^2\right) C_2$, $\left(v + 2v^2\right) C_3^\perp \subseteq \left(v + 2v^2\right) C_3$. We have $(1 + 2v^2)C_1^\perp \oplus \left(2v + 2v^2\right) C_2^\perp \oplus \left(v + 2v^2\right) C_3^\perp \subseteq (1+2v^2)C_1 \oplus \left(2v + 2v^2\right) C_2 \oplus \left(v + 2v^2\right) C_3$. So, $\langle (1 + 2v^2)h_1^* + \left(2v + 2v^2\right) h_2^* + \left(v + 2v^2\right) h_3^*\rangle \subseteq \langle (1 + 2v^2)f_1, \left(2v + 2v^2\right) f_2, \left(v + 2v^2\right) f_3\rangle$. That is $C^\perp \subseteq C$.

Conversely, if $C^\perp \subseteq C$, then $(1 + 2v^2)C_1^\perp \oplus \left(2v + 2v^2\right) C_2^\perp \oplus \left(v + 2v^2\right) C_3^\perp \subseteq (1 + 2v^2)C_1 \oplus \left(2v + 2v^2\right) C_2 \oplus \left(v + 2v^2\right) C_3$. By thinking $mod(1 + 2v^2)$, $mod\left(2v + 2v^2\right)$ and $mod\left(v + 2v^2\right)$ respectively we have $C_i^\perp \subseteq C_i$ for $i = 1, 2, 3$. Therefore, $x^n - 1 \equiv 0\,(mod f_i f_i^*)$ $(x^n + 1 \equiv 0\,(mod f_i f_i^*))$ for $i = 1, 2, 3$. ■

Corollary 23: $C = (1 + 2v^2)C_1 \oplus \left(2v + 2v^2\right) C_2 \oplus \left(v + 2v^2\right) C_3$ is a cyclic (negacyclic) code of length n over R. Then $C^\perp \subseteq C$ iff $C_i^\perp \subseteq C_i$ for $i = 1, 2, 3$.

Example 24: Let $n = 6, R = Z_3 + vZ_3 + v^2Z_3, v^3 = v$. We have $x^6 - 1 = (2x^2 + 2)(x^2 + 2)(2x^2 + 1) = f_1 f_2 f_3$ in $Z_3[x]$. Hence,

$$\begin{aligned} f_1^* &= 2x^2 + 2 = f_1 \\ f_2^* &= 2x^2 + 1 = f_3 \\ f_3^* &= x^2 + 2 = f_2 \end{aligned}$$

Let $C = \left\langle (1 + 2v^2)f_2, \left(2v + 2v^2\right) f_2, \left(v + 2v^2\right) f_3 \right\rangle$. Obviously $x^6 - 1$ is divisibly by $f_i f_i^*$ for $i = 2, 3$. Thus we have $C^\perp \subseteq C$.

Example 25: Let $n = 10, R = Z_3 + vZ_3 + v^2Z_3, v^3 = v$. We have $x^{10}+1 = (x^2+1)(x^4+x^3+2x+1)(x^4+2x^3+x+1) = g_1 g_2 g_3$ in $Z_3[x]$. Hence,

$$\begin{aligned} g_1^* &= x^2 + 1 = g_1 \\ g_2^* &= x^4 + 2x^3 + x + 1 = g_3 \\ g_3^* &= x^4 + x^3 + 2x + 1 = g_2 \end{aligned}$$

Let $C = \left\langle (1 + 2v^2)g_2, \left(2v + 2v^2\right) g_2, \left(v + 2v^2\right) g_3 \right\rangle$. Obviously $x^{10} + 1$ is divisibly by $g_i g_i^*$ for $i = 2, 3$. Thus we have $C^\perp \subseteq C$.

Theorem 26: Let C be linear code of length n over R with $|C| = 3^{3k_1+2k_2+k_3}$ and minimum distance d. Then $\phi(C)$ is ternary linear $[3n, 3k_1 + 2k_2 + k_3, d]$ code.

Using Theorem 14 and Theorem 22 we can construct quantum codes.

Theorem 27: Let $(1 + 2v^2)C_1 \oplus \left(2v + 2v^2\right) C_2 \oplus \left(v + 2v^2\right) C_3$ be a cyclic (negacyclic) code of arbitrary length n over R with type $27^{k_1}9^{k_2}3^{k_3}$. If $C_i^\perp \subseteq C_i$ where $i = 1, 2, 3$ then $C^\perp \subseteq C$ and there exists a quantum error-correcting code with parameters $[[3n, 2(3k_1 + 2k_2 + k_3) - 3n, d_L]]$ where d_L is the minimum Lee weights of C.

Example 28: Let $n = 6$. We have $x^6 - 1 = (2x^2+2)(x^2 + 2)(2x^2+1)$ in $Z_3[x]$. Let $f_1(x) = f_2(x) = x^2+2$, $f_3 = 2x^2 + 1$. Thus $C =< (1 + 2v^2)f_1, \left(2v + 2v^2\right) f_2, \left(v + 2v^2\right) f_3 >$. C is a linear cyclic code of length 6.The dual code $C^\perp = \left\langle (1 + 2v^2)h_1^*, \left(2v + 2v^2\right) h_2^*, \left(v + 2v^2\right) h_3^* \right\rangle$ can be obtained of Proposition 20. Clearly, $C^\perp \subseteq C$. Hence, we obtain a quantum code with parameters $[[18, 6, 2]]$.

Example 29: Let $n = 8$. We have $x^8 - 1 = (x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$ in $Z_3[x]$. Let $f_1(x) = f_2(x) = f_3(x) = x^2 + 1$. Thus $C = \langle (1 + 2v^2)f_1, \left(2v + 2v^2\right) f_2, \left(v + 2v^2\right) f_3\rangle$. C is a linear cyclic code of length 8. Hence, we obtain a quantum code with parameters $[[24, 12, 2]]$.

Example 30: Let $n = 12$. We have $x^{12} - 1 = (x - 1)^3 \left(x^3 + x^2 + x + 1\right)^3$ in $Z_3[x]$. Let $f_1(x) = f_2(x) = f_3(x) = x^3 + x^2 + x + 1$.Thus $C = \langle (1 + 2v^2)f_1, \left(2v + 2v^2\right) f_2, \left(v + 2v^2\right) f_3\rangle$. C is a linear cyclic code of length 12. The dual code $C^\perp = \langle (1 + 2v^2)h_1^*, (2v + 2v^2)h_2^*, (v + 2v^2)h_3^*\rangle$ can be obtained of Proposition 20. Clearly, $C^\perp \subseteq C$. Hence, we obtain a quantum code with parameters $[[36, 18, 2]]$.

Let $n = 27$. We have $x^{27} - 1 = (x - 1)^3(x^3 - 1)^4(x^6 - 2x^3+1)^2$ in $Z_3[x]$. Let $f_1(x) = f_2(x) = f_3(x) = x^6 - 2x^3 + 1$. Hence, we obtain a quantum code with parameters $[[81, 45, 2]]$.

Let $n = 30$. We have $x^{30} - 1 = (x^2 + 2)^3(x^4 + x^3 + x^2 + x + 1)^3(x^4 + 2x^3 + x^2 + 2x + 1)^3$ in $Z_3[x]$. Let $f_1(x) = f_3(x) = x^4 + x^3 + x^2 + x + 1$, $f_2(x) = x^4 + 2x^3 + x^2 + 2x + 1$. Hence, we obtain a quantum code with parameters $[[90, 66, 2]]$.

Example 31: Let $n = 3$. We have $x^3 + 1 = (x + 1)^3$ in $Z_3[x]$. Let $f_1(x) = f_2(x) = f_3(x) = x + 1$. Thus $C = \langle (1 + 2v^2)f_1, (2v + 2v^2) f_2, (v + 2v^2) f_3 \rangle$. C is a linear negacyclic code of length 3. The dual code $C^{\perp} =< (1 + 2v^2)h_1^*, (2v + 2v^2)h_2^*, (v + 2v^2) h_3^* >$ can be obtained of Proposition 20. Clearly, $C^{\perp} \subseteq C$. Hence, we obtain a quantum code with parameters $[[9, 3, 2]]$.

Example 32: Let $n = 10$. We have $x^{10} + 1 = (x^2 + 1)(x^4 + x^3 + 2x + 1)(x^4 + 2x^3 + x + 1)$ in $Z_3[x]$. Let $f_1(x) = x^4 + x^3 + 2x + 1$, $f_2(x) = f_3(x) = x^4 + 2x^3 + x + 1$. Thus $C = \langle (1 + 2v^2)f_1, (2v + 2v^2) f_2, (v + 2v^2) f_3 \rangle$. C is a linear negacyclic code of length 10. The dual code $C^{\perp} = \langle (1 + 2v^2)h_1^*, (2v + 2v^2) h_2^*, (v + 2v^2) h_3^* \rangle$ can be obtained of Proposition 20. Clearly, $C^{\perp} \subseteq C$. Hence, we obtain a quantum code with parameters $[[30, 6, 4]]$.

Example 33: Let $n = 12$. We have $x^{12}+1 = (x^4+1)(x^2+x+2)(x^2+2x+2)(2x^2+2x+1 \left(2x^2 + x + 1\right)$ in $Z_3[x]$. Let $f_1(x) = x^2+x+2$, $f_2(x) = 2x^2+x+1$, $f_3(x) = x^2+2x+2$. Thus $C = \langle (1 + 2v^2)f_1, (2v + 2v^2) f_2, (v + 2v^2) f_3 \rangle$. C is a linear negacyclic code of length 12. The dual code $C^{\perp} =< (1+2v^2)h_1^*, (2v + 2v^2) h_2^*, (v + 2v^2) h_3^* >$ can be obtained of Proposition 20. Clearly, $C^{\perp} \subseteq C$. Hence, we obtain a quantum code with parameters $[[36, 24, 2]]$.

V. CONSTACYCLIC CODES OVER R

Let $\lambda = \alpha + \beta v + \gamma v^2$ be unit element of R. Note that $\lambda^n = 1$ if n even $\lambda^n = \lambda$ if n odd. So we only study λ-constacyclic codes of odd length.

Proposition 34: Let ϱ be the map of $R[x] / \langle x^n - 1 \rangle$ into $R[x] / \langle x^n - \lambda \rangle$ defined by $\varrho(a(x)) = a(\lambda x)$. If n is odd, then ϱ is a ring isomorphism.

Proof: The proof is straightforward if n is odd, $a(x) \equiv b(x)(mod(x^n - 1))$ iff $a(\lambda x) \equiv b(\lambda x)(mod(x^n - \lambda))$ ■

Corollary 35: I is an ideal of $R[x] / \langle x^n - 1 \rangle$ if and only if $\varrho(I)$ is an ideal of $R[x] / \langle x^n - \lambda \rangle$.

Corollary 36: Let $\overline{\varrho}$ be the permutation of R^n with n odd, such that $\overline{\varrho}(a_0, a_1, ..., a_{n-1}) = (a_0, \lambda a_1, \lambda^2 a_2 ..., \lambda^{n-1} a_{n-1})$ and C be a subset of R^n then C is a linear cyclic code iff $\overline{\varrho}(C)$ is a linear λ-constacyclic code.

Corollary 37: C is a cyclic code of parameters $(n, 3^k, d)$ over R iff $\overline{\varrho}(C)$ is a λ-constacyclic code of parameters $(n, 3^k, d)$ over R, when n is odd.

Theorem 38: Let λ be a unit in R. Let $C = (1+2v^2)C_1 \oplus (2v + 2v^2) C_2 \oplus (v + 2v^2) C_3$ be a linear code of length n over R. Then C is a λ-constacyclic code of length n over R iff C_i are either cyclic codes or negacyclic codes of length n over Z_3 for $i = 1, 2, 3$.

Proof: Let ν be the λ-constacyclic shift on R^n. Let C be a λ-constacyclic code of length n over R.Let $(a_0, a_1, ..., a_{n-1}) \in C_1, (b_0, b_1, ..., b_{n-1}) \in C_2$ and $(c_0, c_1, ..., c_{n-1}) \in C_3$. Then the corresponding element of C is $(m_0, m_1, ..., m_{n-1}) = (1 + 2v^2)(a_0, a_1, ..., a_{n-1}) + (2v + 2v^2)(b_0, b_1, ..., b_{n-1}) + (v+2v^2)(c_0, c_1, ..., c_{n-1})$. Since C is a λ-constacyclic code so, $\nu(m) = (\lambda m_{n-1}, m_0, ..., m_{n-2}) \in C$ where $m_i = a_i + b_i v + v^2 c_i$ for $i = 0, 1, ..., n-1$. Let $\lambda = \alpha + v\beta + v^2\gamma$, where $\alpha, \beta, \gamma \in Z_3$. $\nu(m) = (1 + 2v^2)(\lambda a_{n-1}, a_0, ..., a_{n-2}) + (2v + 2v^2)(\lambda b_{n-1}, b_0, ..., b_{n-2}) + (v + 2v^2)(\lambda c_{n-1}, c_0, ..., c_{n-2})$. Since the units of Z_3 are 1 and -1, so $\alpha = \mp 1$. Therefore we have obtained the desired result. The other side it is seen easily. ■

VI. SKEW CODES OVER R

We are interested in studying skew codes using the ring $R = Z_3 + vZ_3 + v^2 Z_3$ where $v^3 = v$. We define non-trivial ring automorphism θ on the ring R by $\theta\left(a + vb + v^2c\right) = a + 2bv + v^2c$ for all $a + vb + v^2c \in R$.

The ring $R[x, \theta] = \{a_0 + a_1 x + ... + a_{n-1}x^{n-1} : a_i \in R, n \in N\}$ is called a skew polynomial ring. This ring is a non-commutative ring. The addition in the ring $R[x, \theta]$ is the usual polynomial addition and multiplication is defined using the rule, $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$. Note that $\theta^2(a) = a$ for all $a \in R$. This implies that θ is a ring automorphism of order 2.

Definition 39: A subset C of R^n is callled a skew cyclic code of length n if C satisfies the following conditions,
$i)$ C is a submodule of R^n,
$ii)$ If $c = (c_0, c_1, ..., c_{n-1}) \in C$, then $\sigma_\theta(c) = \left(\theta(c_{n-1}), \theta(c_0), ..., \theta(c_{n-2})\right) \in C$.

Let $f(x) + (x^n - 1)$ be an element in the set $R_n = R[x, \theta] / (x^n - 1)$ and let $r(x) \in R[x, \theta]$. Define multiplication from left as follows,

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

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

Theorem 40: R_n is a left $R[x, \theta]$-module where multiplication defined as in above.

Theorem 41: A code C in R_n is a skew cyclic code if and only if C is a left $R[x, \theta]$-submodule of the left $R[x, \theta]$-module R_n.

Theorem 42: Let C be a skew cyclic code in R_n and let $f(x)$ be a polynomial in C of minimal degree. If $f(x)$ is monic polynomial, then $C = (f(x))$ where $f(x)$ is a right divisor of $x^n - 1$.

Theorem 43: A module skew cyclic code of length n over R is free iff it is generated by a monic right divisor $f(x)$ of $x^n - 1$. Moreover, the set $\{f(x), xf(x), x^2 f(x), ..., x^{n-\deg(f(x))-1} f(x)\}$ forms a basis of C and the rank of C is $n - \deg(f(x))$.

Theorem 44: Let n be odd and C be a skew cyclic code of length n. Then C is equivalent to cyclic code of length n over R.

Proof: Since n is odd, $gcd(2, n) = 1$. Hence there exist integers b, c such that $2b + nc = 1$. So $2b = 1 - nc = 1 + zn$ where $z > 0$. Let $a(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1}$ be a codeword in C. Note that $x^{2b}a(x) = \theta^{2b}(a_0)x^{1+zn} +$

$\theta^{2b}(a_1)x^{2+zn} + ... + \theta^{2b}(a_{n-1})x^{n+zn} = a_{n-1} + a_0x + ... + a_{n-2}x^{n-2} \in C$. Thus C is a cyclic code of length n. ∎

Corollary 45: Let n be odd. Then the number of distinct skew cyclic codes of length n over R is equal to the number of ideals in $R[x]/(x^n-1)$ because of Theorem 44. If $x^n - 1 = \prod_{i=0}^{r} p_i^{s_i}(x)$ where $p_i(x)$ are irreducible polynomials over Z_3. Then the number of distinct skew cyclic codes of length n over R is $\prod_{i=0}^{r}(s_i+1)^3$.

Example 46: Let $n = 27$ and $f(x) = x^3 - 1$. Then $f(x)$ generates a skew cyclic codes of length 27. This code is equivalent to a cyclic code of length 27. Since $x^{27} - 1 = (x-1)^3(x^3-1)^4(x^6-2x^3+1)^2$, it follows that there are 60^3 skew cyclic code of length 27.

Definition 47: A subset C of R^n is called a skew quasi-cyclic code of length n if C satisfies the following conditions,
$i)$ C is a submodule of R^n,
$ii)$ If $e = (e_{0,0}, ..., e_{0,l-1}, e_{1,0}, ..., e_{1,l-1}, ..., e_{s-1,0}, .., e_{s-1,l-1}) \in C$, then
$\tau_{\theta,s,l}(e) = (\theta(e_{s-1,0}), ..., \theta(e_{s-1,l-1}), \theta(e_{0,0}), ..., \theta(e_{0,l-1}), ..., \theta(e_{s-2,0}), ..., \theta(e_{s-2,l-1})) \in C$.

We note that $x^s - 1$ is a two sided ideal in $R[x,\theta]$ if $m|s$ where m is the order of θ and equal to two. So $R[x,\theta]/(x^s - 1)$ is well defined.

The ring $R_s^l = (R[x,\theta]/(x^s-1))^l$ is a left $R_s = R[x,\theta]/(x^s-1)$ module by the following multiplication on the left $f(x)(g_1(x), ..., g_l(x)) = (f(x)g_1(x), ...f(x)g_l(x))$. If the map γ is defined by

$$\gamma : R^n \longrightarrow R_s^l$$

$(e_{0,0}, ..., e_{0,l-1}, e_{1,0}, ..., e_{1,l-1}, ..., e_{s-1,0}, ..., e_{s-1,l-1}) \mapsto (e_0(x), ..., e_{l-1}(x))$ such that $e_j(x) = \sum_{i=0}^{s-1} e_{i,j}x^i \in R_s^l$ where $j = 0, 1, ..., l-1$ then the map γ gives a one to one correspondence R^n and the ring R_s^l.

Theorem 48: A subset C of R^n is a skew quasi-cyclic code of length $n = sl$ and index l if and only if $\gamma(C)$ is a left R_s-submodule of R_s^l.

A code C is said to be skew constacyclic if C is closed the under the skew constacyclic shift $\sigma_{\theta,\lambda}$ from R^n to R^n defined by $\sigma_{\theta,\lambda}((c_0, c_1, ..., c_{n-1})) = (\theta(\lambda c_{n-1}), \theta(c_0), ..., \theta(c_{n-2}))$.

Privately, such codes are called skew cyclic and skew negacyclic codes when λ is 1 and -1, respectively.

Theorem 49: A code C of length n over R is skew constacyclic iff the skew polynomial representation of C is a left ideal in $R[x,\theta]/(x^n - \lambda)$.

VII. The Gray Images of Skew Codes Over R

Proposition 50: Let σ_θ be the skew cyclic shift on R^n, let ϕ be the Gray map from R^n to Z_3^{3n} and let φ be as in the preliminaries. Then $\phi\sigma_\theta = \rho\varphi\phi$ where $\rho(x,y,z) = (x,z,y)$ for every $x, y, z \in Z_3^n$.

Proof: Let $r_i = a_i + vb_i + v^2c_i$ be the elements of R, for $i = 0, 1, ..., n-1$. We have $\sigma_\theta(r_0, r_1, ..., r_{n-1}) = (\theta(r_{n-1}), \theta(r_0), ..., \theta(r_{n-2}))$. If we apply ϕ, we have

$$\begin{aligned}\phi(\sigma_\theta(r_0, ..., r_{n-1})) &= \phi(\theta(r_{n-1}), \theta(r_0), ..., \theta(r_{n-2})) \\ &= (a_{n-1}, ..., a_{n-2}, a_{n-1} + 2b_{n-1} + c_{n-1}, ..., a_{n-2} + 2b_{n-2} + c_{n-2}, \\ &\quad a_{n-1} + b_{n-1} + c_{n-1}, ..., a_{n-2} + b_{n-2} + c_{n-2})\end{aligned}$$

On the other hand, $\phi(r_0, ..., r_{n-1}) = (a_0, ..., a_{n-1}, a_0 + b_0 + c_0, ..., a_{n-1} + b_{n-1} + c_{n-1}, a_0 + 2b_0 + c_0, ..., a_{n-1} + 2b_{n-1} + c_{n-1})$. If we apply φ, we have

$\varphi(\phi(r_0, r_1, ..., r_{n-1})) = (a_{n-1}, ..., a_{n-2}, a_{n-1} + b_{n-1} + c_{n-1}, ..., a_{n-2} + b_{n-2} + c_{n-2}, a_{n-1} + 2b_{n-1} + c_{n-1}, ..., a_{n-2} + 2b_{n-2} + c_{n-2})$. If we apply ρ, we have $\rho(\varphi(\phi(r_0, r_1, ..., r_{n-1}))) = (a_{n-1}, ..., a_{n-2}, a_{n-1} + 2b_{n-1} + c_{n-1}, ..., a_{n-2} + 2b_{n-2} + c_{n-2}, a_{n-1} + b_{n-1} + c_{n-1}, ..., a_{n-2} + b_{n-2} + c_{n-2})$. So, we have $\phi\sigma_\theta = \rho\varphi\phi$. ∎

Theorem 51: The Gray image a skew cyclic code over R of length n is permutation equivalent to quasi-cyclic code of index 3 over Z_3 with length $3n$.

Proof: Let C be a skew cyclic codes over S of length n. That is $\sigma_\theta(C) = C$. If we apply ϕ, we have $\phi(\sigma_\theta(C)) = \phi(C)$. From the Proposition 50, $\phi(\sigma_\theta(C)) = \phi(C) = \rho(\varphi(\phi(C)))$. So, $\phi(C)$ is permutation equivalent to quasi-cyclic code of index 3 over Z_3 with length $3n$. ∎

Proposition 52: Let $\tau_{\theta,s,l}$ be skew quasi-cyclic shift on R^n, let ϕ be the Gray map from R^n to Z_3^{3n}, let Γ be as in the preliminaries, let ρ be as above. Then $\phi\tau_{\theta,s,l} = \rho\Gamma\phi$.

Theorem 53: The Gray image a skew quasi-cyclic code over R of length n with index l is permutation equivalent to l quasi-cyclic code of index 3 over Z_3 with length $3n$.

Proposition 54: Let $\sigma_{\theta,\lambda}$ be skew constacyclic shift on R^n, let ϕ be the Gray map from R^n to Z_3^{3n}, let ρ be as above. Then $\phi\nu = \rho\phi\sigma_{\theta,\lambda}$.

Theorem 55: The Gray image a skew constacyclic code over R of length n is permutation equivalent to the Gray image of a constacyclic code over Z_3 with length $3n$.

The proofs of Proposition 52, 54 and Theorem 53, 55 are similiar to the proofs Proposition 50 and Theorem 51.

VIII. Quasi-constacyclic and Skew Quasi-constacyclic Codes over R

Let $M_s = R[x]/\langle x^s - \lambda\rangle$ where λ is a unit element of R.

Definition 56: A subset C of R^n is a called a quasi-constacyclic code of length $n = ls$ with index l if
$i)$ C is a submodule of R^n,
$ii)$ if $e = (e_{0,0}, ..., e_{0,l-1}, e_{1,0}, ..., e_{1,l-1}, ..., e_{s-1,0}, ..., e_{s-1,l-1}) \in C$ then
$\nabla_{\lambda,l}(e) = (\lambda e_{s-1,0}, ..., \lambda e_{s-1,l-1}, e_{0,0}, ..., e_{0,l-1}, e_{1,0}, ..., e_{1,l-1}, ..., e_{s-2,0}, ..., e_{s-2,l-1}) \in C$.

When $\lambda = 1$ the quasi-constacyclic codes are just quasi-cyclic codes.

Since $x^s - \lambda = f_1(x)f_2(x)...f_r(x)$, it follows that

$(R[x]/(x^s-\lambda))^l \cong (R[x]/(f_1(x)))^l \times (R[x]/(f_2(x)))^l \times ... \times (R[x]/(f_r(x)))^l$.

Every submodule of $(R[x]/(x^s-\lambda))^l$ is a direct product of submodules of $(R[x]/(f_t(x)))^l$ for $1 \leq t \leq r$.

Theorem 57: If $(s,3)=1$ then a quasi-constacyclic code of length $n=sl$ with index l over R is a direct product of linear codes over $R[x]/(f_t(x))$ for $1 \leq t \leq r$.

Let $x^s-\lambda = f_1(x)f_2(x)...f_r(x)$ be the factorization of $x^s-\lambda$ into irreducible polynomials. Thus, if $(s,3)=1$ and C_i is a linear code of length l over $R[x]/(f_t(x))$ for $1 \leq t \leq r$, then $\prod_{t=1}^{r} C_t$ is a quasi-constacyclic code of length $n=sl$ over R with $\prod_{t=1}^{r} |C_t|$ codewords.

Define a map $\chi : R^n \to M_s^l$ by $\chi(e) = (e_0(x), e_1(x), ..., e_{l-1}(x))$ where $e_j(x) = \sum_{i=o}^{s-1} e_{ij}x^i \in M_s$, $j=0,1,...,l-1$.

Lemma 58: Let $\chi(C)$ denote the image of C under χ. The map χ induces a one to one correspondence between quasi-constacyclic codes over R of length n with index l and linear codes over M_s of length l.

We define a conjugation map on M_s as one that acts as the identity on the elements of R and that sends x to $x^{-1}=x^{s-1}$, and extended linearly.

We define on $R^{n=sl}$ the usual Euclidean inner product for

$$e=(e_{0,0},...,e_{0,l-1},e_{1,0},...,e_{1,l-1},...,e_{s-1,0},...,e_{s-1,l-1})$$

and

$$c=(c_{0,0},...,c_{0,l-1},c_{1,0},...,c_{1,l-1},...,c_{s-1,0},...,c_{s-1,l-1})$$

we define $e.c = \sum_{i=0}^{s-1}\sum_{j=0}^{l-1} e_{ij}c_{ij}$.

On M_s^l, we define the Hermitian inner product for $a(x) = (a_0(x), a_1(x), ..., a_{l-1}(x))$ and $b(x) = (b_0(x), b_1(x), ..., b_{l-1}(x))$,

$$\langle a,b\rangle = \sum_{j=0}^{l-1} a_j(x)\overline{b_j(x)}.$$

Theorem 59: Let $e,c \in R^n$. Then $\left(\nabla_{\lambda,l}^k(e)\right).c=0$ for all $k=0,...,s-1$ iff $\langle \chi(e), \chi(c)\rangle = 0$.

Corollary 60: Let C be a quasi-constacyclic code of length sl with index l over R and $\chi(C)$ be its image in M_s^l under χ. Then $\chi(C)^\perp = \chi(C^\perp)$, where the dual in R^{sl} is taken with respect to the Euclidean inner product, while the dual in M_s^l is taken with respect to the Hermitian inner product. The dual of a quasi-constacyclic code of length sl with index l over R is a quasi-constacyclic code of length sl with index l over .

From [22] we get the following results.

Theorem 61: Let C be a quasi-constacyclic code of length n=sl with index l over R. Let $C^\perp$ is the dual of C. If $C = C_1 \oplus C_2 \oplus ... \oplus C_r$ then $C^\perp = C_1^\perp \oplus C_2^\perp \oplus ... \oplus C_r^\perp$.

Theorem 62: Let $C = C_1 \oplus C_2 \oplus ... \oplus C_r$ be a quasi-constacyclic code of length n=sl with index l over R where C_t is a free linear code of length l with rank k_t over $R[x]/(f_t(x))$for $1 \leq t \leq r$. Then C is a κ-generator quasi-constacyclic code and $C^\perp$ is an $(l-\kappa')$-generator quasi-constacyclic code where $\kappa = \max_t(k_t)$ and $\kappa' = \min_t(k_t)$.

Let $M_{\theta,s} = R[x,\theta]/\langle x^s-\lambda\rangle$ where λ is a unit element of R. Let θ be an automorphism of R with $|\langle\theta\rangle| = m = 2$.

Definition 63: A subset C of R^n is a called a skew quasi-constacyclic code of length $n=ls, m|s$, with index l if
$i)$ C is a submodule of R^n,
$ii)$ if $e=(e_{0,0},...,e_{0,l-1},e_{1,0},...,e_{1,l-1},...,e_{s-1,0},...,e_{s-1,l-1}) \in C$ then
$\nabla_{\theta,\lambda,l}(e) = (\theta(\lambda e_{s-1,0}),...,\theta(\lambda e_{s-1,l-1}),\theta(e_{0,0}),...,\theta(e_{0,l-1}),\theta(e_{1,0}),...,\theta(e_{1,l-1}),...,\theta(e_{s-2,0}),...,\theta(e_{s-2,l-1})) \in C$.

When $\lambda=1$ the skew quasi-constacyclic codes are just skew quasi-cyclic codes.

The ring $M_{\theta,s}^l$ is a left $M_{\theta,s}$ module where we define multiplication from left by $f(x)(g_1(x),...,g_l(x)) = (f(x)g_1(x),...f(x)g_l(x))$.

Define a map $\Lambda : R^n \to M_{\theta,s}^l$ by $\Lambda(e) = (e_0(x), e_1(x), ..., e_{l-1}(x))$ where $e_j(x) = \sum_{i=o}^{s-1} e_{ij}x^i \in M_{\theta,s}$, $j=0,1,...,l-1$.

Lemma 64: Let $\Lambda(C)$ denote the image of C under Λ. The map Λ induces a one to one correspondence between skew quasi-constacyclic codes over R of length n with index l and linear codes over $M_{\theta,s}$ of length l.

Theorem 65: A subset C of R^n is a skew quasi-constacyclic code of length $n=ls$ with index l iff is a left submodule of the ring $M_{\theta,s}^l$.

Proof: Let C be a skew quasi-constacyclic code of index l over R.Suppose that $\Lambda(C)$ forms a submodule of $M_{\theta,s}^l$. $\Lambda(C)$ is closed under addition and scalar multiplication. Let $\Lambda(e) = (e_0(x), e_1(x), ..., e_{l-1}(x)) \in \Lambda(C)$ for $e = (e_{0,0},...,e_{0,l-1},e_{1,0},...,e_{1,l-1},...,e_{s-1,0},...,e_{s-1,l-1}) \in C$. Then $x\Lambda(e) \in \Lambda(C)$. By linearity it follows that $r(x)\Lambda(e) \in \Lambda(C)$ for any $r(x) \in M_{\theta,s}$. Therefore, $\Lambda(C)$ is a left module of $M_{\theta,s}^l$.

Conversely, suppose E is an $M_{\theta,s}$ left submodule of $M_{\theta,s}^l$. Let $C = \Lambda^{-1}(E) = \{e \in R^n : \Lambda(e) \in E\}$. We claim that C is a skew quasi-constacyclic code of R. Since Λ is a isomorphism, C is a linear code of length n over R. Let $e=(e_{0,0},...,e_{0,l-1},e_{1,0},...,e_{1,l-1},...,e_{s-1,0},...,e_{s-1,l-1}) \in C$. Then $\Lambda(e) = (e_0(x), e_1(x), ..., e_{l-1}(x)) \in \Lambda(C)$, where $e_j(x) = \sum_{i=o}^{s-1} e_{ij}x^i \in M_{\theta,s}$ for $j=0,1,...,l-1$. It is easy to see that $\Lambda(\nabla_{\theta,\lambda,l}(e)) = x(e_0(x), e_1(x), ..., e_{l-1}(x)) = (xe_0(x), xe_1(x), ..., xe_{l-1}(x)) \in E$. Hence $\nabla_{\theta,\lambda,l}(e) \in C$. So, C is a skew quasi-constacyclic code C. ■

On $R^{n=sl}$ the usual Euclidean inner product for

$$e=(e_{0,0},...,e_{0,l-1},e_{1,0},...,e_{1,l-1},...,e_{s-1,0},...,e_{s-1,l-1})$$

and

$$c=(c_{0,0},...,c_{0,l-1},c_{1,0},...,c_{1,l-1},...,c_{s-1,0},...,c_{s-1,l-1})$$

we define $e.c = \sum_{i=0}^{s-1}\sum_{j=0}^{l-1} e_{ij}c_{ij}$. We define a conjugation map Ω on $M_{\theta,s}^l$ such that $\Omega(cx^i) = \theta^{-1}(c)x^{s-1}, 0 \leq i \leq s-1$, and extended linearly. We define the Hermitian inner product for $a = (a_0(x), a_1(x), ..., a_{l-1}(x))$ and $b = (b_0(x), b_1(x), ..., b_{l-1}(x))$,

$$\langle a, b\rangle = \sum_{j=0}^{l-1} a_j(x)\Omega\left(b_j(x)\right).$$

Theorem 66: Let $e, c \in R^n$. Then $\left(\nabla^k_{\theta,\lambda,l}(e)\right).c = 0$ for all $k = 0, ..., s-1$ iff $\langle \Lambda(e), \Lambda(c)\rangle = 0$.

Proof: Since $\theta^s = 1, \langle e, c\rangle = 0$ is equivalent to

$$\begin{aligned} 0 &= \sum_{j=0}^{l-1} e_j(x)\Omega\left(c_j(x)\right) = \sum_{j=0}^{l-1}\left(\sum_{i=0}^{s-1} e_{ij}x^i\right)\Omega\left(\sum_{k=0}^{s-1} c_{kj}x^k\right) \\ &= \sum_{j=0}^{l-1}\left(\sum_{i=0}^{s-1} e_{ij}x^i\right)\left(\sum_{k=0}^{s-1}\theta^{-1}(c_{kj})x^{s-k}\right) \\ &= \sum_{j=0}^{l-1}\left(\sum_{j=0}^{l-1}\sum_{i=0}^{s-1} e_{i+h,j}\theta^h(c_{ij})\right)x^h \end{aligned}$$

where the subscript $i+h$ is taken modulo s. Equating the coefficients of x^h on both sides, we have $\sum_{j=0}^{l-1}\sum_{i=0}^{s-1} w_{i+h,j}\theta^h(c_{ij}) = 0$, for all $0 \le h \le s-1$. $\sum_{j=0}^{l-1}\sum_{i=0}^{s-1} e_{i+h,j}\theta^h(c_{ij}) = 0$ is equivalent to $\theta^h(\nabla^{s-h}_{\theta,\lambda,l}(e).c) = 0$ which is further equivalent to $\nabla^{s-h}_{\theta,\lambda,l}(e,c) = 0$, for all $0 \le h \le s-1$. Since $0 \le h \le s-1$, condition is equivalent to $\left(\nabla^k_{\theta,\lambda,l}(e)\right).c = 0$ for all $k = 0, ..., s-1$. ■

Corollary 67: Let C be a skew quasi-constacyclic code of length $n = sl$ with index l over R. Then $C^\perp = \left\{a(x) \in M^l_{\theta,s} \ : \ \langle a(x), b(x)\rangle = 0, \ \forall\ b(x) \in C\right\}$.

Corollary 68: Let C be a skew quasi-constacyclic code of length sl with index l over R and $\Lambda(C)$ be its image in $M^l_{\theta,s}$ under Λ. Then $\Lambda(C)^\perp = \Lambda\left(C^\perp\right)$, where the dual in R^{sl} is taken with respect to the Euclidean inner product, while the dual in $M^l_{\theta,s}$ is taken with respect to the Hermitian inner product. The dual of a skew quasi-constacyclic code of length sl with index l over R is a skew quasi-constacyclic code of length sl with index l over R.

Proposition 69: Let $\nabla_{\theta,\lambda,l}$ be skew quasi-constacyclic shift on R^n, let ϕ be the Gray map from R^n to Z_3^{3n}. Then $\phi\nabla_{\lambda,l} = \rho\phi\nabla_{\theta,\lambda,l}$, where $\rho(x, y, z) = (x, z, y)$ for every $x, y, z \in Z_3^n$.

Proof: The proof is similar to the proof of Proposition 50. ■

Theorem 70: The Gray image a skew quasi-constacyclic code over R of length n is permutation equivalent to the Gray image of a quasi-constacyclic code over Z_3 with length $3n$.

Proof: The proof is similar to the proof of Theorem 51. ■

IX. 1-generator Skew Quasi-constacyclic Codes over R

A 1-generator skew quasi-constacyclic code over R is a left $M_{\theta,s}$-submodule of $M^l_{\theta,s}$ generated by $\mathbf{f(x)} = (f_1(x), f_2(x), ..., f_l(x)) \in M^l_{\theta,s}$ has the form $C = \{g(x)\left(f_1(x), f_2(x), ..., f_l(x)\right) : \ g(x) \in M_{\theta,s}\}$. Define the following map

$$\Pi_i : M^l_{\theta,s} \longrightarrow M_{\theta,s}$$

defined by $(e_1(x), e_2(x), ..., e_l(x)) \longmapsto e_i(x)$, $1 \le i \le l$. Let $\Pi_i(C) = C_i$. Since C is a left $M_{\theta,s}$-submodule of $M^l_{\theta,s}$, C_i is a left $M_{\theta,s}$-submodule of $M_{\theta,s}$,that is a left ideal of $M_{\theta,s}$. C_i is generated by $f_i(x)$. Hence C_i is a principal skew constacyclic code of length n over R. $f_i(x)$ is a monic right divisor of $x^s - \lambda$ that is $x^s - \lambda = h_i(x)f_i(x)$, $1 \le i \le l$.

A generator of C has the form

$$\mathbf{f(x)} = (g_1(x)f_1(x), g_2(x)f_2(x), ..., g_l(x)f_l(x))$$

where $g_i(x) \in R[x, \theta]$ such that $g_i(x)$ and $h_i(x)$ are right coprime for all $1 \le i \le l$.

Definition 71: Let $C = (g_1(x)f_1(x), g_2(x)f_2(x), ..., g_l(x) f_l(x))$ be a skew quasi-constacyclic code of length $n = sl$ with index l. Then unique monic polynomial

$$f(x) = gcld(\mathbf{f(x)}, x^s - \lambda) = gcld(f_1(x), f_2(x), ..., f_l(x), x^s - \lambda)$$

is called the generator polynomial of C.

Theorem 72: Let C be a 1-generator skew quasi-constacyclic code of length $n = sl$ with index l over R generated by $\mathbf{f(x)} = (f_1(x), f_2(x), ..., f_l(x))$ where $f_i(x)$ is a monic divisor of $x^s - \lambda$. Then C is a R-free code with rank $s - deg(f(x))$ where $f(x) = gcld(\mathbf{f(x)}, x^s - \lambda)$. Moreover, the set $\{\mathbf{f(x)}, x\mathbf{f(x)}, ..., x^{n-\deg(f(x))-1}\mathbf{f(x)}\}$ forms an R-basis of C.

Proof: Since $gcld(f_i(x), x^s - \lambda) = m_i(x)$, it follows that $f(x) = gcld(m_1(x), m_2(x), ..., m_l(x))$ where $\Pi_i(C) = (f_i(x)) = (m_i(x))$ with $m_i(x)|(x^s - \lambda)$ for all $1 \le i \le l$. Let $c(x) = \sum_{i=0}^{n-k-1} c_i x^i$ and $c(x)\mathbf{f(x)} = 0$. Then $(x^s - \lambda)|c(x)f_i(x)$ for all $1 \le i \le l$. Hence $(x^s - \lambda)|c(x)f_i(x)c_i(x)$ with $gcld(c_i(x), \frac{x^s-\lambda}{f_i(x)}) = 1$. That is $\frac{x^s-\lambda}{f_i(x)}|c(x)$ which implies that $\frac{x^s-\lambda}{f(x)}|c(x)$. Since $\deg(\frac{x^s-\lambda}{f(x)}) = s - k > \deg(c(x)) = n - k - 1$, it is follows that $c(x) = 0$. Thus, $\mathbf{f(x)}, x\mathbf{f(x)}, ..., x^{n-\deg(f(x))-1}\mathbf{f(x)}$ are R-linear independent. Further, $\mathbf{f(x)}, x\mathbf{f(x)}, ..., x^{n-\deg(f(x))-1}\mathbf{f(x)}$ generate C. So, $\left\{\mathbf{f(x)}, x\mathbf{f(x)}, ..., x^{n-\deg(f(x))-1}\mathbf{f(x)}\right\}$ forms an R-basis of C. ■

Conclusion

In this paper, we have introduced skew cyclic, skew quasi-cyclic, skew constacyclic and skew quasi-constacyclic codes over the finite ring R. By using the Gray map, we have studied the Gray images of cyclic, quasi-cyclic, constacyclic and their skew codes over R. We have obtained a representation of a linear code of length n over R using C_1, C_2 and C_3 which are linear codes of length n over Z_3. We have obtained the parameters of quantum error-correcting codes from both cyclic and negacyclic codes over R. We have determined a sufficient condition for 1-generator skew quasi-constacyclic codes to be free.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their valuable remarks and suggestions. We would like to thank S.T. Dougherty for helping to express a linear code C of length n over R by means of three ternary codes and we would like to thank Sedat Akleylek for helping to find minimum distances by using computer program.

REFERENCES

[1] T. Abualrub, A. Ghrayeb, N. Aydın, I. Siap, *On the construction of skew quasi-cyclic codes*, IEEE Transsactions on Information Theory, **56** 2081-2090, (2010).

[2] T. Abualrub, N. Aydın, P. Seneviratne, *On θ-cyclic codes over F_2+vF_2*, Australasian Journal of Combinatorics, **54** 115-126, (2012).

[3] M. Ashraf, G. Mohammad, *Quantum codes from cyclic codes over F_3+vF_3*, International Journal of Quantum Information, **6** 1450042, (2014).

[4] A. Bayram, I. Siap, *Structure of codes over the ring $Z_3[v]/<v^3-v>$*, AAECC, DOI 10.1007/s00200-013-0208-x, (2013).

[5] M. Bhaintwal, *Skew quasi-cyclic codes over Galois rings*, Des. Codes Cryptogr., DOI 10.1007/s10623-011-9494-0.

[6] M. Bhaintwal, S. K. Wasan, *On quasi-cyclic codes over Z_q* AAECC, **20** 459-480, (2009).

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

[8] D. Boucher, P. Sole, F. Ulmer, *Skew constacyclic codes over Galois rings*, Advance of Mathematics of Communications, **2** 273-292, (2008).

[9] D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, Journal of Symbolic Computation, **44** 1644-1656, (2009).

[10] A. R. Calderbank, E.M.Rains, P.M.Shor, N.J.A.Sloane, *Quantum error correction via codes over $GF(4)$* ,IEEE Trans. Inf. Theory,**44** 1369-1387, (1998).

[11] Y. Cengellenmis, A. Dertli, S.T. Dougherty, *Codes over an infinite family of rings with a Gray map*, Designs, Codes and Cryptography, **72** 559-580, (2014).

[12] A. Dertli, Y. Cengellenmis, S. Ere, *On quantum codes obtained from cyclic codes over A_2* , Int. J. Quantum Inform., **13** 1550031, (2015).

[13] A. Dertli, Y. Cengellenmis, S. Eren, *Quantum codes over the ring $F_2+uF_2+u^2F_2+...+u^mF_2$*, nt. Journal of Alg., **3** 115-121, (2015).

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

[15] J. Gao, L. Shen, F. W. Fu, *Skew generalized quasi-cyclic codes over finite fields*, arXiv: 1309.1621v1.

[16] M. Grassl, T. Beth, *On optimal quantum codes*, International Journal of Quantum Information, **2** 55-64,(2004).

[17] A. R. Hammons, V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Sole, *The Z_4-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inf. Theory, **40** 301-319,(1994).

[18] S. Jitman, S. Ling, P. Udomkovanich, *Skew constacyclic codes over finite chain rings*, AIMS Journal.

[19] X.Kai, S.Zhu, *Quaternary construction bof quantum codes from cyclic codes over F_4+uF_4*, Int. J. Quantum Inform., **9** 689-700, (2011).

[20] S. Ling, P. Sole, *On the algebraic structures of quasi-cyclic codes I: finite fields*, IEEE Trans. Inf. Theory, **47** 2751-2760, (2001).

[21] S. Ling, P. Sole, *On the algebraic structures of quasi-cyclic codes II: chain rings*, Des.Codes Cryptogr., **30** 113130, (2003).

[22] S. Ling, P. Sole, *On the algebraic structures of quasi-cyclic codes III: generator theory*, IEEE Trans. Inf. Theory, **51** 2692-2000, (2005).

[23] Maheshanand, S. K. Wasan, *On Quasi-cyclic Codes over Integer Residue Rings*, AAECC, Lecture Notes in Computer Science, **4851** 330-336, (2007).

[24] J.Qian, *Quantum codes from cyclic codes over F_2+vF_2*, Journal of Inform.& computational Science **6** 1715-1722, (2013).

[25] J.Qian, W.Ma, W.Gou, *Quantum codes from cyclic codes over finite ring*, Int. J. Quantum Inform., **7** 1277-1283, (2009).

[26] J. F. Qian, L. N. Zhang, S. X. Zhu, *$(1+u)$-constacyclic and cyclic codes over F_2+uF_2*, Applied Mathematics Letters, **19** 820-823, (2006).

[27] I. Siap, T. Abualrub, N. Aydın, P. Seneviratne, *Skew cyclic codes of arbitrary length*, Int. Journal of Information and Coding Theory, (2010).

[28] P.W.Shor, *Scheme for reducing decoherence in quantum memory*, Phys. Rev. A., **52** 2493-2496, (1995).

[29] A. M. Steane, *Simple quantum error correcting codes* , Phys. Rev. A., **54** 4741-4751, (1996).

[30] M. Wu, *Skew cyclic and quasi-cyclic codes of arbitrary length over Galois rings*, International Journal of Algebra, **7** 803-807,(2013).

[31] X.Yin, W.Ma, *Gray Map And Quantum Codes Over The Ring $F_2+uF_2+u^2F_2$*, International Joint Conferences of IEEE TrustCom-11, (2011).

[32] S. Zhu, L. Wang, *A class of constacyclic codes over F_p+vF_p and their Gray images*, Discrete Math. **311** 2677-2682, (2011).