Palestine Journal of Mathematics

Vol. 4 (Spec. 1) (2015) , 540–546

On Skew Cyclic and Quasi-cyclic Codes Over $F_2 + uF_2 + u^2F_2$

Abdullah Dertli, Yasemin Cengellenmis and Senol Eren

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 94B05; Secondary 94B15.

Keywords and phrases: Cyclic codes,quasi-cyclic codes, skew cyclclic codes, skew quasi-cyclic codes, Finite rings.

Abstract We construct a new Gray map from S^n to F_2^{3n} where $S = F_2+uF_2+u^2F_2$, $u^3 = 1$. It is both an isometry and a weight preserving map. It was shown that the Gray image of cyclic code over S is quasi-cyclic codes of index 3 and the Gray image of quasi-cyclic code over S is l-quasi-cyclic code of index 3. Moreover, the skew cyclic and skew quasi-cyclic codes over S introduced and the Gray images of them are determined.

1 Introduction

By using generator polynomials in skew polynomial rings, there are a lot of works about generalizing notions of cyclic, constacyclic, quasi-cyclic codes to skew cyclic, skew constacyclic, skew quasi-cyclic codes respectively.

Skew polynomial rings form an important family of non-commutative rings. There are many applications in the construction of algebraic codes. As polynomials in skew polynomial ring exhibit many factorizations, there are many more ideals in a skew polynomial ring than in the commutative case. So the research on codes have result in the discovery of many new codes with better Hamming distance.

Works began with D. Boucher, W. Gieselmann, F. Ulmer's paper in [1]. They generalized the notion of cyclic codes. They gave many examples of codes which improve the previously best known linear codes.

In [3], D. Boucher and F. Ulmer studied linear codes over finite fields obtained from left ideals in a quotient ring of a (non-commutative) skew polynomial ring. They show how existence and properties of such codes are linked to arithmetic properties of skew polynomials. This class of codes is generalization of the $\theta-$cyclic codes discussed in [1]. Moreover, they shown that the dual of a $\theta-$cyclic code is still $\theta-$cyclic.

D. Boucher, P. Sole and F. Ulmer generalized the construction of linear codes via skew polynomial rings by using Galois rings instead of finite fields as coefficients. Codes that are principal ideals in quotient rings of skew polynomial rings by a two side ideals were studied in [2]. In [4], they studied a special type of linear codes called skew cyclic codes in the most general case. They shown that these codes are equivalent to either cyclic or quasi-cyclic codes.

Skew polynomial rings over finite fields and over Galois rings had been used to study codes. In [9], they extended this concept to finite chain rings. The structure of all skew constacyclic codes is completely determined.

In [11], T. Abualrub, P. Seneviratre studied skew cyclic codes over $F_2 + vF_2$, $v^2 = v$.

In [10], T. Abualrub, A. Ghrayeb, N. Aydın, İ. Şiap introduced skew quasi-cyclic codes. They obtained several new codes with Hamming distance exceeding the distance of the previously best known linear codes with comparable parameters. In [7], M. Bhaintwal studied skew quasi-cyclic codes over Galois rings.

In [8], they investigated the structures of skew cyclic and skew quasi-cyclic of arbitrary length over Galois rings. They shown that the skew cyclic codes are equivalent to either cyclic and quasi-cyclic codes over Galois rings. Moreover, they gave a necessary and sufficient condition for skew cyclic codes over Galois rings to be free.

Jian Gao, L. Shen, F. W. Fu studied a class of generalized quasi–cyclic codes called skew generalized quasi-cyclic codes. They gave the Chinese Remainder Theorem over the skew polynomial ring which lead to a canonical decomposition of skew generalized quasi-cyclic codes. Moreover, they focused on 1-generator skew generalized quasi-cyclic code in [6].

J.F. Qian et. al. introduced linear $(1 + u)$-constacyclic codes and cyclic codes over $F_2 + uF_2$ and characterized codes over F_2 which are the Gray images of $(1 + u)$-constacyclic codes or cyclic codes over $F_2 + uF_2$ in [5]. It was introduced $(1 - u^m)$-constacyclic codes over $F_2 + uF_2 + ... + u^mF_2$ and characterized codes over F_2 in [12].

This paper is organized as follows. In section 2, we give some basic knowledges about the finite ring S, cyclic and quasi-cyclic code. In section 3, we define a new Gray map from S to F_2^3, Lee weights of elements of S and Lee distance in the linear codes over S. We show that if C is self orthogonal so is $\varphi(C)$ and we obtain in the Gray images of cyclic and quasi-cyclic codes over S. In section 4, we give skew cyclic and quasi-cyclic codes over S. In section 5, we obtain in the Gray images of skew cyclic and skew quasi-cyclic codes over S and we give some examples.

2 Preliminaries

We first start with a general overview of the ring S. The ring $S = F_2 + uF_2 + u^2F_2$ is defined as characteristic 2 ring subject to the restrictions $u^3 = 1$. S is a commutative ring with eight elements. Note that S is not a finite chain ring, its ideals can easily be described as follows

$$\begin{aligned} I_0 &= \{0\} \subseteq I_{1+u+u^2} \subseteq I_1 = S \\ I_0 &= \{0\} \subseteq I_{1+u} = I_{1+u^2} = I_{u+u^2} \subseteq I_1 = S \end{aligned}$$

where

$$\begin{aligned} I_{1+u} &= I_{1+u^2} = I_{u+u^2} = \{0, 1+u, 1+u^2, u+u^2\} \\ I_{1+u+u^2} &= \{0, 1+u+u^2\} \end{aligned}$$

We note that S is semilocal ring with two maximal ideals and principal ideal ring. The elements 1, u and u^2 are three units of S.

A linear code C over S of length n is a $S-$submodule of S^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 S, the dual code of C

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

which is also a linear code over S of length n. A code C is self orthogonal if $C \subseteq C^{\perp}$ and self dual if $C = C^{\perp}$. We note that the dual ideals of S as follows,

$$\begin{aligned} I_{1+u}^{\perp} &= I_{1+u^2}^{\perp} = I_{u+u^2}^{\perp} = I_{1+u+u^2} \\ I_{1+u+u^2}^{\perp} &= I_{1+u} = I_{1+u^2} = I_{u+u^2} \end{aligned}$$

A cyclic code C over S 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 S^n is a linear cyclic code of length n iff it is polynomial representation is an ideal of $S[x] / \langle x^n - 1 \rangle$.

Let C be code over F_2 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 $\acute{c}_i = 1$ and $w_H(\acute{c}_i) = 0$ if $\acute{c}_i = 0$. The 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 the Hamming distance between two codewords with $d_H(c, \acute{c}) = w_H(c - \acute{c})$.

Let $a \in F_2^{3n}$ with $a = (a_0, a_1, ..., a_{3n-1}) = \left(a^{(0)} \left| a^{(1)} \right| a^{(2)}\right)$, $a^{(i)} \in F_2^n$, for $i = 0, 1, 2$. Let $\sigma^{\otimes 3}$ be a map from F_2^{3n} to F_2^{3n} given by

$$\sigma^{\otimes 3}(a) = \left(\sigma\left(a^{(0)}\right) \left| \sigma\left(a^{(1)}\right) \right| \sigma\left(a^{(2)}\right)\right)$$

where σ is a cyclic shift from F_2^n to F_2^n given by

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

for every $a^{(i)} = \left(a^{(i,0)}, ..., a^{(i,n-1)}\right)$ where $a^{(i,j)} \in F_2$, $j = 0, 1, ..., n-1$. A code of length $3n$ over F_2 is said to be quasi cyclic code of index 3 if $\sigma^{\otimes 3}(C) = C$.

Let $n = sl$. A quasi-cyclic code C over S 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 $a \in F_2^{3n}$ with $a = (a_0, a_1, ..., a_{3n-1}) = \left(a^{(0)} \left| a^{(1)} \right| a^{(2)}\right)$, $a^{(i)} \in F_2^n$, for $i = 0, 1, 2$. Let Γ be a map from F_2^{3n} to F_2^{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 F_2^n to F_2^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 $a^{(i,j)} \in F_2^l$, $j = 0, 1, ..., s-1$ and $n = sl$. A code of length $3n$ over F_2 is said to be $l-$quasi cyclic code of index 3 if $\Gamma(C) = C$.

3 Gray Image of Cyclic and Quasi-cyclic Codes Over S

Let $x = a + ub + u^2c$ be an element of S where $a, b, c \in F_2$. We define Gray map φ from S to F_2^3 by

$$\begin{aligned} \varphi &: S \to F_2^3 \\ a + ub + u^2c &\mapsto \varphi\left(a + ub + u^2c\right) = (a + b + c, a + b, a + c) \end{aligned}$$

From definition, the Lee weight of elements of S are defined as follows

$$\begin{aligned} w_L(0) &= 0 & w_L(1+u) &= 1 \\ w_L(1) &= 3 & w_L\left(1+u^2\right) &= 1 \\ w_L(u) &= 2 & w_L\left(u+u^2\right) &= 2 \\ w_L\left(u^2\right) &= 2 & w_L\left(1+u+u^2\right) &= 1 \end{aligned}$$

Let C be a linear code over S 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 the 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 S^n to F_2^{3n}.

Theorem 3.1. *The Gray map φ is a weight preserving map from (S^n,Lee weight) to (F_2^{3n},Hamming weight). Moreover it is an isometry from (S^n,Lee distance) to (F_2^{3n},Hamming distance).*

Theorem 3.2. *If C is an (n, k, d_L) linear codes over S, then $\varphi(C)$ is a $(3n, k, d_H)$ linear codes over F_2 where $d_H = d_L$.*

Proof. Let $x = a_1 + ub_1 + u^2c_1$, $y = a_2 + ub_2 + u^2c_2 \in S, \alpha \in F_2$, then

$$\begin{aligned} \varphi(x+y) &= \varphi\left(a_1 + a_2 + u(b_1 + b_2) + u^2(c_1 + c_2)\right) \\ &= (a_1 + a_2 + b_1 + b_2 + c_1 + c_2, a_1 + a_2 + b_1 + b_2, a_1 + a_2 + c_1 + c_2) \\ &= (a_1 + b_1 + c_1, a_1 + b_1, a_1 + c_1) + (a_2 + b_2 + c_2, a_2 + b_2, a_2 + c_2) \\ &= \varphi(x) + \varphi(y) \\ \varphi(\alpha x) &= \varphi\left(\alpha a_1 + u\alpha b_1 + u^2\alpha c_1\right) \\ &= (\alpha(a_1 + b_1 + c_1), \alpha(a_1 + b_1), \alpha(a_1 + c_1)) \\ &= \alpha(a_1 + b_1 + c_1, a_1 + b_1, a_1 + c_1) \\ &= \alpha\varphi(x) \end{aligned}$$

So, φ is linear. As φ is bijective, then $|C| = |\varphi(C)|$. From theorem 3.1, we have $d_H = d_L$. □

Theorem 3.3. *If C is self orthogonal, so is $\varphi(C)$.*

Proof. Let $r = a_1 + ub_1 + u^2c_1$, $r_1 = a_2 + ub_2 + u^2c_2$ where $a_1, b_1, c_1, a_2, b_2, c_2 \in F_2$. $r.r_1 = a_1a_2 + b_1c_2 + c_1b_2 + u(a_1b_2 + b_1a_2 + c_1c_2) + u^2(a_1c_2 + b_1b_2 + c_1a_2)$, if C is self orthogonal, so we have $a_1a_2 + b_1c_2 + c_1b_2 = 0, a_1b_2 + b_1a_2 + c_1c_2 = 0, a_1c_2 + b_1b_2 + c_1a_2 = 0$. From

$$\begin{aligned}\varphi(r).\varphi(r_1) &= (a_1 + b_1 + c_1, a_1 + b_1, a_1 + c_1).(a_2 + b_2 + c_2, a_2 + b_2, a_2 + c_2)\\ &= 0\end{aligned}$$

Therefore, we have $\varphi(C)$ is self orthogonal. □

Proposition 3.4. *Let σ and $\sigma^{\otimes 3}$ be as in the preliminaries.Then $\varphi\sigma = \sigma^{\otimes 3}\varphi$.*

Proof. Let $r_i = a_i + ub_i + u^2c_i$ be the elements of S 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

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

On the other hand $\varphi(r_0, ..., r_{n-1}) = (a_0 + b_0 + c_0, ..., a_{n-1} + b_{n-1} + c_{n-1}, a_0 + b_0, ..., a_{n-1} + b_{n-1}, a_0 + c_0, ..., a_{n-1} + c_{n-1})$. If we apply $\sigma^{\otimes 3}$, we have

$\sigma^{\otimes 3}(\varphi(r_0, r_1, ..., r_{n-1})) = (a_{n-1} + b_{n-1} + c_{n-1}, ..., a_{n-2} + b_{n-2} + c_{n-2}, a_{n-1} + b_{n-1}, ..., a_{n-2} + b_{n-2}, a_{n-1} + c_{n-1}, ..., a_{n-2} + c_{n-2})$. Thus, $\varphi\sigma = \sigma^{\otimes 3}\varphi$. □

Theorem 3.5. *Let σ and $\sigma^{\otimes 3}$ be as in the preliminaries. A code C of length n over S is cyclic code if and only if $\varphi(C)$ is quasi cyclic code of index 3 and length $3n$ over F_2.*

Proof. Suppose C is cyclic code. Then $\sigma(C) = C$. If we apply φ, we have $\varphi(\sigma(C)) = \varphi(C)$. From proposition 3.4, $\varphi(\sigma(C)) = \sigma^{\otimes 3}(\varphi(C)) = \varphi(C)$. Hence, $\varphi(C)$ is a quasi- cyclic code of index 3. Conversely, if $\varphi(C)$ is a quasi-cyclic code of index 3, then $\sigma^{\otimes 3}(\varphi(C)) = \varphi(C)$. From proposition 3.4, we have $\sigma^{\otimes 3}(\varphi(C)) = \varphi(\sigma(C)) = \varphi(C)$. Since φ is injective, it follows that $\sigma(C) = C$. □

Proposition 3.6. *Let $\tau_{s,l}$ be quasi-cyclic shift on S. Let Γ be as in the preliminaries. Then $\varphi\tau_{s,l} = \Gamma\varphi$.*

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 $e_{i,j} = a_{i,j} + ub_{i,j} + u^2c_{i,j}$ 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

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

On the other hand,

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

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

Theorem 3.7. *The Gray image of a quasi-cyclic code over S of length n with index l is a l-quasi cyclic code of index 3 over F_2 with length $3n$.*

Proof. Let C be a quasi-cyclic code over S of length n with index l. That is $\tau_{s,l}(C) = C$. If we apply φ, we have $\varphi(\tau_{s,l}(C)) = \varphi(C)$. From the Proposition 3.6, $\varphi(\tau_{s,l}(C)) = \varphi(C) = \Gamma(\varphi(C))$. So, $\varphi(C)$ is a l quasi-cyclic code of index 3 over F_2 with length $3n$. □

4 Skew Cyclic and Quasi-cyclic Codes Over S

We are interested in studying skew codes using the ring $S = F_2 + uF_2 + u^2F_2$ where $u^3 = 1$. We define non-trivial ring automorphism

$$\theta : S \longrightarrow S$$

$$\begin{aligned} 0 &\longrightarrow 0 \\ 1 &\longrightarrow 1 \\ u &\longrightarrow u^2 \\ u^2 &\longrightarrow u \end{aligned}$$

The ring $S[x, \theta] = \{a_0 + a_1x + ... + a_{n-1}x^{n-1} : a_i \in S, n \in N\}$ is called a skew polynomial ring. This ring is a non-commutative ring. The addition in the ring $S[x, \theta]$ 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 $a \in S$. This implies that θ is a ring automorphism of order 2.

Definition 4.1. A subset C of S^n is callled a skew cyclic code of length n if C satisfies the following conditions,
$i)$ C is a submodule of S^n,
$ii)$ If $c = (c_0, c_1, ..., c_{n-1}) \in C$, then $\sigma_\theta(c) = (\theta(c_{n-1}), \theta(c_0), ..., \theta(c_{n-2})) \in C$

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

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

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

Theorem 4.2. *S_n is a left $S[x, \theta]$-module where multiplication defined as in above.*

Theorem 4.3. *A code C in S_n is a skew cyclic code if and only if C is a left $S[x, \theta]$-submodule of the left $S[x, \theta]$-module S_n.*

Theorem 4.4. *Let C be a skew cyclic code in S_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 $(x^n - 1)$.*

Definition 4.5. A subset C of S^n is called a skew quasi-cyclic code of length n if C satisfies the following conditions,
$i)$ C is a submodule of S^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 $S[x, \theta]$ if $m|s$ where $m = 2$ is the order of θ. So $S[x, \theta]/(x^s - 1)$ is well defined.

The ring $R_s^l = (S[x, \theta]/(x^s - 1))^l$ is a left $R_s = S[x, \theta]/(x^s - 1)$ 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

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

$(e_{0,0}, ..., e_{0,l-1}, e_{1,0}, ..., e_{1,l-1}, ..., e_{s-1,0}, ..., e_{s-1,l-1}) \mapsto (c_0(x), ..., c_{l-1}(x))$ 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 S^n and the ring R_s^l.

Theorem 4.6. *A subset C of S^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.*

5 Gray Images of Skew Cyclic and Quasi-cyclic Codes Over S

Proposition 5.1. *Let σ_θ be the skew cyclic shift on S^n, let φ be the Gray map from S^n to F_2^{3n} and let $\sigma^{\otimes 3}$ be as in the preliminaries. Then $\varphi\sigma_\theta = \lambda\sigma^{\otimes 3}\varphi$ where $\lambda(x, y, z) = (x, z, y)$ for every $x, y, z \in F_2^n$.*

Proof. Let $r_i = a_i + ub_i + u^2c_i$ be the elements of S, 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

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

On the other hand, $\varphi(r_0, ..., r_{n-1}) = (a_0 + b_0 + c_0, ..., a_{n-1} + b_{n-1} + c_{n-1}, a_0 + b_0, ..., a_{n-1} + b_{n-1}, a_0 + c_0, ..., a_{n-1} + c_{n-1})$. If we apply $\sigma^{\otimes 3}$, we have

$\sigma^{\otimes 3}(\varphi(r_0, r_1, ..., r_{n-1})) = (a_{n-1}+b_{n-1}+c_{n-1}, ..., a_{n-2}+b_{n-2}+c_{n-2}, a_{n-1}+b_{n-1}, ..., a_{n-2}+b_{n-2}, a_{n-1} + c_{n-1}, ..., a_{n-2} + c_{n-2})$. If we apply λ, we have $\lambda(\sigma^{\otimes 3}(\varphi(r_0, r_1, ..., r_{n-1}))) = (a_{n-1}+b_{n-1}+c_{n-1}, ..., a_{n-2}+b_{n-2}+c_{n-2}, a_{n-1}+c_{n-1}, ..., a_{n-2}+c_{n-2}, a_{n-1}+b_{n-1}, ..., a_{n-2}+b_{n-2})$. So, we have $\varphi\sigma_\theta = \lambda\sigma^{\otimes 3}\varphi$. □

Theorem 5.2. *The Gray image a skew cyclic code over S of length n is permutation equivalent to quasi-cyclic code of index 3 over F_2 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 $\varphi(\sigma_\theta(C)) = \varphi(C)$. From the Proposition 5.1, $\varphi(\sigma_\theta(C)) = \varphi(C) = \lambda(\sigma^{\otimes 3}(\varphi(C)))$. So, $\varphi(C)$ is permutation equivalent to quasi-cyclic code of index 3 over F_2 with length $3n$. □

Proposition 5.3. *Let $\tau_{\theta,s,l}$ be skew quasi-cyclic shift on S^n, let φ be the Gray map from S^n to F_2^{3n}, let Γ be as in the preliminaries, let λ be as above. Then $\varphi\tau_{\theta,s,l} = \lambda\Gamma\varphi$.*

Proof. The proof is similar to the proof of Proposition 5.1. □

Theorem 5.4. *The Gray image a skew quasi-cyclic code over S of length n with index l is permutation equivalent to l quasi-cyclic code of index 3 over F_2 with length $3n$.*

Proof. The proof is similar to the proof of Theorem 5.2. □

Example 5.5. Let $S = F_2 + uF_2 + u^2F_2$, $n = 4$.

$$\begin{aligned}x^4 - 1 &= (x+1)(x+1)(x+1)(x+1) \\ &= (x+u)\left(x+u^2\right)(x+u)\left(x+u^2\right) \\ &= (x+u)\left(x+u^2\right)(x+1)(x+1) \\ &= (x+1)\left(x+u^2\right)(x+u)(x+1)\end{aligned}$$

Let $f(x) = x + u$. Then $f(x)$ generates a skew cyclic code of length 4 with the minimum distance $d = 2$. This code is equivalent to a quasi-cyclic code of index 3 over F_2 with length 12.

Example 5.6. Let $S = F_2 + uF_2 + u^2F_2$, $n = 6$, $x^6 - 1 = (x^3 + u)(x^3 + u^2)$. Let $f(x) = x^3 + u^2$. Then $f(x)$ generates a skew cyclic code of length 6 with the minimum distance $d = 2$. This code is equivalent to a quasi-cyclic code of index 3 over F_2 with length 18.

6 Conclusion

We introduced skew cyclic and skew quasi-cyclic codes over the finite ring S. We construct a new Gray map. It is shown that if C is self orthogonal so is $\varphi(C)$. Moreover, by using this Gray map, the Gray images of cyclic, quasi-cyclic,skew cyclic and skew quasi-cyclic codes over S are obtained. So, it can be obtained the new codes with better Hamming distance.

References

[1] D. Boucher, W. Geiselmann, F. Ulmer, Skew cyclic codes, *Appl. Algebra. Eng.Commun Comput.* **4**, (2007).

[2] D. Boucher, F. Ulmer, Skew constacyclic codes over Galois rings, *Advance of Mathematics of Communications* **3**, 273–292 (2008).

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

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

[5] 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).

[6] J. Gao, L. Shen, F. W. Fu, Skew generalized quasi-cyclic codes over finite fields, *arXiv:* $1309{,}1621v1$.

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

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

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

[10] 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).

[11] T. Abualrub, P. Seneviratne, Skew codes over ring, *Proceeding of the interntional Multi Conference of Engineers and Computer Scientist, IMECS*, (2010).

[12] Y. Cengellenmis, On $(1-u^m)$-cyclic codes over $F_2+uF_2+...+u^mF_2$, *Int J. Contemp. Math. Sciences*, **4**, 987–992 (2009).

Author information

Abdullah Dertli, Department of Mathematics, Ondokuz Mayıs University, Faculty of Arts and Sciences, Samsun, TURKEY.
E-mail: abdullah.dertli@gmail.com

Yasemin Cengellenmis, Department of Mathematics, Trakya University, Faculty of Arts and Sciences, Edirne, TURKEY.
E-mail: ycengellenmis@gmail.com

Senol Eren, Department of Mathematics, Ondokuz Mayıs University, Faculty of Arts and Sciences, Samsun, TURKEY.
E-mail: seren@omu.edu.tr

Received: March 9, 2015.

Accepted: May 7, 2015.