International J.Math. Combin. Vol.1(2026), 66-74

Ξ-cyclic Codes over $\mathbb{M}^l$ and Their Applications

Yasemin Cengellenmis

(Department of Mathematics, Trakya University, Edirne, Turkey)

Rabia Dertli and Abdullah Dertli

(Department of Mathematics, Ondokuz Mayıs University, Samsun, Turkey)

E-mail: ycengellenmis@gmail.com, rabia.alim06@gmail.com, abdullah.dertli@gmail.com

Abstract: In this article, for $\Xi \in Aut(\mathbb{M}^l)$, we give an algebraic characterization of a Ξ-cyclic code over $\mathbb{M}^l$, where $\mathbb{M} = \mathbb{F}_q + v\mathbb{F}_q$ with $v^2 = v$, $\mathbb{F}_q$ is a finite field with q elements, $q = p^m$ for prime p, positive integer m and $l \in \mathbb{N}$. We determine its generator polynomial and find its decomposition over $\mathbb{F}_q$. A necessary and sufficient condition for a Ξ-cyclic code over $\mathbb{M}^l$ to be Euclidean dual containing is given. We define an orthogonality preserving Gray map. By using CSS construction, we have the parameters of quantum codes from Ξ-cyclic codes over $\mathbb{M}^l$.

Key Words: Linear code, cyclic code, quantum code, generator polynomial, Gray map.

AMS(2010): 94B15.

§1. Introduction

As quantum error correcting codes protect quantum information, getting optimal quantum error correcting codes is also important in quantum communication and quantum computation. The first quantum codes were introduced by Shor and independently Steane in [7], [8]. Some authors constructed quantum codes by using the connection between classical error correcting codes and quantum codes [2]. In [1], Bhagat and Sarma studied $(\Theta, \Delta_\Theta, \mathbf{a})$ -cyclic codes on $R = \mathbb{F}_q^l$, for an automorphism Θ of R, a $\Theta-$ derivation Δ_Θ of R and $\mathbf{a} \in R^*$. They obtained quantum error correcting codes from them, by using CSS constructions.

In this article, we study Ξ -cyclic codes on $\mathbb{M}^l$, where $\mathbb{M} = \mathbb{F}_q + v\mathbb{F}_q$ with $v^2 = v$ and $l \geq 1$ constructed using an automorphism. It is worth mentioning that the automorphism class that we consider is much larger than what is considered in previous work in [5]. We take a more general form of an automorphism of $\mathbb{M}^l$, namely $\xi_1 \times \xi_2 ... \times \xi_l$, where each ξ_i is an automorphism of $\mathbb{M}$, for $i = 1, \cdots, l$. Later, motivated by the previous work in [1], we obtain the parameters of quantum codes from Ξ-cyclic codes over $\mathbb{M}^l, l \geq 1$.

The paper is organized as follows. Section 2 gives essential preliminaries on skew cyclic codes over $\mathbb{F}_q$ and $\mathbb{F}_q^l$. Section 3 investigates linear codes over $\mathbb{M}^l$, where $\mathbb{M} = \mathbb{F}_q + v\mathbb{F}_q$ with $v^2 = v$, $l \geq 1$. In section 4, we investigate Ξ-cyclic codes over $\mathbb{M}^l$ and establish a decomposition of Ξ-cyclic codes over $\mathbb{M}^l$. We find generator polynomial of Ξ-cyclic codes over $\mathbb{M}^l$. In section 5,

[1]Received October 17, 2025, Accepted February 16, 2026

we define orthogonality preserving Gray map from $(\mathbb{M}^l)^s$ to $(\mathbb{F}_q)^{2sl}$ and we construct quantum codes from Ξ-cyclic codes over $\mathbb{M}^l$ using CSS construction.

§2. Preliminaries

The set $\mathbb{F}_q^n = \{(r_1, \cdots, r_n) | r_u \in \mathbb{F}_q, u = 1, \cdots, n\}$ is a vector space over $\mathbb{F}_q$ with the usual component-wise addition and multiplication by scalars, where $\mathbb{F}_q$ is a finite field with $q = p^m$ elements, for prime p and positive integer m. A code $C_{\mathbb{F}_q}$ of length n over $\mathbb{F}_q$ is non-empty subset of $\mathbb{F}_q^n$ and a code $C_{\mathbb{F}_q}$ is a linear code over $\mathbb{F}_q$, if it is a subspace of $\mathbb{F}_q^n$. Let $\mathbf{c} = (c_1, \cdots, c_n) \in C_{\mathbb{F}_q}$, then the Hamming weight of $\mathbf{c}$ is defined as the number of non-zero components of $\mathbf{c}$ and denoted by $w_H(\mathbf{c})$. The Hamming distance between two codewords $\mathbf{c}, \mathbf{c}^{'} \in C_{\mathbb{F}_q}$ is given by $d_H(\mathbf{c}, \mathbf{c}^{'}) = w_H(\mathbf{c} - \mathbf{c}^{'})$. The minimum distance of $C_{\mathbb{F}_q}$ is defined as $d_H(C_{\mathbb{F}_q}) = min\{d_H(\mathbf{c}, \mathbf{c}^{'}) | \mathbf{c} \neq \mathbf{c}^{'}, \forall \mathbf{c}, \mathbf{c}^{'} \in C_{\mathbb{F}_q}\}$.

In [6], it was stated that the distinct automorphisms of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ are exactly the mapping $\theta_1, \cdots, \theta_{m-1}$ defined by $\theta_z(\alpha) = \alpha^{p^z}$ for $\alpha \in \mathbb{F}_{p^m}^*$ and $0 \leq z \leq m-1$. The automorphisms of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ construct a cyclic group of order m generated by θ_1.

In [1], Bhagat and Sarma investigated $(\theta, \delta_\theta, \alpha)$ -cyclic codes on $\mathbb{F}_q$, where $\theta \in Aut(\mathbb{F}_q)$, δ_θ is a θ-derivation, $\alpha \in \mathbb{F}_q^*$. By taking $\delta_\theta = 0, \alpha = 1$ in Section 4, [1], we can write the followings.

An $\mathbb{F}_q$-subspace $C_{\mathbb{F}_q}$ of $\mathbb{F}_q^n$ is called θ-cyclic code of length n over $\mathbb{F}_q$ if $T_{\theta, S_{\mathbb{F}_q}}(C_{\mathbb{F}_q}) \subseteq C_{\mathbb{F}_q}$, where $T_{\theta, S_{\mathbb{F}_q}}$ is a map of the form $T_{\theta, S_{\mathbb{F}_q}}(\mathbf{c}) = \theta(\mathbf{c}) S_{\mathbb{F}_q}$, where $\mathbf{c} = (c_0, \cdots, c_{n-1}) \in \mathbb{F}_q$, $\theta \in Aut(\mathbb{F}_q)$, $\theta(\mathbf{c}) = (\theta(c_0), \cdots, \theta(c_{n-1}))$ and

$$S_{\mathbb{F}_q} = \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \\ 1 & 0 & \dots & 0 \end{pmatrix} \in M_{n \times n}(\mathbb{F}_q)$$

For the polynomial representation,

$$\begin{aligned} \Lambda_{\mathbb{F}_q} \quad &: \quad \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x, \theta] / < x^n - 1 > \\ \mathbf{c} \quad &= \quad (c_0, \cdots, c_{n-1}) \longmapsto c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1} \end{aligned}$$

Let $C_{\mathbb{F}_q}$ be a subset of $\mathbb{F}_q^n$. Then $C_{\mathbb{F}_q}$ is a θ-cyclic code of length n over $\mathbb{F}_q$ if and only if $\Lambda_{\mathbb{F}_q}(C_{\mathbb{F}_q})$ is a left $\mathbb{F}_q[x, \theta]$-submodule of $\mathbb{F}_q[x, \theta] / < x^n - 1 >$. Moreover $\Lambda_{\mathbb{F}_q}(C_{\mathbb{F}_q})$ is generated by a unique monic polynomial $g(x) \in \mathbb{F}_q[x, \theta]$ and $g(x)$ is a right divisor of $x^n - 1$ in $\mathbb{F}_q[x, \theta]$.

In [1], by taking a more general form automorphism Θ of $\mathbb{F}_q^l$, they investigated $(\Theta, \Delta_\Theta, \mathbf{a})$-cyclic codes over $\mathbb{F}_q^l$, where Δ_Θ is a Θ-derivation and $\mathbf{a} \in (\mathbb{F}_q^l)^*, l \in \mathbb{N}$. In [1], the automorphisms of $\mathbb{F}_q^l$ were defined as

$$\begin{aligned} \theta_1 \times \cdots \times \theta_l \quad &: \quad \mathbb{F}_q^l \longrightarrow \mathbb{F}_q^l \\ (r_1, \cdots, r_l) \quad &\longmapsto \quad (\theta_1(r_1), \cdots, \theta_l(r_l)) \end{aligned}$$

where $\theta_i \in Aut(\mathbb{F}_q)$, for $i = 1, \cdots, l$. The set of automorphisms of $\mathbb{F}_q^l$ like that was presented as

$$\Omega_{\mathbb{F}_q^l} = \{\theta_1 \times \cdots \times \theta_l | \theta_i \in Aut(\mathbb{F}_q)\} \subset Aut(\mathbb{F}_q^l)$$

By taking $\Delta_\Theta = 0, \mathbf{a} = \mathbf{1}$, we can express the Definition 4.6 and Theorem 4.8 in [1], as follows;

Let $\Theta \in \Omega_{\mathbb{F}_q^l}$. An $\mathbb{F}_q^l$-submodule $C_{\mathbb{F}_q^l}$ of $(\mathbb{F}_q^l)^s$ is called Θ-cyclic code of length s over $\mathbb{F}_q^l$ if $T_{\Theta, \boldsymbol{S}_{\mathbb{F}_q^l}}(C_{\mathbb{F}_q^l}) \subseteq C_{\mathbb{F}_q^l}$, where $T_{\Theta, \boldsymbol{S}_{\mathbb{F}_q^l}}$ is a map of the form $T_{\Theta, \boldsymbol{S}_{\mathbb{F}_q^l}}(\mathbf{d}) = \Theta(\mathbf{d})\boldsymbol{S}_{\mathbb{F}_q^l}$ and

$$\begin{aligned} \mathbf{d} &= (\mathbf{d_0}, \cdots, \mathbf{d_{s-1}}) \in (\mathbb{F}_q^l)^s, \quad \Theta(\mathbf{d}) = (\Theta(\mathbf{d_0}), \cdots, \Theta(\mathbf{d_{s-1}})), \\ \mathbf{d_t} &= (d_{t,1}, \cdots, d_{t,l}), \quad \Theta(\mathbf{d_t}) = (\theta_1(d_{t,1}), \theta_2(d_{t,2}), \cdots, \theta_l(d_{t,l})) \end{aligned}$$

for $t = 0, \cdots, s-1$ and

$$\boldsymbol{S}_{\mathbb{F}_q^l} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \dots \\ \vdots & \vdots & \vdots & \ddots \\ \mathbf{1} & \mathbf{0} & \dots & \mathbf{0} \end{pmatrix} \in M_{s\times s}(\mathbb{F}_q^l)$$

where $\mathbf{1} = (1, \cdots, 1), \mathbf{0} = (0, \cdots, 0) \in \mathbb{F}_q^l$.

For the polynomial representation,

$$\begin{aligned} \Lambda_{\mathbb{F}_q^l} &: (\mathbb{F}_q^l)^s \longrightarrow \mathbb{F}_q^l[x, \Theta]/ < x^s - \mathbf{1} > \\ \mathbf{d} &= (\mathbf{d_0}, \cdots, \mathbf{d_{s-1}}) \longmapsto d(x) = \mathbf{d_0} + \mathbf{d_1}x + \cdots + \mathbf{d_{s-1}}x^{s-1} \end{aligned}$$

Let $C_{\mathbb{F}_q^l}$ be a subset of $(\mathbb{F}_q^l)^s$. Then $C_{\mathbb{F}_q^l}$ is a Θ-cyclic code of length s over $\mathbb{F}_q^l$ if and only if $\Lambda_{\mathbb{F}_q^l}(C_{\mathbb{F}_q^l})$ is a left $\mathbb{F}_q^l[x, \Theta]$-submodule of $\mathbb{F}_q^l[x, \Theta]/\langle x^s - \mathbf{1}\rangle$.

In [1], a linear code $C_{\mathbb{F}_q^l}$ of length s over $\mathbb{F}_q^l$ was uniquely written as

$$C_{\mathbb{F}_q^l} = \mathbf{e_1}C_{\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{\mathbb{F}_q,l} \qquad (*)$$

where

$$C_{\mathbb{F}_q,i} = \widetilde{\Pi_i}(C_{\mathbb{F}_q^l}) = \{(\Pi_i(\mathbf{d_0}), \cdots, \Pi_i(\mathbf{d_{s-1}})) \in (\mathbb{F}_q)^s | (\mathbf{d_0}, \cdots, \mathbf{d_{s-1}}) \in C_{\mathbb{F}_q^l}\}$$

are linear codes of length s over $\mathbb{F}_q$,

$$\begin{aligned} \widetilde{\Pi_i} &: (\mathbb{F}_q^l)^s \longrightarrow \mathbb{F}_q^s, \\ (\mathbf{r_0}, \cdots, \mathbf{r_{s-1}}) &\longmapsto (\Pi_i(\mathbf{r_0}), \cdots, \Pi_i(\mathbf{r_{s-1}})), \\ \Pi_i &: \mathbb{F}_q^l \longrightarrow \mathbb{F}_q, \\ \mathbf{r_t} = (r_{t,1}, \cdots, r_{t,l}) &\longmapsto r_{t,i} \end{aligned}$$

where $t = 0, 1, \cdots, s-1$, for $i = 1, \cdots, l$ and $\mathbf{e_1}, \cdots, \mathbf{e}_l$ standart ordered $\mathbb{F}_q$-basis for $\mathbb{F}_q^l$.

§3. Linear Codes over $\mathbb{M}^l$

For $l \in \mathbb{N}$, consider the product ring $\mathbb{M}^l$, where $\mathbb{M} = \mathbb{F}_q + v\mathbb{F}_q, v^2 = v$. Let

$$\begin{aligned} \mathbf{\Pi_1} \ &: \ \mathbb{M}^l \longrightarrow \mathbb{F}_q^l, \\ &(k_1 + vn_1, k_2 + vn_2, \cdots, k_l + vn_l) \longmapsto (k_1, k_2 \cdots, k_l), \\ \mathbf{\Pi_2} \ &: \ \mathbb{M}^l \longrightarrow \mathbb{F}_q^l \\ &(k_1 + vn_1, k_2 + vn_2, \cdots, k_l + vn_l) \longmapsto (k_1 + n_1, k_2 + n_2, \cdots, k_l + n_l). \end{aligned}$$

Extend each $\mathbf{\Pi_j}$ to $\widetilde{\mathbf{\Pi_j}}$ for $j = 1, 2$ as follows:

$$\begin{aligned} \widetilde{\mathbf{\Pi_j}} \ &: \ (\mathbb{M}^l)^s \longrightarrow (\mathbb{F}_q^l)^s, \\ &(\mathbf{m}_0, \cdots, \mathbf{m}_{s-1}) \longmapsto (\mathbf{\Pi_j(m_0)}, \cdots, \mathbf{\Pi_j(m_{s-1})}) \end{aligned}$$

where $\mathbf{m_t} = (m_{t,1}, \cdots, m_{t,l}) = (k_1^t + vn_1^t, \cdots, k_l^t + vn_l^t) \in \mathbb{M}^l, t = 0, \cdots, s-1$, for $j = 1, 2$.

Let $\boldsymbol{C}_{\mathbb{M}^l}$ be a linear code of length s over $\mathbb{M}^l$. For $j = 1, 2$, define

$$C_{j,\mathbb{F}_q^l} = \mathbf{\Pi}_j(\boldsymbol{C}_{\mathbb{M}^l}) = \widetilde{\{(\mathbf{\Pi}_j}(p_0), \cdots, \Pi_j(p_{s-1})) \in (\mathbb{F}_q^l)^s | (\mathbf{p}_0, \cdots, \mathbf{p}_{s-1}) \in \boldsymbol{C}_{\mathbb{M}^l}\}$$

then each $C_{j,\mathbb{F}_q^l}$ is a linear code of length s over $\mathbb{F}_q^l$, for $j = 1, 2$ and every linear code $\boldsymbol{C}_{\mathbb{M}^l}$ can be uniquely written as

$$\boldsymbol{C}_{\mathbb{M}^l} = (1 - v)C_{1,\mathbb{F}_q^l} \oplus vC_{2,\mathbb{F}_q^l}$$

From (*), we have

$$\boldsymbol{C}_{\mathbb{M}^l} = (1 - v)[\mathbf{e_1}C_{1,\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{1,\mathbb{F}_q,l}] \oplus v[\mathbf{e_1}C_{2,\mathbb{F}_q,1} \oplus ... \oplus \mathbf{e}_l C_{2,\mathbb{F}_q,l}]$$

where $C_{1,\mathbb{F}_q,i}, C_{2,\mathbb{F}_q,i}$ are linear codes of length s over $\mathbb{F}_q$, for $i = 1, \cdots, l$.

§4. Ξ-Cyclic Codes over $\mathbb{M}^l$

The map

$$\begin{aligned} \xi_1 \times \xi_2 \times ... \times \xi_l \ &: \ \mathbb{M}^l \longrightarrow \mathbb{M}^l \\ &(k_1 + vn_1, \cdots, k_l + vn_l) \longmapsto (\xi_1(k_1 + vn_1), \cdots, \xi_l(k_l + vn_l)) \end{aligned}$$

is an automorphism of $\mathbb{M}^l$ where $\xi_i \in Aut(\mathbb{M})$, $\xi_i(k_i + vn_i) = \theta_i(k_i) + v\theta_i(n_i)$, $\theta_i \in Aut(\mathbb{F}_q)$ for $i = 1, \cdots, l$.

The set of automorphisms of $\mathbb{M}^l$ like that is presented as

$$\Omega_{\mathbb{M}^l} = \{\xi_1 \times \cdots \times \xi_l | \xi_i \in Aut(\mathbb{M})\} \subset Aut(\mathbb{M}^l)$$

Let $\Xi \in \Omega_{\mathbb{M}^l}$. An $\mathbb{M}^l$-submodule $\boldsymbol{C}_{\mathbb{M}^l}$ of $(\mathbb{M}^l)^s$ is called Ξ-cyclic code of length s over $\mathbb{M}^l$ if $T_{\Xi,\boldsymbol{S}_{\mathbb{M}^l}}(\boldsymbol{C}_{\mathbb{M}^l}) \subseteq \boldsymbol{C}_{\mathbb{M}^l}$, where $T_{\Xi,\boldsymbol{S}_{\mathbb{M}^l}}$ is a map of the form $T_{\Xi,\boldsymbol{S}_{\mathbb{M}^l}}(\mathbf{p}) = \Xi(\mathbf{p})\boldsymbol{S}_{\mathbb{M}^l}, \mathbf{p} = (\mathbf{p}_0, \cdots, \mathbf{p}_{s-1}) \in (\mathbb{M}^l)^s$, $\Xi(\mathbf{p}) = (\Xi(\mathbf{p}_0), \cdots, \Xi(\mathbf{p}_{s-1})$, $\mathbf{p_t} = (\mathbf{p}_{t,1}, \cdots, \mathbf{p}_{t,l}) = (a_1^t + vb_1^t, \cdots, a_l^t + vb_l^t)$, $\Xi(\mathbf{p_t}) = (\xi_1(p_{t,1}), \xi_2(p_{t,2}), \cdots, \xi_l(p_{t,l})) = (\theta_1(a_1^t) + v\theta_1(b_1^t), \cdots, \theta_l(a_l^t) + v\theta_l(b_l^t))$ for $t = 0, \cdots, s-1$ and

$$\boldsymbol{S}_{\mathbb{M}^l} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \dots \\ \vdots & \vdots & \vdots & \ddots \\ \mathbf{1} & \mathbf{0} & \dots & \mathbf{0} \end{pmatrix} \in M_{s\times s}(\mathbb{M}^l)$$

where $\mathbf{1} = (1, \cdots, 1), \mathbf{0} = (0, \cdots, 0) \in \mathbb{M}^l$.

$$\begin{aligned} \Lambda_{\mathbb{M}^l} &: (\mathbb{M}^l)^s \longrightarrow \mathbb{M}^l[x, \Xi]/ < x^s - \mathbf{1} > \\ \mathbf{p} &= (\mathbf{p_0}, \cdots, \mathbf{p_{s-1}}) \longmapsto p(x) = \mathbf{p_0} + \mathbf{p_1}x + \cdots + \mathbf{p_{s-1}}x^{s-1} \end{aligned}$$

Let $\boldsymbol{C}_{\mathbb{M}^l}$ be a subset of $(\mathbb{M}^l)^s$. Then $\boldsymbol{C}_{\mathbb{M}^l}$ is a Ξ-cyclic code of length s over $\mathbb{M}^l$ if and only if $\Lambda_{\mathbb{M}^l}(\boldsymbol{C}_{\mathbb{M}^l})$ is a left $\mathbb{M}^l[x, \Xi]$-submodule of $\mathbb{M}^l[x, \Xi]/ < x^s - \mathbf{1} >$.

Theorem 4.1 *Let $\boldsymbol{C}_{\mathbb{M}^l} = (1-v)C_{1,\mathbb{F}_q^l} \oplus vC_{2,\mathbb{F}_q^l}$ be a linear code of length s over $\mathbb{M}^l$, where $C_{1,\mathbb{F}_q^l}, C_{2,\mathbb{F}_q^l}$ are linear codes of length s over $\mathbb{F}_q^l$. Then $\boldsymbol{C}_{\mathbb{M}^l}$ is a Ξ-cyclic code over $\mathbb{M}^l$ if and only if each $C_{1,\mathbb{F}_q^l}, C_{2,\mathbb{F}_q^l}$ are Θ-cyclic codes of length s over $\mathbb{F}_q^l$, where $\Xi = \xi_1 \times \cdots \times \xi_l \in \Omega_{\mathbb{M}^l}$, $\xi_i(a_i + vb_i) = \theta_i(a_i) + v\theta_i(b_i)$ for every $a_i + vb_i \in \mathbb{M}$, for $i = 1, \cdots, l$ and $\Theta = \theta_1 \times \cdots \times \theta_l \in \Omega_{\mathbb{F}_q^l}$, $\Theta(\mathbf{r}) = (\theta_1(r_1), \cdots, \theta_l(r_l))$ for every $\mathbf{r} = (r_1, \cdots, r_l) \in \mathbb{F}_q^l$.*

Proof Let $\boldsymbol{C}_{\mathbb{M}^l}$ be a Ξ-cyclic code over $\mathbb{M}^l$. Let $\boldsymbol{\Pi}_j(\mathbf{p}_0), \cdots, \boldsymbol{\Pi}_j(\mathbf{p}_{s-1})) \in C_{j,\mathbb{F}_q^l}$, for $j = 1, 2$ where $\mathbf{p} = (\mathbf{p}_0, \cdots, \mathbf{p}_{s-1}) \in \boldsymbol{C}_{\mathbb{M}^l}$. Let

$$\begin{aligned} \mathbf{p_t} &= (p_{t,1}, \cdots, p_{t,l}) = (a_1^t + vb_1^t, \cdots, a_l^t + vb_l^t), \\ \Xi(\mathbf{p_t}) &= (\xi_1(p_{t,1}), \xi_2(p_{t,2}), \cdots, \xi_l(p_{t,l})) = (\theta_1(a_1^t) + v\theta_1(b_1^t), \cdots, \theta_l(a_l^t) + v\theta_l(b_l^t)) \end{aligned}$$

for $t = 0, \cdots, s-1$. Since $\boldsymbol{C}_{\mathbb{M}^l}$ is a Ξ-cyclic code over $\mathbb{M}^l$, then

$$\begin{aligned} T_{\Xi,\boldsymbol{S}_{\mathbb{M}^l}}(\mathbf{p}) &= \Xi(\mathbf{p})\boldsymbol{S}_{\mathbb{M}^l} \\ &= (\mathbf{1}\Xi(\mathbf{p}_{s-1}), \Xi(\mathbf{p}_0), \cdots, \Xi(\mathbf{p}_{s-2})) = ((\theta_1(a_1^{s-1}) \\ &\quad + v\theta_1(b_1^{s-1}), \theta_2(a_2^{s-1}) + v\theta_2(b_2^{s-1}), \cdots, \theta_l(a_l^{s-1}) \\ &\quad + v\theta_l(b_l^{s-1})), (\theta_1(a_1^0) + v\theta_1(b_1^0), \theta_2(a_2^0) \\ &\quad + v\theta_2(b_2^0)), \cdots, \theta_l(a_l^0) + v\theta_l(b_l^0)), \cdots, (\theta_1(a_1^{s-2}) \\ &\quad + v\theta_1(b_1^{s-2}), \theta_2(a_2^{s-2}) + v\theta_2(b_2^{s-2}), \cdots, \theta_l(a_l^{s-2}) + v\theta_l(b_l^{s-2})) \\ &= ((\theta_1(a_1^{s-1}), \theta_2(a_2^{s-1}), \cdots, \theta_l(a_l^{s-1})) \\ &\quad + v(\theta_1(b_1^{s-1}), \theta_2(b_2^{s-1}), \cdots, \theta_l(b_l^{s-1})), (\theta_1(a_1^0), \theta_2(a_2^0), \cdots, \theta_l(a_l^0)) \\ &\quad + v(\theta_1(b_1^0), \theta_2(b_2^0), \cdots, \theta_l(b_l^0)), \cdots, (\theta_1(a_1^{s-2}), \theta_2(a_2^{s-2}), \cdots, \theta_l(a_l^{s-2})) \end{aligned}$$

$$
\begin{aligned}
& +v(\theta_1(b_1^{s-2}),\theta_2(b_2^{s-2}),\cdots,\theta_l(b_l^{s-2}))\\
= & ((\theta_1(a_1^{s-1}),\theta_2(a_2^{s-1}),\cdots,\theta_l(a_l^{s-1})),(\theta_1(a_1^0),\theta_2(a_2^0),\\
& \cdots,\theta_l(a_l^0)),\cdots,(\theta_1(a_1^{s-2}),\theta_2(a_2^{s-2}),\cdots,\theta_l(a_l^{s-2})))\\
& +v((\theta_1(b_1^{s-1}),\theta_2(b_2^{s-1}),\cdots,\theta_l(b_l^{s-1})),(\theta_1(b_1^0),\theta_2(b_2^0),\cdots,\theta_l(b_l^0)),\cdots,\\
& (\theta_1(b_1^{s-2}),\theta_2(b_2^{s-2}),\cdots,\theta_l(b_l^{s-2})))\\
= & (1-v)((\theta_1(a_1^{s-1}),\cdots,\theta_l(a_l^{s-1})),\cdots,(\theta_1(a_1^{s-2}),\cdots,\theta_l(a_l^{s-2}))\\
& +v((\theta_1(a_1^{s-1})+\theta_1(b_1^{s-1}),\cdots,\theta_l(a_l^{s-1})+\theta_1(b_1^{s-1})),\cdots,(\theta_1(a_1^{s-2})\\
& +\theta_1(b_1^{s-2}),\cdots,\theta_l(a_l^{s-2})+\theta_l(b_l^{s-2}))\in \boldsymbol{C}_{\mathbb{M}^l}.
\end{aligned}
$$

So for every $(\boldsymbol{\Pi_j}(\mathbf{p}_0),\cdots,\boldsymbol{\Pi_j}(\mathbf{p}_{s-1}))\in C_{j,\mathbb{F}_q^l}$, we have

$$(\Theta(\boldsymbol{\Pi_j}(\mathbf{p}_{s-1})),\Theta(\boldsymbol{\Pi_j}(\mathbf{p}_0)),\cdots,\Theta(\boldsymbol{\Pi_j}(\mathbf{p}_{s-2})))\in C_{j,\mathbb{F}_q^l}$$

for $j=1,2$. Therefore $C_{j,\mathbb{F}_q^l}$ are Θ-cyclic codes over $\mathbb{F}_q^l$, for $j=1,2$. The other way can be easily seen that. □

By using Theorem 4.10 in [1], we can obtain:

Corollary 4.2 *Let $\boldsymbol{C}_{\mathbb{M}^l}=(1-v)[\mathbf{e_1}C_{1,\mathbb{F}_q,1}\oplus\cdots\oplus\mathbf{e}_lC_{1,\mathbb{F}_q,l}]\oplus v[\mathbf{e_1}C_{2,\mathbb{F}_q,1}\oplus...\oplus\mathbf{e}_lC_{2,\mathbb{F}_q,l}]$ be a linear code of length s over $\mathbb{M}^l$. Then $\boldsymbol{C}_{\mathbb{M}^l}$ is a Ξ-cyclic code if and only if each $C_{j,\mathbb{F}_q,i}$ is a θ_i-cyclic code for $j=1,2$ and $i=1,\cdots,l$.*

Theorem 4.3 *Let $\boldsymbol{C}_{\mathbb{M}^l}=(1-v)C_{1,\mathbb{F}_q^l}\oplus vC_{2,\mathbb{F}_q^l}$ be a Ξ-cyclic code of length s over $\mathbb{M}^l$, where $C_{j,\mathbb{F}_q^l}$ is a linear code of length s over $\mathbb{F}_q^l$, for $j=1,2$. Then there exists $g_{j,i}(x)\in\mathbb{F}_q[x,\theta_i]$, for $j=1,2$ and $i=1,\cdots,l$ such that $\boldsymbol{C}_{\mathbb{M}^l}=<g(x)>=<(1-v)g_1(x)+vg_2(x)>$, where $g_j(x)=(g_{j,1}(x),g_{j,2}(x),\cdots,g_{j,l}(x))$, for $j=1,2$. Moreover $g(x)$ is a right divisor of $x^s-\mathbf{1}$ in $\mathbb{M}^l[x,\Xi]$.*

Proof It is easily seen from the proof of Theorem 4.11 in [1]. □

§5. Gray Map

We define the Gray map by

$$
\begin{aligned}
\boldsymbol{\Psi} \quad &:\quad (\mathbb{M}^l)^s\longrightarrow(\mathbb{F}_q^l)^{2s}\\
\mathbf{p}=(\mathbf{p}_0,\cdots,\mathbf{p}_{s-1}) \quad &\longmapsto\quad (\boldsymbol{\Pi}_1(\mathbf{p}_0),\cdots,\boldsymbol{\Pi}_1(\mathbf{p}_{s-1}),\boldsymbol{\Pi}_2(\mathbf{p}_0),\cdots,\boldsymbol{\Pi}_2(\mathbf{p}_{s-1}))
\end{aligned}
$$

where $\mathbf{p_t}=(a_1^t+vb_1^t,\cdots,a_l^t+vb_l^t)$, for $t=0,\cdots,s-1$ and

$$
\begin{aligned}
\Psi\quad :\quad & (\mathbb{F}_q^l)^{2s}\longrightarrow\mathbb{F}_q^{2sl}\\
& (\boldsymbol{\Pi}_1(\mathbf{p}_0),\cdots,\boldsymbol{\Pi}_1(\mathbf{p}_{s-1}),\boldsymbol{\Pi}_2(\mathbf{p}_0),\cdots,\boldsymbol{\Pi}_2(\mathbf{p}_{s-1}))\longmapsto o
\end{aligned}
$$

where $o=(\boldsymbol{\Pi}_1(\mathbf{p}_0)S,\cdots,\boldsymbol{\Pi}_1(\mathbf{p}_{s-1})S,\boldsymbol{\Pi}_2(\mathbf{p}_0)S,\cdots,\boldsymbol{\Pi}_2(\mathbf{p}_{s-1}S)$ and $S\in GL(l,\mathbb{F}_q)$.

The Gray weight of an element $\mathbf{p} \in (\mathbb{M}^l)^s$ is defined as

$$w_G(\mathbf{p}) = \sum_{t=0}^{s-1} \sum_{j=1}^{2} w_H(\mathbf{\Pi}_j(\mathbf{p}_t)S)$$

For any two distinct codewords $\mathbf{p}, \mathbf{p}' \in \boldsymbol{C}_{\mathbb{M}^l}$, the Gray distance is defined as $d_G(\mathbf{p}, \mathbf{p}') = w_G(\mathbf{p} - \mathbf{p}')$. The minimum Gray distance of the linear code $\boldsymbol{C}_{\mathbb{M}^l}$ over $\mathbb{M}^l$ denoted by $d_G(\boldsymbol{C}_{\mathbb{M}^l}) = d_G$ is equal to $min\{d_G(\mathbf{p}, \mathbf{p}') | \forall \mathbf{p}, \mathbf{p}' \in \boldsymbol{C}_{\mathbb{M}^l}, \mathbf{p} \neq \mathbf{p}'\}$.

Theorem 5.1 *The Gray map $\Psi \circ \mathbf{\Psi} = \Phi$ is a linear and distance preserving map from $(\mathbb{M}^l)^s$ (Gray Distance) to $\mathbb{F}_q^{2sl}$ (Hamming Distance).*

Theorem 5.2 *If $\boldsymbol{C}_{\mathbb{M}^l}$ is a linear code of length s over $\mathbb{M}^l$ with minimum Gray distance d_G and size M, then $\Phi(\boldsymbol{C}_{\mathbb{M}^l})$ is an $\mathbb{F}_q$ linear code with parameters $(2sl, M, d_H)$ with $d_G = d_H$.*

Theorem 5.3 *Let $\boldsymbol{C}_{\mathbb{M}^l}$ be a linear code of length s over $\mathbb{M}^l$. Then $\Phi(\boldsymbol{C}_{\mathbb{M}^l})$ is Euclidean dual containing if $\boldsymbol{C}_{\mathbb{M}^l}$ is Euclidean dual containing provided $S.S^{\mathbf{T}} = \lambda I_l$, where $S \in GL(l, \mathbb{F}_q)$, $\mathbf{T}$ denotes transpose of a matrix and $\lambda \in \mathbb{F}_q^*$.*

Proof Let $\mathbf{n} = (\mathbf{n}_0, \cdots, \mathbf{n}_{s-1}), f = (f_0, \cdots, f_{s-1}) \in \boldsymbol{C}_{\mathbb{M}^l}$, where

$$\mathbf{n_t} = (a_1^t + b_1^t v, \cdots, a_l^t + b_l^t v), \quad \mathbf{f_t} = (c_1^t + d_1^t v, \cdots, c_l^t + d_l^t v)$$

for $t = 0, \cdots, s-1$. Then

$$\langle \mathbf{n}, \mathbf{f} \rangle_E = \sum_{i=1}^{l} \sum_{t=0}^{s-1} a_i^t c_i^t + v \sum_{i=1}^{l} \sum_{t=0}^{s-1} a_i^t d_i^t + b_i^t c_i^t + b_i^t d_i^t.$$

Since $\langle \mathbf{n}, \mathbf{f} \rangle_E = 0$, then we have

$$\sum_{i=1}^{l} \sum_{t=0}^{s-1} a_i^t c_i^t = 0 \quad \text{and} \quad \sum_{i=1}^{l} \sum_{t=0}^{s-1} a_i^t d_i^t + b_i^t c_i^t + b_i^t d_i^t = 0.$$

Now

$$\langle \Phi(\mathbf{n}), \Phi(\mathbf{f}) \rangle_E = \sum_{t=0}^{s-1} \mathbf{\Pi}_1(\mathbf{n}_t) S S^{\mathbf{T}} (\mathbf{\Pi}_1(\mathbf{f}_t))^T + \sum_{t=0}^{s-1} \mathbf{\Pi}_2(\mathbf{n}_t) S S^{\mathbf{T}} (\mathbf{\Pi}_2(\mathbf{f}_t))^T,$$

where $S \in GL(l, \mathbb{F}_q)$. So

$$\lambda \sum_{i=1}^{l} \sum_{t=0}^{s-1} a_i^t c_i^t + \lambda \sum_{i=1}^{l} \sum_{t=0}^{s-1} a_i^t c_i^t + \lambda \sum_{i=1}^{l} \sum_{t=0}^{s-1} a_i^t d_i^t + b_i^t c_i^t + b_i^t d_i^t = 0$$

The desired result is obtained as the proof of Theorem 5.4 in [1]. □

Theorem 5.4([4]) *Let $C_{\mathbb{F}_q} =< g(x) >$ be a θ-cyclic code of length n over $\mathbb{F}_q$ such that n is* *a multiple of ord(θ) and $\theta \in Aut(\mathbb{F}_q)$. Then $C_{\mathbb{F}_q}$ contains its dual if and only if $h^*(x)h(x)$ is divisible by $x^n - 1$ on the right, where $x^n - 1 = h(x)g(x)$ and $h^*(x) = \beta_{n-1} + \theta(\beta_{n-s-1})x + ... + \theta^{n-s}(\beta_0)x^{n-s}$, for $h(x) = \beta_0 + \beta_1 x + ... + \beta_{n-1}x^{n-1}$.*

Theorem 5.5 *Let $\boldsymbol{C}_{\mathbb{M}^l} = (1-v)[\mathbf{e_1}C_{1,\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{1,\mathbb{F}_q,l}] \oplus v[\mathbf{e_1}C_{2,\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{2,\mathbb{F}_q,l}]$ be a Ξ-cyclic code of length s over $\mathbb{M}^l$ such that s is a multiple of $ord(\Xi) = lcm[ord(\xi_1), \cdots, ord(\xi_l)]$ and $\Xi \in \Omega_{\mathbb{M}^l}$. Let $C_{j,\mathbb{F}_q,i} =< g_{j,i}(x) >$ and $x^s - 1 = h_{j,i}(x)g_{j,i}(x) = g_{j,i}(x)h_{j,i}(x)$, for $h_{j,i}(x), g_{j,i}(x) \in \mathbb{F}_q[x, \theta_i]$. Then $\boldsymbol{C}^{\perp}_{\mathbb{M}^l} \subseteq \boldsymbol{C}_{\mathbb{M}^l}$ if and only if $h^*_{j,i}(x)h_{j,i}(x)$ is divisible by $x^s - 1$, for $j = 1, 2$ and $i = 1, \cdots, l$.*

Corollary 5.6 *Let $\boldsymbol{C}_{\mathbb{M}^l} = (1-v)[\mathbf{e_1}C_{1,\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{1,\mathbb{F}_q,l}] \oplus v[\mathbf{e_1}C_{2,\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{2,\mathbb{F}_q,l}]$ be a Ξ-cyclic code of length s over $\mathbb{M}^l$ such that s is a multiple of $lcm[ord(\xi_1), \cdots, ord(\xi_l)]$ and $\Xi \in \Omega_{\mathbb{M}^l}$. Then $\boldsymbol{C}^{\perp}_{\mathbb{M}^l} \subseteq \boldsymbol{C}_{\mathbb{M}^l}$ if and only if $C^{\perp}_{j,\mathbb{F}_q,i} \subseteq C_{j,\mathbb{F}_q,i}$, for $j = 1, 2$ and $i = 1, \cdots, l$.*

Theorem 5.7(CSS Construction, [2]) *Let C_1 and C_2 be $[n, k_1, d_1]$ and $[n, k_2, d_2]$ linear codes over $\mathbb{F}_q$ respectively with $C_2^{\perp} \subset C_1$. Futhermore, let $d = \{d_1, d_2\}$. Then there exists a QECC, with parameters $[[n, k_1 + k_2 - n, d]]_q$. In particular, if $C_1^{\perp} \subseteq C_1$, then there exists a QECC with parameters $[[n, 2k_1 - n, d]]_q$.*

Theorem 5.8 *Let $\boldsymbol{C}_{\mathbb{M}^l} = (1-v)[\mathbf{e_1}C_{1,\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{1,\mathbb{F}_q,l}] \oplus v[\mathbf{e_1}C_{2,\mathbb{F}_q,1} \oplus \cdots \oplus \mathbf{e}_l C_{2,\mathbb{F}_q,l}]$ be a Ξ-cyclic code of length s over $\mathbb{M}^l$ such that s is a multiple of $lcm[ord(\xi_1), \cdots, ord(\xi_l)]$. If $C^{\perp}_{j,\mathbb{F}_q,i} \subseteq C_{j,\mathbb{F}_q,i}$, for $j = 1, 2$ and $i = 1, \cdots, l$, then $\boldsymbol{C}^{\perp}_{\mathbb{M}^l} \subseteq \boldsymbol{C}_{\mathbb{M}^l}$ and there exists a quantum error correcting code with parameters $[[(2sl, \sum_{i=1}^{l}\sum_{j=1}^{2} k_{j,i} - 2sl, d_H]]_q$, where d_H denotes the Hamming distance of the code $\Phi(\boldsymbol{C}_{\mathbb{M}^l})$ and $k_{j,i} = s-deg\ g_{j,i}(x)$, for $i = 1, \cdots, l$ and $j = 1, 2$.*

Example 5.9 Let $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ be the field of order 8, where $\alpha^3 = \alpha + 1$. Let $l = 2, s = 6$ and $\Theta = \theta \times \theta^2 \in \Omega_{\mathbb{F}_8^2}$, where θ is the Frobenius automorphism of $\mathbb{F}_8$. If

$$\begin{aligned} C_{1,\mathbb{F}_8,i} &= \left\langle g_{1,i}(x) = \left(\alpha + \alpha^2\right)(1+x) + \alpha\left(x^2 + x^3\right)\right\rangle, \\ C_{2,\mathbb{F}_8,i} &= \left\langle g_{2,i}(x) = \left(1 + \alpha^2\right)(1+x) + \left(\alpha + \alpha^2\right)\left(x^2 + x^3\right)\right\rangle \end{aligned}$$

for $i = 1, 2$, then $C_{1,\mathbb{F}_8^2}, C_{2,\mathbb{F}_8^2}$ are Θ-cyclic codes of length 6 over $\mathbb{F}_8^2$. So, $\boldsymbol{C}_{\mathbb{M}^2}$ is an Ξ-cyclic codes of length 6 over $\mathbb{M}^2$. Moreover, we have

$$\begin{aligned} h_{1,i}(x) &= (1+\alpha)\left(1+x^2\right) + \left(\alpha^2+1\right)\left(x+x^3\right) \\ h^*_{1,i}(x) &= \left(1+\alpha^2\right)(1+x) + (1+\alpha)\left(x^2+x^3\right) \\ h_{2,i}(x) &= \alpha + \left(\alpha+\alpha^2\right)x + \left(1+\alpha^2\right)x^2 + (1+\alpha)x^3 \\ h^*_{2,i}(x) &= (1+\alpha)(1+x) + \alpha\left(x^2+x^3\right) \end{aligned}$$

for $i = 1, 2$. So $x^6 - 1$ is divisible by $g_{j,i}(x)\, h^*_{j,i}(x)$ for $i = 1, 2, j = 1, 2$. Then $\boldsymbol{C}^{\perp}_{\mathbb{M}^2} \subseteq \boldsymbol{C}_{\mathbb{M}^2}$. If

$$S = \begin{pmatrix} 1 & 1+\alpha+\alpha^2 \\ 1+\alpha+\alpha^2 & 1 \end{pmatrix}$$

then $\Psi(C_{i,\mathbb{F}_8^2})$ is a $[12,6,6]$ linear code over $\mathbb{F}_8$ for $i=1,2$. Hence $\Phi(\boldsymbol{C}_{\mathbb{M}^2})$ is a $[24,12,6]$ linear code over $\mathbb{F}_8$. Hence, by Theorem 11, we have a quantum code with $[[24,0,6]]$.

§6. Conclusion

We take a more general form of an automorphism of $\mathbb{M}^l$, namely $\xi_1 \times \xi_2 \cdots \times \xi_l$, where each ξ_i is an automorphism of $\mathbb{M}$, for $i=1,\cdots,l$. We introduce the algebraic structure of Ξ-cyclic codes over $\mathbb{M}^l$ and obtain the parameters of quantum codes from Ξ-cyclic codes over $\mathbb{M}^l$, $l \geq 1$, by using CSS constructions.

References

[1] Bhagat, Anuj Kumar and Ritumoni Sarma, $(\Theta, \Delta_\Theta, \mathbf{a})$-cyclic codes over $\mathbb{F}_q^l$ and their applications in the construction of quantum codes, *arXiv* e-prints (2025): arXiv-2501.

[2] Calderbank A.R., E.M. Rains, P.M. Shor, N.J. Sloane, Quantum error correction via codes over $GF(4)$", *IEEE Trans.Inf.Theory*, Vol.44, no 4, pp 1369-1387, July 1998.

[3] Dinh, Hai Q., et al., On a class of skew constacyclic codes over mixed alphabets and applications in constructing optimal and quantum codes, *Cryptography and Communications*, 15.1 (2023): pp 171-198.

[4] Dinh, Hai Q. et al., A class of skew cyclic codes and application in quantum codes construction, *Discrete Mathematics* 344.2 (2021): 112189.

[5] Gursoy, Fatmanur, Irfan Siap and Bahattin Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, *Advances in Mathematics of Communications*, 8.3 (2014): pp 313-322.

[6] Lidl Rudolf and Harald Niederreiter, *Finite Fields*, No. 20. Cambridge University Press, 1997.

[7] Shor Peter W, Scheme for reducing decoherence in quantum computer memory, *Physical Review* A 52.4 (1995): R2493.

[8] Steane Andrew M., Simple quantum error-correcting codes, *Physical Review* A 54.6 (1996): 4741.