On the Gray images of some linear codes and quantum codes

Abdullah Dertli and Yasemin Cengellenmis

Communicated by Ayman Badawi

MSC 2010 Classifications: 94B05; 94B15.

Keywords and phrases: Quantum codes, cyclic codes, quasi-cyclic codes, constacyclic codes, skew codes, finite rings.

Abstract In this paper, we study the structures of cyclic, quasi-cyclic, constacyclic codes and their skew codes over the finite ring $S_p = F_p + uF_p + vF_p$, $u^2 = u, v^2 = v, uv = vu = 0$. The Gray images of cyclic, quasi-cyclic, skew cyclic, skew quasi-cyclic and skew constacyclic codes over $S_p$ are obtained. A necessary and sufficient condition for cyclic (negacyclic) codes over $S_p$ that contains its dual has been given. The parameters of quantum error correcting codes are obtained from both cyclic and negacyclic codes over $S_p$. The MacWilliams identities are obtained.

1 Introduction

Most of researchers concentrate on linear codes, since they have clear structure. Although a lot of researches on error correcting codes are about codes over finite fields, a lot of works on codes over finite rings were done after the discovery that certain good non-linear binary codes can be constructed from cyclic codes over $Z_4$ via the Gray map in [7].

The algebraic structures of certain type of codes over many finite rings were determined such as cyclic, negacyclic, quasi-cyclic and constacyclic codes that were defined in a commutative ring in [11,17,20,23,24,25,26,30].

D. Boucher, W. Gieselman and F. Ulmer in [8] took another direction, when they studied more generalized class of linear and cyclic using a non commutative ring. They studied what they called skew cyclic codes in [9,10]. Later, some researchers generalized the notion of quasi-cyclic and constacyclic codes over finite fields and finite ring as similarly in [2,12,16,19,22,27].

Quantum error correcting codes are used in quantum computing to protect quantum information. Although the theory of quantum error correcting codes has striking differences from the theory of classical error correcting codes, Calderbank et al. gave a way to construct quantum error correcting codes from classical error correcting codes in [6]. 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 [1,3,4,5,13,14,15,18,21,28,29].

In this paper, it is given some definitions. By giving the duality of codes via inner product, it is shown that $C$ is self orthogonal codes over $S_p$, so is $\phi (C)$, where $\phi$ is a Gray map in section 2. In section 3, a linear code over $S_p$ is represented by means of three $p$-ary codes and it is generator matrix is given. It is shown that $C$ is self dual if and only if all three $p$-ary codes are self dual codes. In section 4, the Gray images of cyclic and quasi-cyclic codes over $S_p$ are obtained. It is shown that $C$ is cyclic (negacyclic) code over $S_p$ if and only if all three $p$-ary codes are cyclic (negacyclic) codes. In section 5, after a cyclic (negacyclic) codes over $S_p$ is represented via cyclic (negacyclic) codes over $F_p$, it is determined the dual of cyclic (negacyclic) codes.

A necessary and sufficient condition for cyclic (negacyclic) code over $S_p$ that contains its dual is given. The parameters of quantum error correcting codes are obtained from both cyclic and negacyclic codes over $S_p$. In section 6, it is given details about constacyclic codes over $S_p$. It is expressed a linear code over $S_p$ by means of two linear codes of length $n$ over $F_p + uF_p$ in section 7. It is found the nontrivial automorphism $\theta_p$ on the ring $S_p$. By using this automorphism, the skew cyclic, skew quasi-cyclic and skew constacyclic codes over $S_p$ are introduced. The number of distinct skew cyclic codes over $S_p$ is given. The Gray images of the skew codes are obtained in section 8. In section 9, the MacWilliams identities are obtained.
2 Linear codes over $S_p$

Let $S_p = F_p + uF_p + vF_p$, where $u^2 = u, v^2 = v, uv = vu = 0$ and $p$ is a prime. $S_p$ is a finite commutative ring with identity and characteristic is $p$. It contains $p^3$ elements. Any element $a$ of $S_p$ can be expressed uniquely as $a = r + us + vt$ with $r, s, t \in F_p$. The ring has the following properties:

* There are 8 different ideals of $S_p$ and they are $(1), (u), (v), (1-u-v), (1-u), (1-v), (u+v)$ and $(0)$. $(1)$ is an ideal whose the number of the elements is $p^2$, $(u), (v)$ and $(1-u-v)$ are ideals whose the number of the elements are $p$, $(1-u), (1-v), (u+v)$ are ideals whose the number of the elements are $p^2$, $(0)$ is an ideal whose the number of the element is 1.

* $S_p$ is principal ideal ring and it has three maximal ideals $(1-u), (1-v), (u+v)$. The quotient rings $S_p/(1-u), S_p/(1-v)$ and $S_p/(u+v)$ are isomorphic to $F_p$.

* For any element $a = r + su + tv$ of $S_p$, $a$ is a unit if and only if $r \neq 0$, $r + s \neq 0$ (mod $p$) and $r + t \neq 0$ (mod $p$).

Moreover, $|S_p^n| = (p-1)^3$ where $S_p^n$ is the group of units. For every element of $a$ of $S_p$, we define the Gray map as

$$\phi : S_p \rightarrow F_p^3$$

$$\phi(r + us + vt) = (r, r + s, r + t)$$

It is easy to see that $\phi$ is a ring isomorphism. The mapping $\phi$ can be extended to

$$\phi : S_p^n \rightarrow F_p^{3n}$$

$$\phi(r + us + vt) = (r, r + s, r + t)$$

componentwise in a natural way as $\phi(a) = (r, r + s, r + t)$ where $a = (a_1, \ldots, a_n) \in S_p^n$ and $r = (r_1, \ldots, r_n), s = (s_1, \ldots, s_n)$ and $t = (t_1, \ldots, t_n) \in F_p^n$ with $a_i = r_i + us_i + vt_i$, for $i = 1, \ldots, n$. The Gray weight of $a$ is defined as follows

$$w_G(a) = w_H(r, r + s, r + t)$$

where $w_H(b)$ denotes the Hamming weight of $b$ over $F_p$. Define the Gray weight of a vector $a = (a_1, \ldots, a_n) \in S_p^n$ as

$$w_G(a) = \sum_{i=1}^{n} w_G(a_i)$$

For any elements $b_1, b_2 \in S_p^n$, the Gray distance is given by $d_G(b_1, b_2) = w_G(b_1 - b_2)$.

A code $C$ of length $n$ over $S_p$ is a subset of $S_p^n$. $C$ is linear iff $C$ is an $S_p$-submodule of $S_p^n$.

The minimum Gray distance of $C$ is the smallest nonzero Gray distance between all pairs of distinct codewords. The minimum Gray weight of $C$ is the smallest nonzero Gray weight among all codewords. If $C$ is linear, then the minimum Gray distance is the same as the minimum Gray weight.

**Lemma 2.1.** The Gray map $\phi$ is a distance preserving map from $(S_p^n, Gray distance)$ to $(F_p^{3n}, Hamming distance)$. Moreover it is also $F_p$-linear.

**Proof.** For $s_1, s_2 \in F_p$ and $a_1, a_2 \in S_p^n$, we have $\phi(s_1 a_1 + s_2 a_2) = s_1 \phi(a_1) + s_2 \phi(a_2)$ by using the definition of Gray map. So $\phi$ is $F_p$-linear. Let $a_1 = (a_{1,1}, \ldots, a_{1,n})$ and $a_2 = (a_{2,1}, \ldots, a_{2,n})$ be elements of $S_p^n$ where $a_{1,i} = r_{1,i} + us_{1,i} + vt_{1,i}$ and $a_{2,i} = r_{2,i} + us_{2,i} + vt_{2,i}$ for $i = 1, \ldots, n$. Then $a_1 - a_2 = (a_{1,1} - a_{2,1}, \ldots, a_{1,n} - a_{2,n})$ and $\phi(a_1 - a_2) = \phi(a_1) - \phi(a_2)$. So $d_G(a_1, a_2) = w_G(a_1 - a_2) = w_H(\phi(a_1 - a_2)) = w_H(\phi(a_1) - \phi(a_2)) = d_H(\phi(a_1), \phi(a_2))$. By using the definition of the Gray weight of the element in $S_p$, the second equality above holds. \qed
Lemma 2.2. Let \( C \) be a \((n, M, d)\) linear code over \( S_p \), where \( n \) denotes the length, \( d \) denotes the minimum Gray distance and \( M \) denotes the size of \( C \). Then \( \phi(C) \) is a \([3n, \log_p M, d]\) linear code over \( F_p \).

**Proof.** From Lemma 2.1, we have \( \phi(C) \) is a \( F_p \) linear code. By using the Gray map, \( \phi(C) \) is length \( 3n \). As \( \phi \) is a bijective map from \( S_p^n \) to \( F_p^{3n} \), we have \( \phi(C) \) has dimension \( \log_p M \). As \( \phi \) is preserving distance, \( \phi(C) \) has minimum Hamming distance \( d \).

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 \( C = C^\perp \).

**Theorem 2.3.** Let \( C \) be a linear code over \( S_p \). Then \( \phi(C)^\perp = \phi(C^{\perp}) \). Moreover, if \( C \) is a self dual, so is \( \phi(C) \).

**Proof.** For all \( a_1 = (a_{1,1}, ..., a_{1,n}) \in C, a_2 = (a_{2,1}, ..., a_{2,n}) \in C \) where \( a_{j,i} = r_{j,i} + u s_{j,i} + v t_{j,i} \), with \( j = 1, 2 \) and \( i = 1, 2, ..., n \). If \( a_1 a_2 = 0 \) then we have \( a_1 a_2 = \sum_{i=1}^{n} a_{1,i} a_{2,i} = \sum_{i=1}^{n} (r_{1,i} s_{2,i} + s_{1,i} t_{2,i} + s_{2,i} t_{1,i}) = 0 \) implying \( \sum_{i=1}^{n} r_{1,i} t_{2,i} = 0 \), \( \sum_{i=1}^{n} (r_{1,i} s_{2,i} + s_{1,i} t_{2,i}) = 0 \), \( \sum_{i=1}^{n} (r_{1,i} s_{2,i} + s_{1,i} t_{2,i}) = 0 \), \( \sum_{i=1}^{n} (r_{1,i} t_{2,i} + s_{1,i} s_{2,i}) = 0 \), \( \sum_{i=1}^{n} (r_{1,i} t_{2,i} + t_{1,i} t_{2,i}) = 0 \). Hence \( \phi(C) \subseteq \phi(C^{\perp}) \). By using Lemma 2.2, from \( |\phi(C)^\perp| = |\phi(C^{\perp})| \), we have \( \phi(C)^\perp = \phi(C^{\perp}) \).

Clearly, \( \phi(C) \) is self orthogonal if \( C \) is self dual by Lemma 2.1. By using Lemma 2.2, we have \( |\phi(C)| = |C| \), so \( \phi(C) \) is self dual.

3 A representation of linear codes over \( S_p \)

We denote that

\[
A_1 \oplus A_2 \oplus A_3 = \{(a_1, a_2, a_3) : a_1 \in A_1, a_2 \in A_2, a_3 \in A_3 \}
\]

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 \( S_p \). Define

\[
C_1 = \{ r \in F_p^n : \exists s, t \in F_p^n, r + u s + v t \in C \}
\]

\[
C_2 = \{ r + s \in F_p^n : \exists t \in F_p^n, r + u s + v t \in C \}
\]

\[
C_3 = \{ r + t \in F_p^n : \exists s \in F_p^n, r + u s + v t \in C \}
\]

Then \( C_1, C_2 \) and \( C_3 \) are \( p \)-ary linear codes of length \( n \). Moreover, the linear code \( C \) of length \( n \) over \( S_p \) can be expressed as

\[
C = (1 - u - v)C_1 + u C_2 + v C_3
\]

**Theorem 3.1.** Let \( C \) be a linear code of length \( n \) over \( S_p \). Then \( \phi(C) = C_1 \otimes C_2 \otimes C_3 \) and \( |C| = |C_1||C_2||C_3| \).
Corollary 3.2. If \( \phi(C) = C_1 \otimes C_2 \otimes C_3 \), then \( C = (1 - u - v)C_1 \oplus uC_2 \oplus vC_3 \). It is easy to see that

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

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

Corollary 3.3. If \( G_1, G_2 \) and \( G_3 \) are generator matrices of \( p \)-ary linear codes \( C_1, C_2 \) and \( C_3 \) respectively, then the generator matrix of \( C \) is

\[
G = \begin{bmatrix}
(1 - u - v)G_1 \\
uG_2 \\
vG_3
\end{bmatrix}.
\]

We have

\[
\phi(G) = \begin{bmatrix}
\phi((1 - u - v)G_1) \\
\phi(uG_2) \\
\phi(vG_3)
\end{bmatrix}
\]

Let \( d_G \) minimum Gray weight of linear code \( C \) over \( S_p \). Then,

\[
d_G = d_H(\phi(C)) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}
\]

where \( d_H(C_1) \) denotes the minimum Hamming weights of \( p \)-ary codes \( C_1, C_2 \) and \( C_3 \), respectively.

4 Cyclic and Quasi-Cyclic Codes over \( S_p \)

Definition 4.1. A linear code \( C \) over \( S_p \) with the property that if \( a = (a_0, ..., a_{n-1}) \in C \) then \( \sigma(a) = (a_{n-1}, a_0, ..., a_{n-2}) \in C \) is called cyclic code.

A subset \( C \) of \( S_p^n \) is a linear cyclic code of length \( n \) iff it is a polynomial representation \( P(C) = \left\{ \sum_{i=0}^{n-1} a_i x^i : (a_0, ..., a_{n-1}) \in C \right\} \) is an ideal of \( S_p[x]/x^n - 1 \).

Definition 4.2. Let \( a \in F_{p}^{3n} \) with \( a = (a_0, a_1, ..., a_{3n-1}) = (a^{(0)} a^{(1)} a^{(2)}) \), \( a^{(i)} \in F_{p}^n \) for \( i = 0, 1, 2 \). Let \( \phi \) be a map from \( F_{p}^{3n} \) to \( F_{p}^{3n} \) given by \( \phi(a) = (\sigma(a^{(0)}), \sigma(a^{(1)}), \sigma(a^{(2)})) \) where \( \sigma \) is a cyclic shift from \( F_{p}^{n} \) to \( F_{p}^{n} \) given by \( \sigma(a^{(i)}) = (a^{(i+1)}, a^{(i+2)}, ..., a^{(i+n-2)}) \) for every \( a^{(i)} = (a^{(i,0)}, ..., a^{(i,n-1)}) \) where \( a^{(i,j)} \in F_{p}, j = 0, 1, ..., n - 1 \). A code of length \( 3n \) over \( F_{p} \) is said to be quasi cyclic code of index 3 if \( \phi(C) = C \).

Proposition 4.3. Let \( \phi \) be Gray map from \( S_p^n \) to \( F_{p}^{3n} \). Let \( \sigma \) be cyclic shift and \( \varphi \) be as above. Then \( \phi \sigma = \varphi \phi \).

Proof. Let \( c_i = r_i + u s_i + v t_i \) be the elements of \( S_p \) for \( i = 0, 1, ..., n - 1 \). We have \( \sigma(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2}) \). If we apply \( \phi \), we have

\[
\phi(\sigma(c_0, ..., c_{n-1})) = \phi(c_{n-1}, c_0, ..., c_{n-2}) = (r_{n-1}, ..., r_{n-2}, r_{n-1} + s_{n-1}, ..., r_{n-2} + s_{n-2}, r_{n-1} + t_{n-1}, ..., r_{n-2} + t_{n-2})
\]

On the other hand \( \phi(c_0, ..., c_{n-1}) = (r_0, ..., r_{n-1}, r_0 + s_0, ..., r_{n-1} + s_{n-1}, r_0 + t_0, ..., r_{n-1} + t_{n-1}) \). If we apply \( \varphi \), we have \( \varphi(\phi(c_0, c_1, ..., c_{n-1})) = (r_{n-1}, ..., r_{n-2}, r_{n-1} + s_{n-1}, ..., r_{n-2} + s_{n-2}, r_{n-1} + t_{n-1}, ..., r_{n-2} + t_{n-2}) \). Thus, \( \phi \sigma = \varphi \phi \).

Theorem 4.4. Let \( \sigma \) and \( \varphi \) be as above. A code \( C \) of length \( n \) over \( S_p \) is cyclic code if and only if \( \phi(C) \) is quasi-cyclic code of index 3 over \( F_p \) with length \( 3n \).
Proof. If $C$ is cyclic code, then $\sigma(C) = C$. By using Proposition 4.3, we have $\phi(\sigma(C)) = \varphi(\phi(C)) = \phi(C)$. So $\phi(C)$ is a quasi-cyclic code of index 3 of length $3n$ over $F_p$. Conversely if $\phi(C)$ is quasi-cyclic code of index 3, so $\varphi(\phi(C)) = \phi(C)$. So by using Proposition 4.3, we have $\phi(\sigma(C)) = \varphi(\phi(C)) = \phi(C)$. Since $\phi$ is injective, it follows that $\sigma(C) = C$.

Definition 4.5. A linear code $C$ over $S_p$ with the property that if $a = (a_0, ..., a_{n-1}) \in C$ then $\beta(a) = (-a_{n-1}, a_0, ..., a_{n-2}) \in C$ is called negacyclic code.

A subset of $S^n_p$ is a linear negacyclic code of length $n$ if it is polynomial representation

$P(C) = \left\{ \sum_{i=0}^{n-1} a_ix^i : (a_0, ..., a_{n-1}) \in C \right\}$ is an ideal of $S_p[x]/<x^n + 1>$. 

Proposition 4.6. Let $C = (1-u-v)C_1 \oplus uC_2 \oplus vC_3$ be a linear code over $S_p$. Then $C$ is a cyclic code (negacyclic) over $S_p$ if $C_1, C_2$ and $C_3$ are all cyclic (negacyclic) codes over $F_p$.

Proof. Let $(r_1, r_2, ..., r_n) \in C_1, (s_1, s_2, ..., s_n) \in C_2$ and $(t_1, t_2, ..., t_n) \in C_3$. Assume that $a_i = (1-u-v)r_i + us_i + vt_i$ for $i = 1, ..., n$. Then $(a_0, a_1, ..., a_{n-1}) \in C$. Since $C$ is a cyclic code, it follows that $(a_n, a_1, ..., a_{n-1}) \in C$. Note that $(a_n, a_1, ..., a_{n-1}) = (1-u-v)(r_n, r_1, ..., r_{n-1}) + u(s_n, s_1, ..., s_{n-1}) + v(t_n, t_1, ..., t_{n-1})$. Hence $(r_n, t_1, ..., t_{n-1}) \in C_1, (s_n, s_1, ..., s_{n-1}) \in C_2$ and $(t_n, t_1, ..., t_{n-1}) \in C_3$. Therefore, $C_1, C_2$ and $C_3$ are cyclic codes over $F_p$.

Conversely, suppose that $C_1, C_2$ and $C_3$ are all cyclic codes over $F_p$. Let $(a_1, a_2, ..., a_n) \in C$ where $a_i = (1-u-v)r_i + us_i + vt_i$ for $i = 1, ..., n$. Then $(r_1, r_2, ..., r_n) \in C_1, (s_1, s_2, ..., s_n) \in C_2$ and $(t_1, t_2, ..., t_n) \in C_3$. Note that $(a_n, a_1, ..., a_{n-1}) = (1-u-v)(r_n, r_1, ..., r_{n-1}) + u(s_n, s_1, ..., s_{n-1}) + v(t_n, t_1, ..., t_{n-1}) \in C = (1-u-v)C_1 \oplus uC_2 \oplus vC_3$. So, $C$ is a cyclic code over $S_p$.

For negacyclic codes, the proof is shown as similarly.

Definition 4.7. A subset $C$ of $S^n_p$ is called a quasi-cyclic code of length $n = sl$ and index $l$ if $C$ satisfies the following conditions,

i) $C$ is a submodule of $S^n_p$,

ii) If $e = (e_0, 0, ..., e_{0-l+1}, e_1, 0, ..., e_1-l+1, e_2, 0, ..., e_2-l+1, ..., e_{s-1,0}, ..., e_{s-1-l+1}, e_0, 0, ..., e_0-l+1, ..., e_{s-2,0}, ..., e_{s-2-l+1}) \in C$, 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 $a \in F_p^n$ with $a = (a_0, a_1, ..., a_{n-1}) = (a^{(0)}(a^{(1)}a^{(2)}))$, $a^{(i)} \in F_p^n$, for $i = 0, 1, 2$. Let $\Gamma$ be a map from $F_p^{3n}$ to $F_p^n$ given by

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

where $\mu$ is the map from $F_p^n$ to $F_p^n$ given by

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

for every $a^{(i)} = (a^{(i+s-1)}, ..., a^{(i+s-2)})$ where $a^{(i+j)} \in F_p^n$, $j = 0, 1, ..., s-1$ and $n = sl$. A code of length $3n$ over $F_p$ is said to be $l$-quasi cyclic code of index 3 if $\Gamma(C) = C$.

Proposition 4.8. Let $\tau_{s,l}$ be quasi-cyclic shift on $S_p$. Let $\Gamma$ be as above. Then $\phi \tau_{s,l} = \Gamma \phi$.

Proof. It is shown as proof of Proposition 4.3.

Theorem 4.9. The Gray image of quasi-cyclic codes over $S_p$ of length $n$ with index $l$ is a $l$-quasicyclic code of index 3 over $F_p$ with length $3n$.

Proof. It is shown as proof of Theorem 4.4.

5 Quantum Codes From Cyclic (Negacyclic) Codes Over $S_p$

Theorem 5.1. Let $C_1 = [n, k_1, d_1]_p$ and $C_2 = [n, k_2, d_2]_p$ be linear codes over $GF(q)$ with $C_2^\perp \subseteq C_1$. Furthermore, let $d = \min\{wt(v) : v \in (C_1 \setminus C_2^\perp) \cup (C_2^\perp \setminus C_1)\} \geq \min\{d_1, d_2\}$. Then there exists a quantum error-correcting code $C = [n, k_1 + k_2 - n, d]_p$. 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 $d_1 = \min\{wt(v) : v \in (C_1^\perp \setminus C_1)\}$.
Proposition 5.2. Suppose $C = (1-u-v)C_1 \oplus uC_2 \oplus vC_3$ is a cyclic (negacyclic) code of length $n$ over $S_p$. Then
\[ C = \langle (1-u-v)f_1(x), u f_2(x), v f_3(x) \rangle \]
and $|C| = p^{3n-(\deg f_1(x)+\deg f_2(x)+\deg f_3(x))}$ where $f_1(x), f_2(x)$ and $f_3(x)$ generator polynomials of $C_1$, $C_2$ and $C_3$ respectively.

Proposition 5.3. Suppose $C$ is a cyclic (negacyclic) code of length $n$ over $S_p$, then there is a unique polynomial $f(x)$ such that $C = \langle f(x) \rangle$ and $f(x) | x^n - 1$ if $(f(x) | x^n + 1)$ where $f(x) = (1-u-v)f_1(x) + u f_2(x) + v f_3(x)$.

Proposition 5.4. Let $C$ be a linear code of length $n$ over $S_p$, then $C^\perp = (1-u-v)C_1^\perp \oplus uC_2^\perp \oplus vC_3^\perp$. Furthermore, $C$ is self-dual code iff $C_1, C_2$ and $C_3$ are self-dual codes over $F_p$.

Proposition 5.5. If $C = (1-u-v)C_1 \oplus uC_2 \oplus vC_3$ is a cyclic (negacyclic) code of length $n$ over $S_p$. Then
\[ C^\perp = \langle (1-u-v)h_1(x)^* + uh_2(x)^* + vh_3(x)^* \rangle \]
and $|C^\perp| = p^{\deg f_1(x)+\deg f_2(x)+\deg f_3(x)}$ where for $i = 1, 2, 3$, $h_i(x)^*$ are the reciprocal polynomials of $h_i(x)$ i.e., $h_i(x) = (x^n - 1) / f_i(x), h_i(x) = (x^n + 1) / f_i(x), h_i^*(x) = x^{\deg h_i(x)}h_i(x^{-1})$ for $i = 1, 2, 3$.

Lemma 5.6. A p-ary linear cyclic (negacyclic) code $C$ with generator polynomial $f$ contains its dual code iff $x^n - 1 \equiv 0 \pmod{f f^*}$ ( $x^n + 1 \equiv 0 \pmod{f f^*}$), where $f^*$ is the reciprocal polynomial of $f$.

Theorem 5.7. Let $C = \langle (1-u-v)f_1, u f_2, v f_3 \rangle$ be a cyclic (negacyclic) code of length $n$ over $S_p$. Then $C^\perp \subseteq C$ iff $x^n - 1 \equiv 0 \pmod{f_1 f_2^*} \pmod{f_1 f_3^*}$ for $i = 1, 2, 3$.

Proof. Let $x^n - 1 \equiv 0 \pmod{f_1 f_2^*} \pmod{f_1 f_3^*}$ 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 $\langle 1-u-v \rangle C_1^{\perp} \subseteq \langle 1-u-v \rangle C_1 \subseteq uC_2^{\perp} \subseteq uC_2, vC_3^{\perp} \subseteq vC_3$. We have $\langle 1-u-v \rangle C_1^{\perp} \oplus uC_2^{\perp} \oplus vC_3^{\perp} \subseteq \langle 1-u-v \rangle C_1 \oplus uC_2 \oplus vC_3$. So, $\langle 1-u-v \rangle h_1^* + uh_2^* + vh_3^* \subseteq \langle 1-u-v \rangle f_1, u f_2, v f_3 >$. That is $C^{\perp} \subseteq C$.

Conversely, if $C^{\perp} \subseteq C$, then $\langle 1-u-v \rangle C_1^{\perp} \oplus uC_2^{\perp} \oplus vC_3^{\perp} \subseteq \langle 1-u-v \rangle C_1 \oplus uC_2 \oplus vC_3$. By thinking mod$(1-u-v)$, mod$(u)$ and mod$(v)$ respectively, we have $C_i^{\perp} \subseteq C_i$ for $i = 1, 2, 3$. Therefore, $x^n - 1 \equiv 0 \pmod{f_1 f_2^*} \pmod{f_1 f_3^*}$ for $i = 1, 2, 3$. \qed

Corollary 5.8. Let $C = \langle 1-u-v \rangle C_1 \oplus uC_2 \oplus vC_3$ be a cyclic (negacyclic) code of length $n$ over $S_p$. Then $C^{\perp} \subseteq C$ iff $C_i^{\perp} \subseteq C_i$ for $i = 1, 2, 3$.

Theorem 5.9. Let $C$ be a linear code of length $n$ over $S_p$ with $|C| = p^{3k_1+2k_2+k_3}$ and minimum distance $d$. Then $\phi(C)$ is a p-ary code $[3n, 3k_1 + 2k_2 + k_3, d]$ code.

Theorem 5.10. Let $(1-u-v)C_1 \oplus uC_2 \oplus vC_3$ be a cyclic (negacyclic) code of arbitrary length $n$ over $S_p$ with type $p^{3k_1}p^{2k_2}p^{k_3}$. If $C_i^{\perp} \subseteq C_i$, then $C^{\perp} \subseteq C$ and there exists a quantum error-correcting code with parameters $[[3n, 2(3k_1 + 2k_2 + k_3) - 3n, d_G]]$ where $d_G$ is the minimum Gray weights of $C$.

Example 5.11. Let $p = 2, n = 21$.
\[ x^{21} - 1 = (x+1)(x^2 + x + 1)(x^3 + x^2 + 1)(x^6 + x^4 + x^2 + 1) \]
\[ (x^6 + x^5 + x^4 + x^2 + 1) \]
in $F_2[x]$. Let $f_1(x) = f_2(x) = f_3(x) = x^6 + x^5 + x^4 + x^2 + 1$. $C$ is a linear code of length 21 and minimum Gray weight $d_G = 3$. Clearly, $C^\perp \subseteq C$. Hence we obtain a quantum code with parameters $[[63, 27, 3]]$.

Example 5.12. Let $p = 3, n = 10$. We have $x^{10} + 1 = (x^2 + 1)(x^4 + x^3 + 2x + 1)(x^4 + 2x^3 + x + 1)$. Let $f_1(x) = f_2(x) = x^4 + x^3 + 2x + 1, f_3(x) = x^4 + 2x^3 + x + 1$. Clearly, $C_i^\perp \subseteq C_i$. $\phi(C)$ is a linear code with parameters $[[30, 18, 4]]$. Hence, we obtain a quantum code with parameters $[[30, 6, 4]]$.
Example 5.13. Let \( p = 3, n = 12 \). We have \( x^{12} - 1 = (x - 1)^{3}(x^3 + x^2 + x + 1)^3 \) in \( F_3[x] \).

Example 5.14. Let \( p = 7, n = 3 \). We have \( x^3 + 1 = (x + 4)(x + 2)(x + 1) \phi(C) \) is a linear code with parameters \([9, 6, 2]\). Hence, we obtain a quantum code with parameters \([9, 3, 2]\).

6 Constacyclic codes over \( S_p \)

Definition 6.1. A linear code \( C \) over \( S_p \) with the property that if \( a = (a_0, ..., a_{n-1}) \in C \) then \( \nu(a) = (\lambda a_{n-1}, a_0, ..., a_{n-2}) \in C \) is called \( \lambda \)-constacyclic code over \( S_p \) where \( \lambda \) a unit element of \( S_p \).

A subset \( C \) of \( S_p^n \) is a linear \( \lambda \)-constacyclic code of length \( n \) iff it is polynomial representation \( P(C) = \{ \sum_{i=0}^{n-1} a_ix^i | (a_0, ..., a_{n-1}) \in C \} \) is an ideal of \( S_p[x] \) \( < x^n - \lambda >. \)

If \( \lambda \) is equal to 1 (-1), then \( C \) is called cyclic code (negacyclic) respectively.

We characterized the units of \( S_p \). For any element \( \lambda = r + us + vt \) of \( S_p \), \( \lambda \) is a unit if and only if \( r \neq 0, r + s \neq 0(\text{mod } p) \) and \( r + t \neq 0(\text{mod } p) \).

It is easily seen that 1 is only unit for \( p = 2 \).

Note that \( \lambda^n = 1 \), if \( n \) even; \( \lambda^n = \lambda \), if \( n \) odd, so for \( p \) is odd prime. We only study \( \lambda \)-constacyclic codes of odd length.

Theorem 6.2. Let \( \lambda \) be a unit in \( S_p \). Let \( C = (1 - u - v)C_1 \oplus uC_2 \oplus vC_3 \) be a linear code of length \( n \) over \( S_p \). Then \( C \) is a \( \lambda \)-constacyclic code of length \( n \) over \( S_p \) if \( C_i \) is either a cyclic code or a negacyclic code of length \( n \) over \( F_p \) for \( i = 1, 2, 3 \).

Proof. Let \( \nu \) be \( \lambda \)-constacyclic shift on \( S_p^n \). Let \( C \) be a \( \lambda \)-constacyclic code of length \( n \) over \( S_p \). 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 \( (m_0, m_1, ..., m_{n-1}) = (1 - u - v)(a_0, a_1, ..., a_{n-1}) + u(b_0, b_1, ..., b_{n-1}) + v(c_0, c_1, ..., c_{n-1}) \).

Since \( C \) is a \( \lambda \)-constacyclic code so, \( \nu(m) = (\lambda m_{n-1}, m_0, ..., m_{n-2}) \in C \) where \( m_i = a_i + b_iu + vc_i \) for \( i = 0, 1, ..., n - 1 \). Let \( \lambda = \alpha + u\beta + v\gamma \), where \( \alpha, \beta, \gamma \in F_p \). \( \nu(m) = (1 - u - v)(\lambda a_{n-1}, a_0, ..., a_{n-2}) + u(\lambda b_{n-1}, b_0, ..., b_{n-2}) + v(\lambda c_{n-1}, c_0, ..., c_{n-2}) \).

Then the units of \( F_p \) are 1 and -1, so \( \alpha = \pm 1 \). Therefore we have obtained the desired result. The other side it is seen easily.

Example 6.3. Let \( p = 3 \). Let \( C = (1 - u - v)C_1 \oplus uC_2 \oplus vC_3 \) be a linear code of length \( n \) over \( S_3 \).

The set of units of the ring \( S_3 \) is \( S_3^* = \{1, 2, 1 + u, 1 + v, 2 + 2u, 2 + 2v, 1 + u + v, 2 + 2u + 2v\} \).

So if \( C \) is a \( \lambda \)-constacyclic codes over \( S_3 \) where \( \lambda \) is a unit, then

<table>
<thead>
<tr>
<th>( C )</th>
<th>( C_1 )</th>
<th>( C_2 )</th>
<th>( C_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-constacyclic</td>
<td>negacyclic</td>
<td>negacyclic</td>
<td>negacyclic</td>
</tr>
<tr>
<td>1 + u constacyclic</td>
<td>cyclic</td>
<td>negacyclic</td>
<td>cyclic</td>
</tr>
<tr>
<td>1 + v constacyclic</td>
<td>cyclic</td>
<td>cyclic</td>
<td>negacyclic</td>
</tr>
<tr>
<td>2 + 2u constacyclic</td>
<td>negacyclic</td>
<td>cyclic</td>
<td>negacyclic</td>
</tr>
<tr>
<td>2 + 2v constacyclic</td>
<td>negacyclic</td>
<td>cyclic</td>
<td>negacyclic</td>
</tr>
<tr>
<td>1 + u + v constacyclic</td>
<td>cyclic</td>
<td>cyclic</td>
<td>negacyclic</td>
</tr>
<tr>
<td>2 + 2u + 2v constacyclic</td>
<td>cyclic</td>
<td>cyclic</td>
<td>negacyclic</td>
</tr>
</tbody>
</table>

where \( C_1, C_2 \) and \( C_3 \) are codes over \( F_3 \).
7 A representation linear codes over $S_p$ in terms of two linear codes over $F_p + uF_p$

Expressing an element of $S_p$ as $r + us + vt = a + vq$ where $a = r + su$ and $q = t$ are both in $F_p + uF_p$, we can see that $w_G(r + us + vt) = w_G(a + vq) = w_L(a) + w_L(a + q)$ where $w_L(x)$ denotes the Lee weight of $x$ in $F_p + uF_p$. This leads to the following Gray map

$$\phi_1 : (S_p, \text{Gray distance}) \longrightarrow ((F_p + uF_p)^2, \text{Lee distance})$$

$$\phi_1(r + us + vt) = a + vq = (a, a + q)$$

It is easy to verify $\phi_1$ is a linear map and it can be extended to $S_p^n$ naturally,

$$\phi_1(c_1, ..., c_n) = (a_1, ..., a_n, a_1 + a_2 + ... + a_n + q)$$

where $r_i = a_i + vq_i$. Moreover $\phi_1$ is a linear isometry from $(S_p^n, \text{Gray distance})$ to $((F_p + uF_p)^2n, \text{Lee distance}).$

Theorem 7.1. If $C$ is a linear code of length $n$ over $S_p$, then $\phi_1(C)$ is a linear code of length $2n$ over $F_p + uF_p$.

Define

$$C_1 = \{a \in (F_p + uF_p)^n | a + vq \in C \text{ for some } q \in (F_p + uF_p)^n\}$$

and

$$C_2 = \{a + q \in (F_p + uF_p)^n | a + vq \in C\}$$

Theorem 7.2. Let $C$ be a linear code of length $n$ over $S_p$. Then $C = (1 - v)C_1 \oplus vC_2$, $\phi_1(C) = C_1 \oplus C_2$ and $|C| = |C_1||C_2|$.

Theorem 7.3. Let $C$ be a linear code of length $n$ over $S_p$. Then $\phi_1(C^\perp) = (\phi_1(C))^\perp$.

Theorem 7.4. Let $C$ be a linear code of length $n$ over $S_p$ such that $C = (1 - v)C_1 \oplus vC_2$. Then $C^\perp = (1 - v)C_1^\perp \oplus vC_2^\perp$.

Theorem 7.5. Let $\lambda$ be a unit in $S_p$. Let $C = (1 - v)C_1 \oplus vC_2$ be a linear code of length $n$ over $S_p$. Then $C$ is a $\lambda$-constacyclic code of length $n$ over $S_p$ if and only if $C_i$ is either a cyclic code or a negacyclic code or $\xi$-constacyclic codes of length $n$ over $F_p$ for $i = 1, 2, 3$ where $\xi$ is a unit on $F_p + uF_p$.

Proof. It is shown as in the proof of the Theorem 6.2. □

Example 7.6. Let $p = 3$. Let $C = (1 - v)C_1 \oplus vC_2$ be a linear code of length $n$ over $S_3$. The set of units of the ring $S_3$ is $S_3^* = \{1, 2, 1 + u, 1 + v, 2 + 2u, 2 + 2v, 1 + u + v, 2 + 2u + 2v\}$. The set of units of the ring $F_3 + uF_3$ is $(F_3 + uF_3)^* = \{1, 2, 1 + u, 2 + 2u\}$.

If $C$ is a $\lambda$-constacyclic codes over $S_3$, where $\lambda$ is a unit, then

<table>
<thead>
<tr>
<th>$C$</th>
<th>$C_1$</th>
<th>$C_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 + u$</td>
<td>$1 + u$-constacyclic</td>
<td>cyclic</td>
</tr>
<tr>
<td>$1 + v$</td>
<td>cyclic</td>
<td>negacyclic</td>
</tr>
<tr>
<td>$2 + 2u$</td>
<td>$(2 + 2u)$constacyclic</td>
<td>$(2 + 2u)$constacyclic</td>
</tr>
<tr>
<td>$2 + 2v$</td>
<td>negacyclic</td>
<td>cyclic</td>
</tr>
<tr>
<td>$1 + u + v$</td>
<td>$(1 + u)$constacyclic</td>
<td>negacyclic</td>
</tr>
<tr>
<td>$2 + 2u + 2v$</td>
<td>$(2 + 2u)$constacyclic</td>
<td>negacyclic</td>
</tr>
</tbody>
</table>

where $C_1$ and $C_2$ are codes over $F_3 + uF_3$, $u^2 = u$. 
8 Skew Codes Over $S_p$

We are interested in studying skew codes using the ring $S_p$. We define non-trivial ring automorphism $\theta_p$ on the ring $S_p$ by $\theta_p(r+us+vt) = r + ut + vs$ for all $r + us + vt \in S_p$.

The ring $S_p[x, \theta_p] = \{a_0 + a_1x + ... + a_{n-1}x^{n-1} : a_i \in S_p, n \in N\}$ is called a skew polynomial ring. This ring is a non-commutative ring. The addition in the ring $S_p[x, \theta_p]$ is the usual polynomial addition and multiplication is defined using the rule, $(ax^i)(bx^j) = ab\theta_p^{i+j}(x)x^{i+j}$.

Note that $\theta_p^2(a) = a$ for all $a \in R$. This implies that $\theta_p$ is a ring automorphism of order 2.

**Definition 8.1.** A subset $C$ of $S_p^n$ is called a skew cyclic code of length $n$ if $C$ satisfies the following conditions,

i) $C$ is a submodule of $S_p^n$,

ii) If $c = (c_0, c_1, ..., c_{n-1}) \in C$, then $\sigma_{\theta_p}(c) = (\theta_p(c_{n-1}), \theta_p(c_0), ..., \theta_p(c_{n-2})) \in C$.

Let $f(x) + (x^n - 1)$ be an element in the set $S_{p,n} = S_p[x, \theta_p] / (x^n - 1)$ and let $r(x) \in S_p[x, \theta_p]$. Define multiplication from left as follows,

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

for any $r(x) \in S_p[x, \theta_p]$.

**Theorem 8.2.** $S_{p,n}$ is a left $S_p[x, \theta_p]$-module where multiplication defined as in above.

**Theorem 8.3.** A code $C$ in $S_p$ is a skew cyclic code if and only if $C$ is a left $S_p[x, \theta_p]$-submodule of the left $S_p[x, \theta_p]$-module $S_{p,n}$.

**Theorem 8.4.** Let $C$ be a skew cyclic code in $S_p$ 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 8.5.** A module skew cyclic code of length $n$ over $S_p$ is free iff it is generated by a monic right divisor $f(x)$ of $x^n - 1$. Moreover, the set $\{f(x), xf(x), x^2f(x), ..., x^{n-deg(f(x))}f(x)\}$ forms a basis of $C$ and the rank of $C$ is $n - \deg(f(x))$.

**Theorem 8.6.** Let $n$ be odd and $C$ be a skew cyclic code of length $n$ over $S_p$. Then $C$ is equivalent to cyclic code of length $n$ over $S_p$.

**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 $a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ be a codeword in $C$.

Note that $x^{2b}a(x) = \theta_p^{2b}(a_0)x^{1+zn} + \theta_p^{2b}(a_1)x^{2+zn} + ... + \theta_p^{2b}(a_{n-1})x^{n+z2n} = a_{n-1} + a_0x + ... + a_{n-2}x^{n-2} \in C$. Thus $C$ is a cyclic code of length $n$.

**Corollary 8.7.** Let $n$ be odd. Then the number of distinct skew cyclic codes of length $n$ over $S_p$ is equal to the number of ideals in $S_p[x] / (x^n - 1)$ because of Theorem 8.6. If $x^n - 1 = \sum_{i=0}^{r} p_i(x)$ where $p_i(x)$ are irreducible polynomials over $F_p$. Then the number of distinct skew cyclic codes of length $n$ over $S_p$ is $\sum_{i=0}^{r}(s_i + 1)^3$.

**Definition 8.8.** A subset $C$ of $S_p^n$ is called a skew quasi-cyclic code of length $n$ if $C$ satisfies the following conditions,

i) $C$ is a submodule of $S_p^n$,

ii) If $c = (c_{0,0}, ..., c_{0,1}, 1, 0, ..., c_{1,1}, 1, 0, ..., c_{s-1,1}, 1, 0, ..., c_{s-1,1}) \in C$, then $\tau_{p,s}[c] = (\theta_p(c_{s-1,0}), ..., \theta_p(c_{1,1}), \theta_p(c_{0,1}), ..., \theta_p(c_{0,0}), ..., \theta_p(c_{s-2,0}), ..., \theta_p(c_{s-1,1})) \in C$.

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

The ring $S_{p,s} = (S_p[x, \theta_p] / (x^s - 1))$ is a left $S_{p,s} = S_p[x, \theta_p] / (x^s - 1)$ module by the following multiplication on the left

$$f(x)(g_1(x), ..., g_t(x)) = (f(x)g_1(x), ..., f(x)g_t(x))$$
If the map $\gamma$ is defined by

$$\gamma : S_p^n \rightarrow S_{p,s}^l$$

$$(c_0,0, ..., c_{l-1}, c_1,0, ..., c_{l-1}, ..., c_s-1,0, ..., c_{s-1},l-1) \mapsto (c_0(x), ..., c_{l-1}(x))$$

such that $c_j(x) = \sum_{i=0}^{n-1} c_{i,j} x^i \in S_{p,s}^l$, where $j = 0, 1, ..., l-1$ then the map $\gamma$ gives a one to one correspondence $S_p^n$ and the ring $S_{p,s}^l$.

**Theorem 8.9.** A subset $C$ of $S_p^n$ is a skew quasi-cyclic code of length $n = sl$ and index $l$ if and only if $\gamma(C)$ is a left $S_{p,s}$-submodule of $S_{p,s}^l$.

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

Privately, such codes are called skew cyclic and skew negacyclic codes when $\lambda$ is equal to 1 and $-1$, respectively.

**Theorem 8.10.** A code $C$ of length $n$ over $S_p$ is skew constacyclic iff the skew polynomial representation of $C$ is a left ideal in $S_p\{x, \theta_p\}/(x^n - \lambda)$.

## 9 The Gray Images of Skew Codes Over $S_p$

**Proposition 9.1.** Let $\sigma_{p,\lambda}$ be the skew cyclic shift on $S_p^n$, let $\phi$ be the Gray map from $S_p^n$ to $F_p^{3n}$ and let $\varphi$ be as in the Section 4. Then $\phi \sigma_{p,\lambda} = \rho \varphi \phi$ where $\rho(x, y, z) = (x, z, y)$ for every $x, y, z \in F_p^n$.

**Proof.** Let $r_i = a_i + ub_i + \gamma c_i$ be the elements of $S_p$, for $i = 0, 1, ..., n-1$. We have $\sigma_{p,\lambda}((r_0, r_1, ..., r_{n-1})) = (\theta_p(r_{n-1}), \theta_p(r_0), ..., \theta_p(r_{n-2}))$. If we apply $\phi$, we have

$$\phi(\sigma_{p,\lambda}(r_0, ..., r_{n-1})) = \phi(\theta_p(r_{n-1}), \theta_p(r_0), ..., \theta_p(r_{n-2})) = (a_{n-1}, a_{n-2}, a_{n-1} + c_{n-1}, ..., a_{n-2} + c_{n-2}, a_{n-1} + b_{n-1}, ..., a_{n-2} + b_{n-2})$$

On the other hand, $\phi(r_0, ..., r_{n-1}) = (a_0, ..., a_{n-1}, a_0 + b_0, ..., a_{n-1} + b_{n-1}, a_0 + c_0, ..., a_{n-1} + c_{n-1})$. If we apply $\varphi$, we have $\varphi(\phi(r_0, r_1, ..., r_{n-1})) = (a_{n-1}, a_{n-2}, a_{n-1} + b_{n-1}, ..., a_{n-2} + b_{n-2}, a_{n-1} + c_{n-1}, ..., a_{n-2} + c_{n-2})$. If we apply $\rho$, we have $\rho(\phi(\phi(r_0, ..., r_{n-1}))) = (a_{n-1}, a_{n-2}, a_{n-1} + b_{n-1}, a_{n-2} + b_{n-2}, a_{n-1} + c_{n-1}, ..., a_{n-2} + c_{n-2})$. So, we have $\phi \sigma_{p,\lambda} = \rho \varphi \phi$.

**Theorem 9.2.** The Gray image a skew cyclic code over $S_p$ of length $n$ is permutation equivalent to quasi-cyclic code of index 3 over $F_p$ with length $3n$.

**Proof.** Let $C$ be a skew cyclic codes over $S_p$ of length $n$. That is $\sigma_{p,\lambda}(C) = C$. If we apply $\phi$, we have $\phi(\sigma_{p,\lambda}(C)) = \phi(C)$. From the Proposition 9.1, $\phi(\sigma_{p,\lambda}(C)) = \phi(C) = \rho(\varphi(\phi(C)))$. So, $\phi(C)$ is permutation equivalent to quasi-cyclic code of index 3 over $F_p$ with length $3n$.

**Proposition 9.3.** Let $\tau_{p,\lambda}$ be skew quasi-cyclic shift on $S_p^n$, let $\phi$ be the Gray map from $S_p^n$ to $F_p^{3n}$, let $\Gamma$ be as in the preliminaries, let $\rho$ be as above. Then $\phi \tau_{p,\lambda} = \rho \Gamma \phi$.

**Theorem 9.4.** The Gray image a skew quasi-cyclic code over $S_p$ of length $n$ is permutation equivalent to quasi-cyclic code of index 3 over $F_p$ with length $3n$.

**Proposition 9.5.** Let $\sigma_{p,\lambda}$ be skew constacyclic shift on $S_p^n$, let $\phi$ be the Gray map from $S_p^n$ to $F_p^{3n}$, let $\rho$ be as above. Then $\phi \sigma_{p,\lambda} = \rho \phi \sigma_{p,\lambda}$.

**Theorem 9.6.** The Gray image a skew constacyclic code over $S_p$ of length $n$ is permutation equivalent to the Gray image of constacyclic code over $F_p$ with length $3n$.

The proof of Proposition 9.3, 9.5 and Theorem 9.4, 9.6 are similar to the proof Proposition 9.1 and Theorem 9.2.
10 The MacWilliams Identities

The MacWilliams identity which describes how the weight enumerator of a linear code and the weight enumerator of the dual code relate to each other is very important subject in coding theory. It can be used to determine error detecting and error correcting capabilities of a code.

In this section, it is verified MacWilliams identity.

**Definition 10.1.** Let $A_i$ be the number of the elements of the Gray weight $i$ in $C$. Then the set $\{A_0, \ldots, A_{3n}\}$ is called the Gray weight distribution of $C$. Define the Gray weight enumerator of $C$ as

$$Gray_C(x, y) = \sum_{i=0}^{3n} A_i x^{3n-i} y^i$$

Clearly,

$$Gray_C(x, y) = \sum_{c \in C} x^{3n-w_C(c)} y^{w_C(c)}$$

Besides, define the complete weight enumerator of $C$ as

$$cwe_C(x_1, \ldots, x_{p-1+u(p-1)+v(p-1)}) = \sum_{c \in C} x_1^{w_1(c)} x_2^{w_2(c)} \cdots x_{p-1+u(p-1)+v(p-1)}^{w_{p-1+u(p-1)+v(p-1)}(c)}$$

For any codewords $c$ of $C$, let $u_0, u_1, u_2, u_3$ be the number of components of $C$ with Gray weights 0, 1, 2, 3 respectively. Then the Gray weight of $c$

$$w_C(c) = u_1 + 2u_2 + 3u_3$$

Define the symmetrized weight enumerator of $C$ as

$$swe_C(x_0, \ldots, x_3) = cwe_C(x_0, x_1, \ldots, x_{p-1+u(p-1)+v(p-1)}) = \sum_{c \in C} x_0^{u_0} \cdots x_3^{u_3}$$

The Hamming weight enumerator of $C$ is defined as

$$Ham_C(x, y) = \sum_{c \in C} x^{n-w_H(c)} y^{w_H(c)}$$

then we have the following results.

**Theorem 10.2.** Let $C$ be a linear code of length $n$ over $S_p$. Then

i) $Gray_C(x, y) = swe_C(x^3, x^2 y, xy^2, y^3)$

ii) $Ham_C(x, y) = swe_C(x, y, y, y)$

iii) $Gray_C(x, y) = Ham_{\phi(C)}(x, y)$

iv) $Gray_{C^\perp}(x, y) = \frac{1}{|C|} Gray_C(x + (p - 1)y, x - y)$

v) $Ham_{C^\perp}(x, y) = \frac{1}{|C|} Ham_C(x + (p^3 - 1)y, x - y)$

**Example 10.3.** Let $C = \{(0, 0), (1, 1)\}$ be a linear code of length 2 over $S_p$. The Gray weight enumerators for this code is $Gray_C(x, y) = x^6 + y^6$. The Gray weight enumerator of $C^\perp$ is $Gray_{C^\perp}(x, y) = \frac{1}{2}((x + (p - 1)y)^6 + (x - y)^6)$.

References


Author information
Abdullah Dertli, Department of Mathematics, Ondokuz Mayis 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

Received: June 12, 2017.
Accepted: March 15, 2018.