Chapter 2

Cyclic Codes over $\mathbb{F}_q[\mathsf{u},\mathsf{v},\mathsf{w}]/\langle \mathsf{u}^3-\mathsf{u}, \mathsf{v}^2-\mathsf{v}, \mathsf{w}^2-\mathsf{w}, \mathsf{uv}, \mathsf{vu}, \mathsf{uw}, \mathsf{wu}, \mathsf{vw}-\mathsf{wv}\rangle$

In this chapter, we study cyclic codes over a finite non-chain ring $\mathcal{S} \coloneqq \mathbb{F}_q[\mathsf{u},\mathsf{v},\mathsf{w}]/\langle \mathsf{u}^3-\mathsf{u}, \mathsf{v}^2-\mathsf{v}, \mathsf{w}^2-\mathsf{w}, \mathsf{uv}, \mathsf{vu}, \mathsf{uw}, \mathsf{wu}, \mathsf{vw}-\mathsf{wv}\rangle$. We discuss the structural properties of cyclic codes over $\mathcal{S}$ and their duals. We provide the construction of quantum and LCD codes from them and consequently obtain many new codes with better parameters.

2.1 The Ring $\mathcal{S}$

Let $\mathbb{F}_q$ be a finite field of order q, where $q = p^m$, p is an odd prime, and m is a positive integer. Consider,

$$\begin{aligned}\mathcal{S} :&= \mathbb{F}_q[\mathsf{u},\mathsf{v},\mathsf{w}]/\langle \mathsf{u}^3-\mathsf{u}, \mathsf{v}^2-\mathsf{v}, \mathsf{w}^2-\mathsf{w}, \mathsf{uv}, \mathsf{vu}, \mathsf{uw}, \mathsf{wu}, \mathsf{vw}-\mathsf{wv}\rangle \\ &= \mathbb{F}_q + \mathsf{u}\mathbb{F}_q + \mathsf{v}\mathbb{F}_q + \mathsf{w}\mathbb{F}_q + \mathsf{u}^2\mathbb{F}_q + \mathsf{vw}\mathbb{F}_q \\ &= \{r_1 + \mathsf{u}r_2 + \mathsf{v}r_3 + \mathsf{w}r_4 + \mathsf{u}^2 r_5 + \mathsf{vw}r_6 : r_j \in \mathbb{F}_q,\ j \in J\}.\end{aligned}$$

Then, $\mathcal{S}$ is a finite commutative ring under usual addition and multiplication of multivariate polynomials with identity $1+\mathsf{u}.0+\mathsf{v}.0+\mathsf{w}.0+\mathsf{u}^2.0+\mathsf{vw}.0$. Throughout this chapter, $J \coloneqq \{1,2,3,4,5,6\}$ Consider, two ideals $\langle \mathsf{u} \rangle$ and $\langle \mathsf{v} \rangle$ of $\mathcal{S}$ given as:

$$\begin{aligned}
\langle \mathsf{u} \rangle &= \{\mathsf{u}.(r_1 + \mathsf{u}r_2 + \mathsf{v}r_3 + \mathsf{w}r_4 + \mathsf{u}^2 r_5 + \mathsf{vw}r_6) : r_j \in \mathbb{F}_q,\ j \in J\} \\
&= \{\mathsf{u}(r_1 + r_5) + \mathsf{u}^2 r_2 : r_1, r_2, r_5 \in \mathbb{F}_q\} = \{\mathsf{u}r + \mathsf{u}^2 s : r, s \in \mathbb{F}_q\} \\
\langle \mathsf{v} \rangle &= \{\mathsf{v}.(r_1 + \mathsf{u}r_2 + \mathsf{v}r_3 + \mathsf{w}r_4 + \mathsf{u}^2 r_5 + \mathsf{vw}r_6) : r_j \in \mathbb{F}_q,\ j \in J\} \\
&= \{\mathsf{v}(r_1 + r_3) + \mathsf{vw}(r_4 + r_6) : r_1, r_4, r_5, r_6 \in \mathbb{F}_q\} = \{\mathsf{v}r + \mathsf{vw}s : r, s \in \mathbb{F}_q\}.
\end{aligned}$$

We observe that neither $\langle \mathsf{u} \rangle \subseteq \langle \mathsf{v} \rangle$ nor $\langle \mathsf{v} \rangle \subseteq \langle \mathsf{u} \rangle$. This shows that $\mathcal{S}$ is a **non-chain ring**.

Let

$$\begin{aligned}
\zeta_1 &= 1 - \mathsf{v} - \mathsf{w} + \mathsf{vw} - \mathsf{u}^2, \\
\zeta_2 &= 2^{-1}(\mathsf{u}^2 + \mathsf{u}), \\
\zeta_3 &= 2^{-1}(\mathsf{u}^2 - \mathsf{u}), \\
\zeta_4 &= \mathsf{vw}, \\
\zeta_5 &= \mathsf{v} - \mathsf{vw}, \\
\zeta_6 &= \mathsf{w} - \mathsf{vw}.
\end{aligned} \tag{2.1}$$

It can be easily verified that $\sum_{j=1}^{6} \zeta_j = 1$, $\zeta_j^2 = \zeta_j$ and $\zeta_i \zeta_j = 0$ for $i \neq j,\ i, j \in J$. Hence, $\{\zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_5, \zeta_6\}$ is a complete set of primitive orthogonal idempotents. Thus by a decomposition theorem of ring theory 1.1.48,

$$\mathcal{S} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{S} \cong \bigoplus_{j=1}^{6} \zeta_j \mathbb{F}_q.$$

Hence, any element $\mathsf{w} \in \mathcal{S}$ can be uniquely expressed as:

$$\mathsf{w} = \sum_{j=1}^{6} \zeta_j w_j, \ w_j \in \mathbb{F}_q, \ j \in J.$$

Moreover, we can view the ring $\mathcal{S}$ as a finite $\mathbb{F}_q$-algebra with $B_1 = \{1, u, v, w, u^2, vw\}$ and $B_2 = \{\zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_5, \zeta_6\}$ as its two bases. We define a bilinear form $(,) : \mathcal{S} \times \mathcal{S} \longrightarrow \mathbb{F}_q$ as:

$$(\mathsf{r}, \mathsf{s}) = (\sum_{j=1}^{6} \zeta_j r_j, \sum_{j=1}^{6} \zeta_j s_j) = \sum_{j=1}^{6} r_j s_j.$$

Then $(\mathsf{r}, \mathsf{s}) = 0, \ \forall \ \mathsf{s} \in \mathcal{S} \implies \mathsf{r} = 0$. This can be easily proved by taking $\mathsf{s} = \zeta_j, \ j \in J$. This shows that $(,)$ is non-degenerate. Therefore, $\mathcal{S}$ is a commutative, finite-dimensional Frobenius algebra over a finite field and hence it is a **Frobenius ring**.

Next, let $M \in GL_6(\mathbb{F}_q)$ be a matrix such that $MM^T = \lambda Id_6$ for some $\lambda \in \mathbb{F}_q^*$. We define a **Gray map** $\phi : \mathcal{S} \longrightarrow \mathbb{F}_q^6$ as:

$$\phi(\zeta_1 v_1 + \zeta_2 v_2 + \zeta_3 v_3 + \zeta_4 v_4 + \zeta_5 v_5 + \zeta_6 v_6) = (v_1, v_2, v_3, v_4, v_5, v_6)M.$$

It is easy to see that ϕ is bijective and linear. For any $\mathsf{v} = \sum_{j=1}^{6} v_j \zeta_j \in \mathcal{S}$, we define its Lee weight as: $wt_L(\mathsf{v}) = wt_H(\phi(\mathsf{v}))$, where wt_H denotes the Hamming weight. For any two $\mathsf{v}, \mathsf{w} \in \mathcal{S}$, their Lee distance is defined as: $d_L(\mathsf{v}, \mathsf{w}) = wt_L(\mathsf{v} - \mathsf{w})$. Now we can extend ϕ to $\Phi : \mathcal{S}^n \longrightarrow \mathbb{F}_q^{6n}$ as:

$$\Phi(\mathbf{w}) = \Phi(\mathsf{w}^0, \mathsf{w}^1, \ldots, \mathsf{w}^{n-1}) = (\phi(\mathsf{w}^0), \phi(\mathsf{w}^1), \ldots, \phi(\mathsf{w}^{n-1})).$$

For any $\mathbf{w} = (\mathsf{w}^0, \mathsf{w}^1, \ldots, \mathsf{w}^{n-1}) \in \mathcal{S}^n$, its Lee weight is given as:

$$wt_L(\mathbf{w}) = \sum_{i=0}^{n-1} wt_L(\mathsf{w}^i) = \sum_{i=0}^{n-1} wt_H(\phi(\mathsf{w}^i))$$

and for any two $\mathbf{v},\ \mathbf{w} \in \mathcal{S}^n$, their Lee distance is defined as: $d_L(\mathbf{v}, \mathbf{w}) = wt_L(\mathbf{v} - \mathbf{w})$.

Now, we'll give some properties of the Gray map defined above.

Theorem 2.1.1. The Gray map Φ is a bijective, linear, and distance-preserving map.

Proof. Since ϕ is bijective and linear, Φ is also bijective and linear. For the proof of later part, let $\mathbf{r}$ and $\mathbf{t} \in \mathcal{S}^n$ be such that

$\mathbf{r} = (\mathsf{r}^0, \mathsf{r}^1, \ldots, \mathsf{r}^{n-1}),\ \mathbf{t} = (\mathsf{t}^0, \mathsf{t}^1, \ldots, \mathsf{t}^{n-1}),$ where $\mathsf{r}^i = \sum_{j=1}^{6} \zeta_j r_j^i,\ \mathsf{t}^i = \sum_{j=1}^{6} \zeta_j t_j^i$. Now,

$$\begin{aligned}
d_L(\mathbf{r},\ \mathbf{t}) &= wt_L(\mathbf{r} - \mathbf{t}) \\
&= wt_L(\mathsf{r}^0 - \mathsf{t}^0, \mathsf{r}^1 - \mathsf{t}^1, \ldots, \mathsf{r}^{n-1} - \mathsf{t}^{n-1}) \\
&= \sum_{i=0}^{n-1} wt_L(\mathsf{r}^i - \mathsf{t}^i) \\
&= \sum_{i=0}^{n-1} wt_H(\phi(\mathsf{r}^i - \mathsf{t}^i)) \\
&= \sum_{i=0}^{n-1} wt_H(\phi(\mathsf{r}^i) - \phi(\mathsf{t}^i)) \\
&= wt_H(\phi(\mathsf{r}^0) - \phi(\mathsf{t}^0), \phi(\mathsf{r}^1) - \phi(\mathsf{t}^1), \ldots, \phi(\mathsf{r}^{n-1}) - \phi(\mathsf{t}^{n-1})) \\
&= wt_H((\phi(\mathsf{r}^0), \phi(\mathsf{r}^1), \ldots, \phi(\mathsf{r}^{n-1})) - (\phi(\mathsf{t}^0), \phi(\mathsf{t}^1), \ldots, \phi(\mathsf{t}^{n-1}))) \\
&= wt_H(\Phi(\mathbf{r}) - \Phi(\mathbf{t})) \\
&= d_H(\Phi(\mathbf{r}),\ \Phi(\mathbf{t})).
\end{aligned}$$

Hence, Φ is distance-preserving between $(\mathcal{S}^n, d_L)$ and $(\mathbb{F}_q^{6n}, d_H)$. □

Definition 2.1.2. For any two $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \ldots, \mathsf{c}^{n-1})$, $\mathbf{d} = (\mathsf{d}^0, \mathsf{d}^1, \ldots, \mathsf{d}^{n-1}) \in \mathcal{S}^n$, their Euclidean inner product is defined as:

$$\mathbf{c}.\mathbf{d} = \sum_{i=0}^{n-1} \mathsf{c}^i.\mathsf{d}^i,$$

and $\mathbf{c}$ is said to be orthogonal to $\mathbf{d}$ denoted as $\mathbf{c} \perp \mathbf{d}$ if $\mathbf{c}.\mathbf{d} = 0$.

Theorem 2.1.3. For any two $\mathbf{c}, \mathbf{d} \in \mathcal{S}^n$, $\mathbf{c} \perp \mathbf{d}$ if and only if $\Phi(\mathbf{c}) \perp \Phi(\mathbf{d})$. In other words, Φ preserves orthogonality.

Proof. Let $\mathbf{c}, \mathbf{d} \in \mathcal{S}^n$ such that $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \ldots, \mathsf{c}^{n-1})$ and $\mathbf{d} = (\mathsf{d}^0, \mathsf{d}^1, \ldots, \mathsf{d}^{n-1})$, where $\mathsf{c}^i = \sum_{j=1}^{6} \zeta_j c_j^i$ and $\mathsf{d}^i = \sum_{j=1}^{6} \zeta_j d_j^i$, $i = 0, 1, \ldots, n-1$. Now, using the definition of Euclidean inner product and properties of primitive orthogonal idempotents, we get

$$\begin{aligned}
\mathbf{c}.\mathbf{d} &= \sum_{i=0}^{n-1} \mathsf{c}^i.\mathsf{d}^i \\
&= \sum_{i=0}^{n-1} (\sum_{j=1}^{6} c_j^i \zeta_i).(\sum_{k=1}^{6} d_k^i \zeta_k) \\
&= \sum_{i=0}^{n-1} (\sum_{j=1}^{6} c_j^i d_j^i \zeta_j) \\
&= \sum_{j=1}^{6} (\sum_{i=0}^{n-1} c_j^i d_j^i) \zeta_j, \qquad (2.2)
\end{aligned}$$

and

$$\begin{aligned}
\Phi(\mathbf{c}).\Phi(\mathbf{d}) &= \Phi(\mathbf{c})\Phi(\mathbf{d})^T \\
&= \sum_{i=0}^{n-1} \phi(\mathsf{c}^i)\phi(\mathsf{d}^i)^T
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{n-1}(c_1^i, c_2^i, c_3^i, c_4^i, c_5^i, c_6^i)MM^T(d_1^i, d_2^i, d_3^i, d_4^i, d_5^i, d_6^i)^T \\
&= \lambda \sum_{i=0}^{n-1}(\sum_{j=1}^{6} c_j^i d_j^i) \\
&= \lambda \sum_{j=1}^{6}\sum_{i=0}^{n-1} c_j^i d_j^i. \qquad (2.3)
\end{aligned}
$$

Since, $\{\zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_5, \zeta_6\}$ is a linearly independent set and $\lambda \in \mathbb{F}_q^*$, from (2.2) and (2.3), we conclude that $\mathbf{c}.\mathbf{d} = 0$ if and only if $\Phi(\mathbf{c}).\Phi(\mathbf{d}) = 0$, i.e. $\mathbf{c} \perp \mathbf{d}$ if and only if $\Phi(\mathbf{c}) \perp \Phi(\mathbf{d})$. □

2.2 Linear and Cyclic Codes over $\mathcal{S}$

In this section, we describe the properties of linear and cyclic codes over $\mathcal{S}$. Using the results of the previous section (Theorems 2.1.1 and 2.1.3), we give the relation between a linear code over $\mathcal{S}$ and its Gray image (Theorem 2.2.2). Further, we discuss the structural properties of cyclic codes (Theorems 2.2.5, 2.2.6 and 2.2.7) and its dual (Corollaries 2.2.9 and 2.2.10). Finally, we conclude this section with a result that the Gray image of cyclic codes over $\mathcal{S}$ is quasi-cyclic code. (Theorem 2.2.11).

Definition 2.2.1. An $\mathcal{S}$-submodule of $\mathcal{S}^n$ is called a linear code of length n over $\mathcal{S}$.

Let $J = \{1, 2, 3, 4, 5, 6\}$. For a linear code $\mathcal{C}$ of length n over $\mathcal{S}$, we define

$$\mathcal{C}_k = \{\mathbf{a}_k \in \mathbb{F}_q^n | \ \exists\ \mathbf{a}_j \in \mathbb{F}_q^n \text{ for } j \in J \setminus \{k\} \text{ such that } \sum_{j=1}^{6} \zeta_j \mathbf{a}_j \in \mathcal{C}\}.$$

It may be noted that $\mathcal{C}_k$ is also a q-ary linear code of length n, for all $k \in J$. Moreover, $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$. It is worth noting that if $M = Id_6$ (identity matrix of order 6), then $\Phi(\mathcal{C}) = \bigotimes_{j=1}^{6} \mathcal{C}_j$ and $d(\mathcal{C}) = min_{j \in J} d(\mathcal{C}_j)$.

Theorem 2.2.2. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be an (n, q^k, d_L) linear code over $\mathcal{S}$. Then,

(i) $\Phi(\mathcal{C})$ is a $[6n, k, d_H]$ linear code over $\mathbb{F}_q$, where $d_H = d_L$;

(ii) $\Phi(\mathcal{C})^{\perp} = \Phi(\mathcal{C}^{\perp})$;

(iii) $\mathcal{C}^{\perp} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j^{\perp}$;

(iv) $\mathcal{C}$ is a self-orthogonal code if and only if $\Phi(\mathcal{C})$ is a self-orthogonal code over $\mathbb{F}_q$;

(v) $\mathcal{C}$ is a dual-containing code if and only if $\Phi(\mathcal{C})$ is a dual-containing code over $\mathbb{F}_q$;

(vi) $\mathcal{C}$ is a self-dual code if and only if $\Phi(\mathcal{C})$ is a self-dual code over $\mathbb{F}_q$.

Proof. (i) Clearly, length of $\Phi(\mathcal{C})$ is $6n$ as it is a subset of $\mathbb{F}_q^{6n}$. Furthermore, as Φ is bijective, we have $|\Phi(\mathcal{C})| = |\mathcal{C}| = q^k$. Therefore, $dim_{\mathbb{F}_q} \Phi(\mathcal{C}) = \log_q |\Phi(\mathcal{C})| = \log_q q^k = k$. By Theorem 2.1.1, $d_H = d_L$. Hence, $\Phi(\mathcal{C})$ is a $[6n, k, d_H]$ linear code over $\mathbb{F}_q$, where $d_H = d_L$.

(ii) Let $\mathbf{w} \in \Phi(\mathcal{C})^{\perp}$. Then, $\langle \mathbf{w}, \mathbf{v} \rangle = 0, \ \forall \ \mathbf{v} \in \Phi(\mathcal{C})$. Since Φ is bijective, we have $\langle \mathbf{w}, \Phi(\mathbf{u}) \rangle = 0, \ \forall \ \mathbf{u} \in \mathcal{C}$. Let $\mathbf{z} = \Phi^{-1}(\mathbf{w}) \in \mathcal{S}^n$. Thus, $\langle \Phi(\mathbf{z}), \Phi(\mathbf{u}) \rangle = 0, \ \forall \ \mathbf{u} \in \mathcal{C}$. Therefore, by Theorem 2.1.3, we have $\langle \mathbf{z}, \mathbf{u} \rangle = 0, \ \forall \ \mathbf{u} \in \mathcal{C}$. This shows that $\mathbf{z} \in \mathcal{C}^{\perp}$ and so $\mathbf{w} = \Phi(\mathbf{z}) \in \Phi(\mathcal{C}^{\perp})$. Therefore, $\Phi(\mathcal{C})^{\perp} \subseteq \Phi(\mathcal{C}^{\perp})$.

Conversely, let $\mathbf{w} \in \Phi(\mathcal{C}^{\perp})$. Then, $\exists!\ \mathbf{z} \in \mathcal{C}^{\perp}$ such that $\mathbf{w} = \Phi(\mathbf{z})$. Since Φ is bijective, we have $\langle \mathbf{z}, \Phi^{-1}(\mathbf{v}) \rangle = 0, \ \forall \ \mathbf{v} \in \Phi(\mathcal{C})$. Therefore, by Theorem 2.1.3, we have $\langle \Phi(\mathbf{z}), \mathbf{v} \rangle = \langle \mathbf{w}, \mathbf{v} \rangle = 0, \ \forall \ \mathbf{v} \in \Phi(\mathcal{C})$. This shows that $\mathbf{w} \in \Phi(\mathcal{C})^{\perp}$. Therefore, $\Phi(\mathcal{C}^{\perp}) \subseteq \Phi(\mathcal{C})^{\perp}$ as well. Hence, $\Phi(\mathcal{C}^{\perp}) = \Phi(\mathcal{C})^{\perp}$

(iii) Let $\mathcal{D} = \mathcal{C}^{\perp}$. Then,

$$\mathcal{D} = \left\{ \mathbf{w} \in \mathcal{S}^n \ : \langle \mathbf{w}, \mathbf{v} \rangle = 0, \forall\ \mathbf{v} \in \mathcal{C} \right\} .$$

$$= \left\{ \mathbf{w} \in \mathcal{S}^n : \langle \mathbf{w}, \sum_{j=1}^{6} \zeta_j \mathbf{v}_j \rangle = 0, \forall\ \mathbf{v}_j \in \mathcal{C}_j,\ j \in J \right\}.$$

Now,

$$\mathcal{D}_j = \left\{ \mathbf{w}_j \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_k \in \mathbb{F}_q^n, k \in J \setminus \{j\} \text{ such that } \sum_{j=1}^{6} \zeta_j \mathbf{w}_j \in \mathcal{D} \right\} .$$

$$= \left\{ \mathbf{w}_j \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_k \in \mathbb{F}_q^n, k \in J \setminus \{j\} \text{ such that } \left\langle \sum_{j=1}^{6} \zeta_j \mathbf{w}_j, \sum_{j=1}^{6} \zeta_j \mathbf{v}_j \right\rangle = 0 \right\} .$$

$$= \left\{ \mathbf{w}_j \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_k \in \mathbb{F}_q^n, k \in J \setminus \{j\} \text{ such that such that } \sum_{j=1}^{6} \zeta_j \langle \mathbf{w}_j, \mathbf{v}_j \rangle = 0 \right\} .$$

$$= \left\{ \mathbf{w}_j \in \mathbb{F}_q^n \ : \exists\ \mathbf{w}_k \in \mathbb{F}_q^n, k \in J \setminus \{j\} \text{ such that } \langle \mathbf{w}_j, \mathbf{v}_j \rangle = 0 \right.$$
$$\left. \forall\ j \in J, \text{ for any } \sum_{j=1}^{6} \zeta_j \mathbf{v}_j \in \mathcal{C} \right\} .$$

$$= \mathcal{C}_j^{\perp}.$$

Hence, $\mathcal{C}^{\perp} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{D}_j = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j^{\perp}$.

(iv) and (v) directly follow from the fact that for a bijective map Φ, $A \subseteq B \implies \Phi(A) \subseteq \Phi(B)$. Finally, (vi) follows by combining (iv) and (v).

□

Theorem 2.2.3. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a linear code of length n over $\mathcal{S}$. Furthermore, let G_j be a generator matrix of $[n, k_j]$ q-ary linear code $\mathcal{C}_j$, $j \in J$ and M be

the matrix used in Gray map ϕ such that

$$G_j = \begin{bmatrix} a_{00}^j & a_{01}^j & \dots & a_{0(n-1)}^j \\ a_{10}^j & a_{11}^j & \dots & a_{1(n-1)}^j \\ \vdots & \vdots & \vdots & \vdots \\ a_{(k_j-1)0}^j & a_{(k_j-1)1}^j & \dots & a_{(k_j-1)(n-1)}^j \end{bmatrix}_{k_j \times n} \quad \text{and } M = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{16} \\ m_{21} & m_{22} & \dots & m_{26} \\ \vdots & \vdots & \vdots & \vdots \\ m_{61} & m_{62} & \dots & m_{66} \end{bmatrix}.$$

Then, $G = \begin{bmatrix} G_1 \otimes M_{R_1} \\ G_2 \otimes M_{R_2} \\ \vdots \\ G_6 \otimes M_{R_6} \end{bmatrix}$ is a generator matrix of $\Phi(\mathcal{C})$, where M_{R_j} denotes the j^{th} row of M, $j \in J$.

Proof. Let $\mathbf{w} \in \Phi(\mathcal{C})$ be an arbitrary element. Since, Φ is bijective, there exists a unique $\mathbf{v} = \sum_{j=1}^{6} \zeta_j \mathbf{v}_j \in \mathcal{C}$ such that $\mathbf{v}_j = (\mathsf{v}_j^0, \mathsf{v}_j^1, \dots, \mathsf{v}_j^{n-1})$. Since, G_j is a generator matrix of $\mathcal{C}_j$, there exist $\alpha_{j,0}, \alpha_{j,1}, \dots, \alpha_{j,k_j-1}$ such that

$$\begin{aligned} \mathbf{v}_j &= \sum_{l=0}^{k_j-1} \alpha_{j,l}(a_{l0}^j, a_{l1}^j, \dots, a_{l(n-1)}^j) \\ &= \left(\sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l0}^j, \sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l1}^j, \dots \sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l(n-1)}^j \right). \end{aligned}$$

Then,

$$\begin{aligned} \mathbf{v} &= \sum_{j=1}^{6} \zeta_j \mathbf{v}_j \\ &= \sum_{j=1}^{6} \zeta_j \left(\sum_{l=0}^{k_j-1} \alpha_l a_{l0}^j, \sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l1}^j, \dots, \sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l(n-1)}^j \right) \\ &= \left(\sum_{j=1}^{6} \zeta_j (\sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l0}^j), \sum_{j=1}^{6} \zeta_j (\sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l1}^j), \dots, \sum_{j=1}^{6} \zeta_j (\sum_{l=0}^{k_j-1} \alpha_{j,l} a_{l(n-1)}^j) \right). \end{aligned}$$

Therefore, $\mathbf{w} = \Phi(\mathbf{v}) = (\mathtt{w}^0, \mathtt{w}^1, \ldots, \mathtt{w}^{n-1})$, where

$$\begin{aligned}
\mathtt{w}^i &= \phi(\sum_{j=1}^{6} \zeta_j(\sum_{l=0}^{k_j-1} \alpha_l a_{li}^j)) \\
&= (\sum_{l=0}^{k_1-1} \alpha_l a_{li}^1, \sum_{l=0}^{k_2-1} \alpha_l a_{li}^2, \sum_{l=0}^{k_3-1} \alpha_l a_{li}^3, \sum_{l=0}^{k_4-1} \alpha_l a_{li}^4, \sum_{l=0}^{k_5-1} \alpha_l a_{li}^5, \sum_{l=0}^{k_6-1} \alpha_l a_{li}^6) M \\
&= (\sum_{j=1}^{6} m_{j1}(\sum_{l=0}^{k_j-1} \alpha_l a_{li}^j), \sum_{j=1}^{6} m_{j2}(\sum_{l=0}^{k_j-1} \alpha_l a_{li}^j), \ldots, \sum_{j=1}^{6} m_{j6}(\sum_{l=0}^{k_j-1} \alpha_l a_{li}^j)) \\
&= \mathbf{a}\mathcal{G}^i, \text{ where}
\end{aligned}$$

$$\mathbf{a} = \begin{bmatrix} \alpha_{1,0} & \ldots & \alpha_{1,k_1-1} & \alpha_{2,0} & \ldots & \alpha_{2,k_2-1} & \ldots & \alpha_{6,0}, & \ldots & \alpha_{6,k_6-1} \end{bmatrix} \text{ and}$$

$$\mathcal{G}^i = \begin{bmatrix} m_{11}a_{0i}^1 & m_{12}a_{0i}^1 & \ldots & m_{16}a_{0i}^1 \\ m_{11}a_{1i}^1 & m_{12}a_{1i}^1 & \ldots & m_{16}a_{1i}^1 \\ \vdots & \vdots & \vdots & \vdots \\ m_{11}a_{(k_1-1)i}^1 & m_{12}a_{(k_1-1)i}^1 & \ldots & m_{16}a_{(k_1-1)i}^1 \\ \vdots & \vdots & \vdots & \vdots \\ m_{61}a_{0i}^6 & m_{62}a_{0i}^6 & \ldots & m_{66}a_{0i}^6 \\ m_{61}a_{1i}^6 & m_{62}a_{1i}^6 & \ldots & m_{66}a_{1i}^6 \\ \vdots & \vdots & \vdots & \vdots \\ m_{61}a_{(k_6-1)i}^6 & m_{62}a_{(k_6-1)i}^6 & \ldots & m_{66}a_{(k_6-1)i}^6 \end{bmatrix} = \begin{bmatrix} G_{1,C_i} \otimes M_{R_1} \\ G_{2,C_i} \otimes M_{R_2} \\ G_{3,C_i} \otimes M_{R_3} \\ G_{4,C_i} \otimes M_{R_4} \\ G_{5,C_i} \otimes M_{R_5} \\ G_{6,C_i} \otimes M_{R_6} \end{bmatrix},$$

where G_{j,C_i} denotes the i^{th} column of G_j, $j \in J$ and M_{R_j} denotes the j^{th} row of M. Thus,

$$\begin{aligned}
\mathbf{w} &= (\mathsf{w}^0, \mathsf{w}^1, \ldots, \mathsf{w}^{n-1}) \\
&= \mathbf{a} \begin{bmatrix} \mathcal{G}^0 & \mathcal{G}^1 & \ldots & \mathcal{G}^{n-1} \end{bmatrix}.
\end{aligned}$$

Hence,

$$G = \begin{bmatrix} \mathcal{G}^0 & \mathcal{G}^1 & \ldots & \mathcal{G}^{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} G_{1,C_0} \otimes M_{R_1} & G_{1,C_1} \otimes M_{R_1} & \dots & G_{1,C_{n-1}} \otimes M_{R_1} \\ G_{2,C_0} \otimes M_{R_2} & G_{2,C_1} \otimes M_{R_2} & \dots & G_{2,C_{n-1}} \otimes M_{R_2} \\ G_{3,C_0} \otimes M_{R_3} & G_{3,C_1} \otimes M_{R_3} & \dots & G_{3,C_{n-1}} \otimes M_{R_3} \\ G_{4,C_0} \otimes M_{R_4} & G_{4,C_1} \otimes M_{R_4} & \dots & G_{4,C_{n-1}} \otimes M_{R_4} \\ G_{5,C_0} \otimes M_{R_5} & G_{5,C_1} \otimes M_{R_5} & \dots & G_{5,C_{n-1}} \otimes M_{R_5} \\ G_{6,C_0} \otimes M_{R_6} & G_{6,C_1} \otimes M_{R_6} & \dots & G_{6,C_{n-1}} \otimes M_{R_6} \end{bmatrix} = \begin{bmatrix} G_1 \otimes M_{R_1} \\ G_2 \otimes M_{R_2} \\ G_3 \otimes M_{R_3} \\ G_4 \otimes M_{R_4} \\ G_5 \otimes M_{R_5} \\ G_6 \otimes M_{R_6} \end{bmatrix}$$

is a generator matrix of $\Phi(\mathcal{C})$. □

Definition 2.2.4. A linear code $\mathcal{C}$ of length n over $\mathcal{S}$ is said to be a cyclic code over $\mathcal{S}$ if $\sigma(\mathsf{c}_0, \mathsf{c}_1, \dots, \mathsf{c}_{n-1}) = (\mathsf{c}_{n-1}, \mathsf{c}_0, \mathsf{c}_1, \dots, \mathsf{c}_{n-2}) \in \mathcal{C}$ whenever $(\mathsf{c}_0, \mathsf{c}_1, \dots, \mathsf{c}_{n-1}) \in \mathcal{C}$.

Theorem 2.2.5. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a linear code of length n over $\mathcal{S}$. Then $\mathcal{C}$ is a cyclic code if and only if $\mathcal{C}_j$ is a cyclic code, for all $j \in J$.

Proof. Let $\mathcal{C}_j$ be a cyclic code, for all $j \in J$. Let $\mathbf{c} = (\mathsf{c}^0, \mathsf{c}^1, \mathsf{c}^2, \dots, \mathsf{c}^{n-1}) \in \mathcal{C}$. Suppose that for $i \in \{0, 1, \dots, n-1\}$, $\mathsf{c}^i = \sum_{j=1}^{6} \zeta_j c_j^i$. Then $(c_j^0, c_j^1, \dots, c_j^{n-1}) \in \mathcal{C}_j$. Since $\mathcal{C}_j$ is cyclic, we have

$\sigma(c_j^0, c_j^1, \dots, c_j^{n-1}) = (c_j^{n-1}, c_j^0, c_j^1, \dots, c_j^{n-2}) \in \mathcal{C}_j$, $j \in J$.

Thus $\sum_{j=1}^{6} \zeta_j (c_j^{n-1}, c_j^0, c_j^1, \dots, c_j^{n-2}) \in \mathcal{C}$.

This implies that

$$\begin{aligned} \sum_{j=1}^{6} \zeta_j (c_j^{n-1}, c_j^0, c_j^1, \dots, c_j^{n-2}) &= (\sum_{j=1}^{6} \zeta_j c_j^{n-1}, \sum_{j=1}^{6} \zeta_j c_j^0, \sum_{j=1}^{6} \zeta_j c_j^1, \dots, \sum_{j=1}^{6} \zeta_j c_j^{n-2}) \\ &= (\mathsf{c}^{n-1}, \mathsf{c}^0, \mathsf{c}^1, \dots, \mathsf{c}^{n-2}) \\ &= \sigma(\mathbf{c}) \in \mathcal{C}. \end{aligned}$$

This proves that $\mathcal{C}$ is cyclic.

Conversely, suppose that $\mathcal{C}$ is cyclic. Let $(c_j^0, c_j^1, \ldots, c_j^{n-1}) \in \mathcal{C}_j$, $j \in J$. Then

$$\sum_{j=1}^{6} \zeta_j (c_j^0, c_j^1, \ldots, c_j^{n-1}) = (\sum_{j=1}^{6} \zeta_j c_j^0, \sum_{j=1}^{6} \zeta_j c_j^1, \ldots, \sum_{j=1}^{6} \zeta_j c_j^{n-1}) \in \mathcal{C}$$

Since $\mathcal{C}$ is cyclic, we have

$$(\sum_{j=1}^{6} \zeta_j c_j^{n-1}, \sum_{j=1}^{6} \zeta_j c_j^0, \sum_{j=1}^{6} \zeta_j c_j^1, \ldots, \sum_{j=1}^{6} \zeta_j c_j^{n-2}) = \sum_{j=1}^{6} \zeta_j (c_j^{n-1}, c_j^0, c_j^1, \ldots, c_j^{n-2})$$
$$\in \mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j.$$

This implies that $(c_j^{n-1}, c_j^0, c_j^1, \ldots, c_j^{n-2}) = \sigma(c_j^0, c_j^1, \ldots, c_j^{n-1}) \in \mathcal{C}_j$, for all $j \in J$ which proves that they all are cyclic. □

Theorem 2.2.6. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a cyclic code of length n over $\mathcal{S}$ such that $\mathcal{C}_j = \langle f_j(y) \rangle$, i.e. $f_j(y)$ is the generator polynomial of $\mathcal{C}_j$, $j \in J$. Then $\mathcal{C} = \langle \zeta_1 f_1(y), \zeta_2 f_2(y), \zeta_3 f_3(y), \zeta_4 f_4(y), \zeta_5 f_5(y), \zeta_6 f_6(y) \rangle$ and $|\mathcal{C}| = q^{6n - \sum_{j=1}^{6} deg(f_j(y))}$

Proof. Since $\mathcal{C}_j = \langle f_j(y) \rangle$, $j \in J$ and $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$, we have

$$\mathcal{C} = \{c(y) | c(y) = \sum_{j=1}^{6} \zeta_j k_j(y), \text{ for some } k_j(y) \in \mathcal{C}_j, \ j \in J\}.$$

Therefore, $\mathcal{C} \subseteq \langle \zeta_1 f_1(y), \zeta_2 f_2(y), \zeta_3 f_3(y), \zeta_4 f_4(y), \zeta_5 f_5(y), \zeta_6 f_6(y) \rangle$. For any

$$\sum_{j=1}^{6} \zeta_j u_j(y) f_j(y) \in \langle \zeta_1 f_1(y), \zeta_2 f_2(y), \zeta_3 f_3(y), \zeta_4 f_4(y), \zeta_5 f_5(y), \zeta_6 f_6(y) \rangle$$
$$\subseteq \mathcal{S}[y]/\langle y^n - 1 \rangle,$$

where $u_j(y) \in \mathcal{S}[y]/\langle y^n - 1 \rangle$ for $j \in J$, there are $v_j(y) \in \mathbb{F}_q[y]$, $j \in J$ such that

$$\zeta_j u_j(y) = \zeta_j v_j(y)$$

This means that $\langle \zeta_1 f_1(y), \zeta_2 f_2(y), \zeta_3 f_3(y),\ \zeta_4 f_4(y),\ \zeta_5 f_5(y),\ \zeta_6 f_6(y)\rangle \subseteq \mathcal{C}$. Hence,

$$\langle \zeta_1 f_1(y), \zeta_2 f_2(y), \zeta_3 f_3(y), \zeta_4 f_4(y), \zeta_5 f_5(y), \zeta_6 f_6(y)\rangle = \mathcal{C}.$$

Since, $|\mathcal{C}| = \prod_{j=1}^{6} |\mathcal{C}_j|$, we have

$$|\mathcal{C}| = \prod_{j=1}^{6} |\mathcal{C}_j| = \prod_{j=1}^{6} q^{n-deg(f_j(y))} = q^{6n-\sum_{j=1}^{6} deg(f_j(y))}.$$

□

Theorem 2.2.7. For a cyclic code $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ of length n over $\mathcal{S}$, $\exists$ a unique $f(y)$ such that $\mathcal{C} = \langle f(y)\rangle$ and $f(y)|(y^n - 1)$ with $f(y) = \sum_{j=1}^{6} \zeta_j f_j(y)$, where $f_j(y)$ is the generator polynomial of $\mathcal{C}_j,\ j \in J$.

Proof. By Theorem 2.2.6, we have

$$\mathcal{C} = \langle \zeta_1 f_1(y), \zeta_2 f_2(y), \zeta_3 f_3(y), \zeta_4 f_4(y), \zeta_5 f_5(y), \zeta_6 f_6(y)\rangle,$$

where $f_j(y)$ is the generator polynomial of $\mathcal{C}_j,\ j \in J$. Let $f(y) = \sum_{j=1}^{6} \zeta_j f_j(y)$. Clearly $\langle f(y)\rangle \subseteq \mathcal{C}$. Note that $\zeta_j f_j(y) = \zeta_j f_j(y), \forall\ j \in J$ and $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ so $\mathcal{C} \subseteq \langle f(y)\rangle$. Since $f_j(y),\ j \in J$ are monic divisors of $y^n - 1 \in \mathbb{F}_q[y]$, $\exists\ v_j(y) \in \mathbb{F}_q[y]/\langle y^n - 1\rangle$ such that

$$y^n - 1 = v_j(y) f_j(y),\ j \in J$$

This implies that

$$y^n - 1 = \left(\sum_{j=1}^{6} \zeta_j v_j(y)\right) f(y) \in \mathcal{S}[y].$$

Hence, $f(y)|(y^n - 1)$. Since $f_j(y),\ j \in J$, are unique, so is $f(y)$. □

Corollary 2.2.8. For any positive integer n, $\mathcal{S}[y]/\langle y^n - 1\rangle$ is a principal ideal ring.

Proof. Let $\mathcal{C}$ be an ideal of $\mathcal{S}[y]/\langle y^n - 1\rangle$. Then $\mathcal{C}$ is a cyclic code of length n over $\mathcal{S}$. By Theorem 2.2.7, $\exists$ unique $f(y)$ such that $\mathcal{C} = \langle f(y)\rangle$. Hence, $\mathcal{S}[y]/\langle y^n - 1\rangle$ is a principal ideal ring. □

Corollary 2.2.9. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a cyclic code of length n over $\mathcal{S}$ then $\mathcal{C}^\perp = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j^\perp$ is also a cyclic code of length n over $\mathcal{S}$.

Proof. By Proposition 1.2.20, a linear code over a finite field is cyclic if and only if its dual is cyclic. And by Theorem 2.2.5, $\mathcal{C}$ is cyclic if and only if $\mathcal{C}_j$ is cyclic, $\forall\ j \in J$. Combining both these statements, the result follows. □

Corollary 2.2.10. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be cyclic code of length n over $\mathcal{S}$ such that $\mathcal{C}_j = \langle f_j(y)\rangle$, $j \in J$. Then $\mathcal{C}^\perp = \langle \sum_{j=1}^{6} \zeta_j g_j^*(y)\rangle$, where $g_j^*(y)$ is the reciprocal polynomials of $g_j(y) = (y^n - 1)/f_j(y)$, $j \in J$. Moreover, $|\mathcal{C}^\perp| = q^{\sum_{j=1}^{6} deg(f_j(y))}$.

Theorem 2.2.11. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be cyclic code of length n over $\mathcal{S}$. Then its Gray image $\Phi(\mathcal{C})$ is a quasi-cyclic code of length $6n$ and index 6 over $\mathbb{F}_q$.

Proof. By Proposition 2.2.2(i), $\Phi(\mathcal{C})$ is a linear code of length $6n$ over $\mathbb{F}_q$. In order to prove that $\Phi(\mathcal{C})$ is a quasi-cyclic code of index 6, let

$$(d_1^0, d_2^0, \ldots, d_6^0 | d_1^1, d_2^1, \ldots, d_6^1 | \ldots | d_1^{(n-1)}, d_2^{(n-1)}, \ldots, d_6^{(n-1)}) \in \Phi(\mathcal{C}).$$

Further, let $(d_1^i, d_2^i, \ldots, d_6^i)M^{-1} = (c_1^i, c_2^i, \ldots, c_6^i)$, $i = 0, 1, \ldots, n-1$. Then, $\phi(\sum_{j=1}^{6} \zeta_j c_j^i) = (d_1^i, d_2^i, \ldots, d_6^i)$ and $(\sum_{j=1}^{6} \zeta_j c_j^0, \sum_{j=1}^{6} \zeta_j c_j^1, \ldots, \sum_{j=1}^{6} \zeta_j c_j^{(n-1)}) \in \mathcal{C}$. Since, $\mathcal{C}$ is a cyclic code, we have

$$(\sum_{j=1}^{6} \zeta_j c_j^{(n-1)}, \sum_{j=1}^{6} \zeta_j c_j^0, \sum_{j=1}^{6} \zeta_j c_j^1, \ldots, \sum_{j=1}^{6} \zeta_j c_j^{(n-2)}) \in \mathcal{C}.$$

Therefore,

$$\begin{aligned}
&\Phi(\sum_{j=1}^{6}\zeta_j c_j^{(n-1)}, \sum_{j=1}^{6}\zeta_j c_j^{0}, \ldots, \sum_{j=1}^{6}\zeta_j c_j^{(n-2)}) \\
=&(\phi(\sum_{j=1}^{6}\zeta_j c_j^{(n-1)}), \phi(\sum_{j=1}^{6}\zeta_j c_j^{0}), \ldots, \phi(\sum_{j=1}^{6}\zeta_j c_j^{(n-2))}) \\
=&(d_1^{(n-1)}, d_2^{(n-1)}, \ldots, d_6^{(n-1)} | d_1^0, d_2^0, \ldots, d_6^0 | \ldots | d_1^{(n-2)}, d_2^{(n-2)}, \ldots, d_6^{(n-2)}) \\
&\in \Phi(\mathcal{C}).
\end{aligned}$$

This proves that $\Phi(\mathcal{C})$ is a quasi-cyclic code of index 6. □

2.3 Quantum Codes from Cyclic Codes over $\mathcal{S}$

This section deals with the construction of quantum codes from cyclic codes over $\mathcal{S}$. We start by recalling a criterion to find dual-containing cyclic codes over $\mathbb{F}_q$ and use it to characterize dual-containing cyclic codes over $\mathcal{S}$. Finally, we give a method to obtain quantum codes from dual-containing cyclic codes over $\mathcal{S}$ and utilize it to construct some new and better quantum codes.

Lemma 2.3.1. [22, Theorem 13] A cyclic code C with generator polynomial $f(y)$ contains its dual if and only if

$$y^n - 1 \equiv 0 \pmod{f(y)f^*(y)},$$

where $f^*(y)$ denotes the reciprocal polynomial of $f(y)$.

Theorem 2.3.2. Let $\mathcal{C} = \langle f(y) \rangle$ be a cyclic code of length n over $\mathcal{S}$, where $f(y) = \sum_{j=1}^{6} \zeta_j f_j(y)$. Then $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ iff

$$y^n - 1 \equiv 0 \pmod{f_j(y) f_j^*(y)}, \ \forall \ j \in J$$

where $f_j^*(y)$ denotes the reciprocal polynomials of $f_j(y), \ j \in J$.

Proof. Let $y^n - 1 \equiv 0 \pmod{f_j(y) f_j^*(y)}, \ \forall \ j \in J$. Then by the Lemma 2.3.1, we have

$$\mathcal{C}_j^{\perp} \subseteq \mathcal{C}_j, \ \forall \ j \in J.$$

This implies that

$$\zeta_j \mathcal{C}_j^{\perp} \subseteq \zeta_j \mathcal{C}_j, \ j \in J.$$

Therefore,

$$\bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j^{\perp} \subseteq \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j.$$

Hence, $\mathcal{C}^{\perp} \subseteq \mathcal{C}$.

Conversely, let us assume that $\mathcal{C}^{\perp} \subseteq \mathcal{C}$. Then

$$\bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j^{\perp} \subseteq \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j.$$

Since $\mathcal{C}_j$ is a q-ary code such that $\zeta_j \mathcal{C}_j = \mathcal{C} \pmod{\zeta_j}, \ j \in J$, we get $\mathcal{C}_j^{\perp} \subseteq \mathcal{C}_j, \ \forall \ j \in J$. Therefore,

$$y^n - 1 \equiv 0 \pmod{f_j(y) f_j^*(y)}, \ \forall \ j \in J.$$

□

Corollary 2.3.3. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a cyclic code of length n over $\mathcal{S}$. Then $\mathcal{C}^{\perp} \subseteq \mathcal{C}$ if and only if $\mathcal{C}_j^{\perp} \subseteq \mathcal{C}_j, \ \forall \ j \in J$.

Theorem 2.3.4. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be an (n, q^k, d_L) cyclic code over $\mathcal{S}$ and $f_j(y)$ be the generator polynomials of $\mathcal{C}_j$, $j \in J$.

(i) If $\mathcal{C}^{\perp} \subseteq \mathcal{C}$, then there exists a quantum error-correcting code with parameters $[[6n, 2k - 6n, d_H]]$, where $d_H = d_L$.

(ii) If $y^n - 1 \equiv 0 \pmod{f_j(y) f_j^*(y)}$, $\forall\ j \in J$, where $f_j^*(y)$ denotes the reciprocal polynomial of $f_j(y)$, then there exists a quantum error-correcting code(QECC) with parameters $[[6n, 2k - 6n, d_H]]$, where $d_H = d_L$.

Proof. (i) Let $\mathcal{C}^{\perp} = \mathcal{C}$. We have, $\Phi(\mathcal{C}^{\perp}) = (\Phi(\mathcal{C}))^{\perp}$, by part(ii) of Theorem 2.2.2. Using part(i) and part(iv) of Theorem 2.2.2, we conclude that $\Phi(\mathcal{C})$ is dual-containing $[6n, k, d_H]$ linear (in fact, 6-quasi cyclic) code over $\mathbb{F}_q$. Hence, by Lemma 1.3.6, there exists a quantum error-correcting code with parameters $[[6n, 2k - 6n, d_H]]$, where $d_H = d_L$.

(ii) Combining part (i) and Theorem 2.3.2, the result follows.

□

Now we conclude this section with some examples and a table of quantum codes constructed using Theorem 2.3.4. For computation purposes, SageMath [90] and MAGMA [17, 23] software are used.

Example 2.3.5. Let $q = 5,\ n = 5$ and

$$M = \begin{pmatrix} 4 & 2 & 2 & 4 & 2 & 2 \\ 3 & 1 & 3 & 3 & 1 & 3 \\ 2 & 2 & 4 & 2 & 2 & 4 \\ 3 & 1 & 2 & 2 & 4 & 3 \\ 3 & 3 & 4 & 2 & 2 & 1 \\ 4 & 2 & 3 & 1 & 3 & 2 \end{pmatrix} \in GL_6(\mathbb{F}_5).$$

Then $MM^T = 3Id_6$, so M can be used in Gray map $\phi : \mathcal{S} \longmapsto \mathbb{F}_5^6$. Consider the factorisation of $y^5 - 1$ in $\mathbb{F}_5[y]$ as: $\mathbf{y^5 - 1 = (y + 4)^5}$. Let

$$\begin{aligned} f_1(y) &= y + 4, \\ f_2(y) &= f_3(y) = 1, \\ f_4(y) &= y + 4, \\ f_5(y) &= 1, \\ f_6(y) &= (y + 4)^2 = y^2 + 3y + 1. \end{aligned}$$

From the factorization of $y^5 - 1$, it is clear that

$$y^5 - 1 \equiv 0 \pmod{f_j(y) f_j^*(y)},\ \forall\ j \in J.$$

Therefore $\mathcal{C}_j = \langle f_j(y) \rangle$ is a dual-containing cyclic codes of length 5 over $\mathbb{F}_5$, for all $j \in J$. Then $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ is a dual-containing cyclic code of length 5 and $\Phi(\mathcal{C})$ is a $[30, 26, 3]$ dual-containing 6-quasi cyclic code over $\mathbb{F}_5$. Hence by Theorem 2.3.4, there exists a $[[30, 22, 3]]_5$ quantum code which is better than $[[30, 20, 3]]_5$ obtained in [67].

Example 2.3.6. Let $q = 9$ and $n = 16$. Then $\mathbb{F}_9 \cong \mathbb{F}_3[X]/\langle X^2 - X - 1\rangle = \mathbb{F}_3(\gamma)$, where γ is a root of $X^2 - X - 1$. Further, let

$$M = \begin{pmatrix} \gamma+2 & 2\gamma+1 & 2\gamma & \gamma+2 & 2\gamma+1 & 2\gamma \\ 2 & 2\gamma+2 & \gamma+2 & 2 & 2\gamma+2 & \gamma+2 \\ \gamma+1 & 1 & \gamma+2 & \gamma+1 & 1 & \gamma+2 \\ 2\gamma+1 & \gamma+2 & \gamma & \gamma+2 & 2\gamma+1 & 2\gamma \\ 1 & \gamma+1 & 2\gamma+1 & 2 & 2\gamma+2 & \gamma+2 \\ 2\gamma+2 & 2 & 2\gamma+1 & \gamma+1 & 1 & \gamma+2 \end{pmatrix} \in GL_6().$$

Then $MM^T = (\gamma+1)Id_6$. Consider the factorisation of $y^{16} - 1 \in \mathbb{F}_9[y]$ as:

$$\begin{aligned} y^{16} - 1 =& (y+1)(y+2)(y+\gamma)(y+\gamma+1)(y+\gamma+2)(y+2\gamma)(y+2\gamma+1)(y+2\gamma+ \\ & 2)(y^2+\gamma)(y^2+\gamma+2)(y^2+2\gamma)(y^2+2\gamma+1). \end{aligned}$$

Let

$$\begin{aligned} f_1(y) &= y + \gamma, \\ f_2(y) &= 1, \\ f_3(y) &= y + 2\gamma + 1, \\ f_4(y) &= y + 2\gamma + 2, \\ f_5(y) &= 1, \\ f_6(y) &= y^2 + 2\gamma + 1. \end{aligned}$$

From the factorization of $y^{16} - 1$, it is clear that

$$y^{16} - 1 \equiv 0 \pmod{f_j(y) f_j^*(y)},$$

for all $j \in J$. Therefore $\mathcal{C}_j = \langle f_j(y) \rangle$ is a dual-containing cyclic codes of length 16 over $\mathbb{F}_9$, for all $j \in J$. Then $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ is a cyclic code of length 16 and $\Phi(\mathcal{C})$ is a $[96, 91, 3]$ dual-containing 6-quasi cyclic code over $\mathbb{F}_9$. Hence, by Theorem 2.3.4, there exists a $[[96, 86, 3]]_9$ QECC which has better parameters than $[[96, 84, 3]]_9$ constructed in [94].

In Table 2.2, we enlist the quantum codes obtained. The matrices used in the Gray map for $q = 5, 9$ will be the same as that used in Examples 2.3.5 and 2.3.6 respectively and those for $q = 7, 11, 13$ and 17 are listed below in Table 2.1:

q	7	11	13	17
M	$\begin{pmatrix} 5 & 3 & 4 & 5 & 3 & 4 \\ 3 & 5 & 3 & 3 & 5 & 3 \\ 4 & 3 & 5 & 4 & 3 & 5 \\ 2 & 4 & 3 & 5 & 3 & 4 \\ 4 & 2 & 4 & 3 & 5 & 3 \\ 3 & 4 & 2 & 4 & 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 5 & 4 & 1 & 5 & 4 & 1 \\ 6 & 10 & 7 & 6 & 10 & 7 \\ 5 & 6 & 6 & 5 & 6 & 6 \\ 6 & 7 & 10 & 5 & 4 & 1 \\ 5 & 1 & 4 & 6 & 10 & 7 \\ 6 & 5 & 5 & 5 & 6 & 6 \end{pmatrix}$	$\begin{pmatrix} 11 & 10 & 9 & 11 & 10 & 9 \\ 9 & 6 & 4 & 9 & 6 & 4 \\ 10 & 7 & 6 & 10 & 7 & 6 \\ 11 & 10 & 9 & 2 & 3 & 4 \\ 4 & 7 & 9 & 9 & 6 & 4 \\ 3 & 6 & 7 & 10 & 7 & 6 \end{pmatrix}$	$\begin{pmatrix} 4 & 5 & 12 & 4 & 5 & 12 \\ 7 & 5 & 14 & 7 & 5 & 14 \\ 16 & 4 & 10 & 16 & 4 & 10 \\ 13 & 12 & 5 & 4 & 5 & 12 \\ 10 & 12 & 3 & 7 & 5 & 14 \\ 1 & 13 & 7 & 16 & 4 & 10 \end{pmatrix}$
MM^T	$2Id_6$	$7Id_6$	$6Id_6$	$13Id_6$

q	n	$f_1(y)$	$f_2(y)$	$f_3(y)$	$f_4(y)$	$f_5(y)$	$f_6(y)$	$\Phi(C)$	$[[n,k,d]]_q$	Remark
5	4	1	1	1	1	1	$y+3$	$[24,23,2]$	$[[24,22,2]]_5$	MDS, new
5	5	$y+4$	1	1	$y+4$	1	y^2+3y+1	$[30,26,3]$	$[[30,22,3]]_5$	$[[30,20,3]]_5$ [67]
5	10	$y+1$	1	1	$y+1$	1	y^3+4y^2+4y+1	$[60,55,3]$	$[[60,50,3]]_5$	$[[60,48,3]]_5$ [91]
7	18	$y+3$	1	1	$y+3$	1	y^4+4y^3+2y+1	$[108,102,3]$	$[[108,96,3]]_7$	$[[108,93,3]]_7$ [16, 16]
9	13	y^3+2y^2+2y+2	1	1	1	1	y^3+y^2+y+2	$[78,72,3]$	$[[78,66,3]]_9$	new
9	16	$y+\gamma$	1	$y+2\gamma+1$	$y+2\gamma+2$	1	$y^2+2\gamma+1$	$[96,91,3]$	$[[96,86,3]]_9$	$[[96,84,3]]_9$ [94]
11	10	$y+5$	$y+9$	$y+8$	$y+7$	$y+5$	1	$[60,55,4]$	$[[60,50,4]]_{11}$	new BKQC
11	11	$y+10$	1	1	$y+10$	1	$(y+10)^3$	$[66,60,4]$	$[[66,54,4]]_{11}$	[[66,52,4]] [67]
13	3	$y+4$	1	$y+10$	1	$y+4$	1	$[18,15,3]$	$[[18,12,3]]_{13}$	$[[18,10,3]]_{13}$[67]
13	8	$y+5$	1	1	1	$y+8$	y^2+8	$[48,44,3]$	$[[48,40,3]]_{13}$	new
13	9	$y+4$	1	1	1	$y+10$	y^4+10y^3+4y+1	$[54,48,3]$	$[[54,42,3]]_{13}$	new
13	12	$y+3$	$y+10$	$y+9$	$y+8$	$y+10$	$y+3$	$[72,66,4]$	$[[72,60,4]]_{13}$	$[[36,30,2]]_{13}$[39]
17	4	$y+4$	1	1	1	1	1	$[24,23,2]$	$[[24,22,2]]_{17}$	MDS $[[24,18,2]]_{17}$ [39]
17	8	$y+4$	1	1	1	1	1	$[48,47,2]$	$[[48,46,2]]_{17}$	MDS, [25]
25	6	$w^{20}1$	1	1	$w^{16}1$	1	$w^4 1$	$[36,33,3]$	$[[36,30,3]]$	$[[36,28,3]]_{25}$ [93]

2.4 LCD Codes over $\mathcal{S}$

This section deals with LCD codes over $\mathcal{S}$. First, we recall some important characterizations for cyclic codes over a finite field to be LCD, given by Yang and Massey [97]. Then using these characterizations and decomposition of cyclic codes over $\mathcal{S}$, we give a method to find LCD codes from cyclic codes over $\mathcal{S}$. We conclude the section with some examples and provide a table of LCD codes over $\mathcal{S}$ whose Gray images are LCD codes over $\mathbb{F}_q$. Some of them are optimal.

Definition 2.4.1. ([68]) A code is said to be reversible if it has the property that reversing the order of the components of any codeword is again a codeword.

Lemma 2.4.2. ([97]) Let $C = \langle f(y) \rangle$ be a cyclic code of length n over $\mathbb{F}_q$, where $n = p^{k_1}.t$, p and t are relatively prime and $k_1 \geq 0$. Then C is an LCD cyclic code if and only if $f(y)$ is self-reciprocal and all monic irreducible factors of $f(y)$ have the same multiplicity in $f(y)$ and $y^n - 1$.

Lemma 2.4.3. ([97]) Let C be a cyclic code of length n over $\mathbb{F}_q$ such that $gcd(n, p) = 1$, where p is the characteristic of $\mathbb{F}_q$. Then C is an LCD code if and only if it is reversible.

Definition 2.4.4. A linear code $\mathcal{C}$ of length n over $\mathcal{S}$ is said to be a linear complementary dual (LCD) code over $\mathcal{S}$ if $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$.

Theorem 2.4.5. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a linear code of length n over $\mathcal{S}$. Then $\mathcal{C}$ is an LCD code if and only if $\mathcal{C}_j$ is an LCD code of length n over $\mathbb{F}_q$, $\forall\ j \in J$.

Proof. The proof follows from the fact that $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$ if and only if $\mathcal{C}_j \cap \mathcal{C}_j^{\perp} = \{0\}$, $\forall\ j \in J$. □

Theorem 2.4.6. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a cyclic code of length n over $\mathcal{S}$ and $f_j(y)$ be the generator polynomial of $\mathcal{C}_j$, $j \in J$. Then $\mathcal{C}$ is an LCD code if and only if

$f_j(y)$ is self-reciprocal and all the monic irreducible factors of $f_j(y)$ have the same multiplicity in $f_j(y)$ and $y^n - 1$, for $j \in J$.

Proof. Combining Lemma 2.4.2 and Theorem 2.4.5, the proof follows. □

Theorem 2.4.7. Let $\mathcal{C} = \bigoplus_{j=1}^{6} \zeta_j \mathcal{C}_j$ be a cyclic code of length n over $\mathcal{S}$ such that $gcd(n, p) = 1$. Then $\mathcal{C}$ is an LCD code if and only if $\mathcal{C}_j$, $j \in J$ are all reversible cyclic codes of length n.

Proof. Combining Lemma 2.4.3 and Theorem 2.4.5, the proof follows. □

Lemma 2.4.8. Let $\mathcal{C}$ be a linear code of length n over $\mathcal{S}$. Then $\Phi(\mathcal{C} \cap \mathcal{C}^{\perp}) = \Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp}$.

Proof. Let $\mathbf{w} \in \Phi(\mathcal{C} \cap \mathcal{C}^{\perp})$. Since Φ is onto, $\exists\ \mathbf{v} \in \mathcal{C} \cap \mathcal{C}^{\perp}$ such that $\Phi(\mathbf{v}) = \mathbf{w}$. As $\mathbf{v} \in \mathcal{C} \cap \mathcal{C}^{\perp}$, we have $\mathbf{v} \in \mathcal{C}$ and $\mathbf{v} \in \mathcal{C}^{\perp}$. Therefore, $\mathbf{w} \in \Phi(\mathcal{C})$, and $\mathbf{w} \in \Phi(\mathcal{C}^{\perp})$ and so $\mathbf{w} \in \Phi(\mathcal{C}) \cap \Phi(\mathcal{C}^{\perp}) = \Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp}$. Since, $\mathbf{w} \in \Phi(\mathcal{C} \cap \mathcal{C}^{\perp})$ is arbitrary, we have, $\Phi(\mathcal{C} \cap \mathcal{C}^{\perp}) \subseteq \Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp}$.

Again, let $\mathbf{w} \in \Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp}$, i.e. $\mathbf{w} \in \Phi(\mathcal{C})$, and $\mathbf{w} \in \Phi(\mathcal{C})^{\perp} = \Phi(\mathcal{C}^{\perp})$. Then $\exists\ \mathbf{u} \in \mathcal{C}$ and $\exists\ \mathbf{v} \in \mathcal{C}^{\perp}$ such that $\Phi(\mathbf{u}) = \mathbf{w}$ and $\Phi(\mathbf{v}) = \mathbf{w}$. Since, Φ is one-one as well, we have, $\mathbf{u} = \mathbf{v}$ and so $\mathbf{u}(= \mathbf{v}) \in \mathcal{C} \cap \mathcal{C}^{\perp}$. Therefore, $\mathbf{w} \in \Phi(\mathcal{C} \cap \mathcal{C}^{\perp})$. Since, $\mathbf{w} \in \Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp}$ is arbitrary, we have $\Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp} \subseteq \Phi(\mathcal{C} \cap \mathcal{C}^{\perp})$. Hence, $\Phi(\mathcal{C} \cap \mathcal{C}^{\perp}) = \Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp}$. □

Theorem 2.4.9. Let $\mathcal{C}$ be a linear code of length n over $\mathcal{S}$. Then $\mathcal{C}$ is an LCD code if and only if $\Phi(\mathcal{C})$ is an LCD code of length $6n$ over $\mathbb{F}_q$.

Proof. Suppose that $\mathcal{C}$ is an LCD code of length n over $\mathcal{S}$. Then by definition, $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$. By Lemma 2.4.8, we get $\Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp} = \Phi(\mathcal{C} \cap \mathcal{C}^{\perp}) = \Phi(\{0\}) = \{0\}$

which concludes that $\Phi(\mathcal{C})$ is an LCD of length $6n$ over $\mathcal{S}$. Conversely, suppose that $\Phi(\mathcal{C})$ is an LCD of length $6n$ over $\mathcal{S}$. Then $\Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp} = \{0\}$. Therefore, by Lemma 2.4.8, we have $\Phi(\mathcal{C} \cap \mathcal{C}^{\perp}) = \Phi(\mathcal{C}) \cap \Phi(\mathcal{C})^{\perp} = \{0\}$ which implies that $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$ as Φ is one-one. Hence, $\mathcal{C}$ is an LCD code of length n over $\mathcal{S}$. □

Now, we utilize the results obtained in this section to provide some examples of LCD codes over $\mathcal{S}$. For computation purposes, SageMath [90] and MAGMA [17, 23] software are used. The matrices used in the Gray map will be same as those in the previous section.

Example 2.4.10. Let $q = 5$ and $n = 8$. Now, consider the factorisation of $y^8 - 1$ in $\mathbb{F}_5[y]$ as:

$$y^8 - 1 = (y+1)(y+2)(y+3)(y+4)(y^2+2)(y^2+3).$$

Let

$$\begin{aligned} f_1(y) &= f_2(y) = 1, \\ f_3(y) &= f_4(y) = f_5(y) = y + 1, \\ f_6(y) &= (y^2+2)(y^2+3) = y^4 + 1. \end{aligned}$$

Then $f_j^*(y) = f_j(y)$ and all the irreducible factors of them have the same multiplicity in $f_j(y)$ and $y^8 - 1$, for all $j \in J$. Therefore $\mathcal{C}_j = \langle f_j(y) \rangle$, $j \in J$ are LCD codes of length 8 over $\mathbb{F}_5$. Hence by Theorem 2.4.6, $\mathcal{C} = \sum_{j=1}^{6} \zeta_j \mathcal{C}_j$ is an LCD code of length 8 over $\mathcal{S}$ with $d_L = 4$ and $\Phi(\mathcal{C})$ is a $[48, 41, 4]$ LCD 6-quasi cyclic code over $\mathbb{F}_5$ which is best known linear code (BKLC).

Example 2.4.11. Let $q = 7$ and $n = 6$. Consider the factorisation of $y^6 - 1$ in $\mathbb{F}_7[y]$ as:

$$y^6 - 1 = (y+1)(y+2)(y+3)(y+4)(y+5)(y+6).$$

Let

$$f_1(y) = 1,$$
$$f_2(y) = f_3(y) = f_4(y) = f_5(y) = y + 1,$$
$$f_6(y) = (y + 3)(y + 5) = y^2 + y + 1.$$

Then $f_j^*(y) = f_j(y)$ and all the irreducible factors of $f_j(y)$ have same multiplicity in $f_j(y)$ and $y^6 - 1$, for all $j \in J$. Therefore $\mathcal{C}_j = \langle f_j(y) \rangle$, $j \in J$ are LCD codes of length 6 over $\mathbb{F}_7$. Hence by Theorem 2.4.6, $\mathcal{C} = \sum_{j=1}^{6} \zeta_j \mathcal{C}_j$ is an LCD 6-quasi cyclic code of length 6 over $\mathcal{S}$ with $d_L = 4$ and $\Phi(\mathcal{C})$ is a $[36, 30, 4]$ LCD code over $\mathbb{F}_7$.

Finally, we conclude this section by enlisting some LCD codes over $\mathcal{S}$ in Table 2.3.

TABLE 2.3: LCD codes over $\mathcal{S}$ and their Gray Images

q	n	$f_1(y)$	$f_2(y)$	$f_3(y)$	$f_4(y)$	$f_5(y)$	$f_6(y)$	$\Phi(\mathcal{C})$	Remark
5	4	$y+1$	1	1	1	1	1	$[24, 23, 2]$	Optimal
5	6	$y+1$	$y+1$	$y+1$	$y+1$	$y+1$	y^3+2y^2+2y+1	$[36, 28, 4]$	
5	8	$y+1$	1	1	1	1	y^2+1	$[48, 45, 2]$	Optimal
5	8	1	1	$y+1$	$y+1$	$y+1$	y^4+1	$[48, 41, 4]$	BKLC
5	12	$y+1$	1	$y+1$	$y+1$	1	$y^4+y^3+2y^2+y+1$	$[72, 65, 4]$	BKLC
7	6	1	$y+1$	$y+1$	$y+1$	$y+1$	y^2+y+1	$[36, 30, 4]$	
7	10	$y+1$	1	1	1	1	$y^5+2y^4+2y^3+2y^2+2y+1$	$[60, 54, 3]$	
9	2	1	1	1	1	1	$y+1$	$[12, 11, 2]$	Optimal
9	5	1	1	1	1	1	$y^2+(2\gamma+1)y+1$	$[30, 28, 2]$	Optimal
17	3	y^2+y+1	1	1	1	1	y^2+y+1	$[18, 14, 3]$	

****