*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 1, pp. 189–201
DOI : 10.47974/JDMSC-1730

# Algebraic structure of cyclic codes over $M_3(\mathbb{F}_p)$

Habibul Islam †
Om Prakash *
Dipak Kumar Bhunia §
*Department of Mathematics*
*Indian Institute of Technology Patna*
*Patna 801106*
*Bihar*
*India*

**Abstract**

Let $\mathbb{F}_p$ be the finite field of order $p$ and $M_3(\mathbb{F}_p)$, the ring of $3\times 3$ matrices over $\mathbb{F}_p$, where $p$ is a prime. For certain prime $p$, we determine the complete algebraic properties of cyclic codes of length $N$ $(p \nmid N)$ over $M_3(\mathbb{F}_p)$. We define an isometry from $M_3(\mathbb{F}_p)$ to $\mathbb{F}_{p^3} + e\mathbb{F}_{p^3} + e^2\mathbb{F}_{p^3}$, where $e^3 = 1$. As an outcome, we derive numerous optimal and good linear $\mathbb{F}_8$ codes induced from $\mathbb{F}_8$ -images of cyclic codes over $M_3(\mathbb{F}_2)$.

***Subject Classification:*** *(2010) 94B05, 94B15, 94B35, 94B60.*

***Keywords:*** *Matrix ring, Linear code, Cyclic code, Gray map, Optimal code.*

## 1. Introduction

Cyclic codes over finite rings have been at the centre of attraction among researchers since 1994 [9]. They have a rich algebraic structure and, consequently, produce a huge amount of good linear codes. Initially, cyclic codes were considered over finite commutative as well as noncommutative rings. To discover new codes, cyclic codes over finite commutative rings are investigated in [7, 10–12, 14–17, 19, 22, 24, 25, 29]. Till now, a few papers [1, 3, 5, 8, 13, 18, 20, 21, 23] have come into the literature that presented the study of these codes over noncommutative rings, namely, matrix rings.

† *E-mail:* habibul.pma17@iitp.ac.in
* *E-mail:* om@iitp.ac.in (Corresponding Author)
§ *E-mail:* dipak.mtmc17@iitp.ac.in

Like skew polynomial rings, matrix rings also produce new and good linear codes. Towards this, Alahmadi et al. [1] obtained cyclic codes structure over $M_2(\mathbb{F}_2)$ about Euclidean self-dual cyclic codes and obtained many self-dual $\mathbb{F}_4$-codes. Also, Falcunit & Sison [5] studied algebraic properties of cyclic codes over a more general ring $M_2(\mathbb{F}_p)$, where $p \equiv 2$ or $3 \pmod 5$ in 2014. Further, in 2018, Luo & Udaya [18] studied cyclic codes over the matrix ring $M_2(\mathbb{F}_2[u]/\langle u^2\rangle)$. They have obtained many quaternary optimal codes by using an isometry between $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ and $\mathbb{F}_4[u,v]/\langle u^2, v^2, uv - vu\rangle$. Again, Pal et al. [21] explored cyclic codes over $M_4(\mathbb{F}_2)$, and Bhowmick et al. [3] considered self-dual cyclic codes over $M_2(\mathbb{Z}_4)$. Recently, in [13], we extended the concept of [18] to $M_2(\mathbb{F}_p + u\mathbb{F}_p)$ for $p = 2$ or $3 \pmod 5$, and obtained the structure of cyclic codes.

It is still open to obtain self-dual and cyclic codes over another important matrix ring $M_3(\mathbb{F}_p)$, where $p$ is a prime. In other words, it is logical to explore whether cyclic codes over $M_3(\mathbb{F}_p)$ are capable of producing good linear and optimal codes over $\mathbb{F}_{p^3}$. Here, the answer is affirmative, and this paper justifies the possibility. For certain prime $p$, we consider the ring $M_3(\mathbb{F}_p)$ of $3 \times 3$ matrices over $\mathbb{F}_p$ and define an isometry from $M_3(\mathbb{F}_p)$ to $\mathbb{F}_{p^3} + e\mathbb{F}_{p^3} + e^2\mathbb{F}_{p^3}$, where $e^3 = 1$, in order to analyze cyclic codes over $M_3(\mathbb{F}_p)$. Finally, we give many optimal linear codes induced from $\mathbb{F}_p$-images of these codes. The major contribution includes the derivation of algebraic properties of cyclic codes over $M_3(\mathbb{F}_p)$, which has enough potential of producing optimal linear $p$-ary codes.

## 2. Preliminaries

For a prime $p$, let $\mathbb{F}_p$ be the finite field of $p$ elements, and $f(x) \in \mathbb{F}_p[x]$, an irreducible polynomial of degree 3. For example, $f(x) = x^3 - x - 1$ has no roots in $\mathbb{F}_p$ and hence irreducible in $\mathbb{F}_p[x]$ for $p \in \{2, 3, 13, 29, 31, 41, 47, 71, 73\}$ $(p \le 100)$. Now, $\mathbb{F}_{p^3} = \mathbb{F}_p[\omega]$ is a Galois field where $f(\omega) = 0$. The Galois group $G = \mathrm{Gal}(\mathbb{F}_{p^3}/\mathbb{F}_p)$ is cyclic generated by the Frobenius automorphism $\sigma : \mathbb{F}_{p^3} \to \mathbb{F}_{p^3}$ defined by $\sigma(a) = a^p$. By using the technique of [20], we construct a cyclic algebra $\mathbb{A} = (\mathbb{F}_{p^3}/\mathbb{F}_p, \sigma, 1)$ as follows: $\mathbb{A}$ contains $\mathbb{F}_{p^3}$ and has a right $\mathbb{F}_{p^3}$-basis containing $1, e, e^2$ such that $\mathbb{A} = \mathbb{F}_{p^3} + e\mathbb{F}_{p^3} + e^2\mathbb{F}_{p^3}$, where $ae = e\sigma(a)$ and $e^3 = 1$ for all $a \in \mathbb{F}_{p^3}$. Note that $\mathbb{A}$ is a central simple algebra with $\dim \mathbb{A} = 9$. Therefore, $\mathbb{A} \cong M_3(\mathbb{F}_p)$, that is, $M_3(\mathbb{F}_p) \cong \mathbb{F}_{p^3} + e\mathbb{F}_{p^3} + e^2\mathbb{F}_{p^3}$ with $e^3 = 1$, where $M_3(\mathbb{F}_p)$ is the ring of $3 \times 3$ matrices over $\mathbb{F}_p$.

Here, $\mathfrak{R}$ represents the ring $M_3(\mathbb{F}_p) \cong \mathbb{F}_{p^3} + e\mathbb{F}_{p^3} + e^2\mathbb{F}_{p^3}$, which is a noncommutative ring (with unity) of size $p^9$. An element $\tilde{s} \in \mathfrak{R}$ can be

expressed as $\tilde{s} = \tilde{a}_1 + e\tilde{a}_2 + e^2\tilde{a}_3$, where $\tilde{a}_1, \tilde{a}_2, \tilde{a}_3 \in \mathbb{F}_{p^3}$. Recall that $\{0\} \neq \mathcal{C} \subseteq \mathfrak{R}^N$ is said to be *linear* if $\mathcal{C}$ is an $\mathfrak{R}$-submodule of $\mathfrak{R}^N$. Vectors of $\mathcal{C}$ are called *codewords*. Further, $\mathcal{C}$ is said to be *cyclic* if $(\tilde{s}_{N-1}, \tilde{s}_0, \ldots, \tilde{s}_{N-2}) \in \mathcal{C}$ whenever $(\tilde{s}_0, \tilde{s}_1, \ldots, \tilde{s}_{N-1}) \in \mathcal{C}$. We define a Gray map $\Pi : \mathfrak{R} \to \mathbb{F}_{p^3}^3$ by

$$\Pi(\tilde{a}_1 + e\tilde{a}_2 + e^2\tilde{a}_3) = (\tilde{a}_3, \tilde{a}_3 + \tilde{a}_2, \tilde{a}_1 + \tilde{a}_2 + \tilde{a}_3),$$

where $\tilde{a}_1, \tilde{a}_2, \tilde{a}_3 \in \mathbb{F}_{p^3}$. The mapping $\Pi$ is linear bijective and its extension $\Pi : \mathfrak{R}^N \to \mathbb{F}_{p^3}^{3N}$ is defined by

$$\begin{aligned}&\Pi(\tilde{s}_0, \ldots, \tilde{s}_{N-1})\\ &= (\tilde{c}_0, \ldots, \tilde{c}_{N-1}, \tilde{c}_0 + \tilde{b}_0, \ldots, \tilde{c}_{N-1} + \tilde{b}_{N-1}, \tilde{a}_0 + \tilde{b}_0 + \tilde{c}_0, \ldots, \tilde{a}_{N-1} + \tilde{b}_{N-1} + \tilde{c}_{N-1}),\end{aligned}$$

where $\tilde{s}_i = \tilde{a}_i + e\tilde{b}_i + e^2\tilde{c}_i \in \mathfrak{R}$ with $0 \leq i \leq N-1$. The Gray weight $wt_G$ of $\tilde{s} = \tilde{a} + e\tilde{b} + e^2\tilde{c} \in \mathfrak{R}$ is define by

$$wt_G(\tilde{s}) = wt_H(\tilde{c}) + wt_H(\tilde{c} + \tilde{b}) + wt_H(\tilde{a} + \tilde{b} + \tilde{c}),$$

where the Hamming weight is denoted $wt_H$ in $\mathbb{F}_{p^3}$. Recall that for a vector $\vec{v}$ in $\mathbb{F}_{p^3}^N$, $wt_H(\vec{v}) = |\{i : v_i \neq 0 \ \forall\, i\}|$. Also, the Gray weight $\vec{s} = (\tilde{s}_0, \ldots, \tilde{s}_{N-1}) \in \mathfrak{R}^N$ is define as $wt_G(\vec{\mathbf{s}}) = \sum_{j=0}^{N-1} wt_G(\tilde{s}_j)$, while the Gray distance, $d_G(\mathcal{C}) = \min\{wt_G(\vec{c}) : \vec{c} \in \mathcal{C} \setminus \{0\}\}$. Thus, we have that $\Pi$ is an isometry from $(R^N, d_G(\mathcal{C}))$ to $(\mathbb{F}_{p^3}^{3N}, d_H(\mathcal{C}))$.

**Definition 2.1:** [11] Assume $N = \alpha\beta$, where $\alpha, \beta \geq 1$ are integers. Based on a cyclic shift operator $\gamma$, another operator $\pi_\alpha$, called quasi-cyclic shift, is defined by

$$\pi_\alpha(\vec{a}^1 | \ldots | \vec{a}^\alpha) = (\gamma(\vec{a}^1) | \ldots | \gamma(\vec{a}^\alpha)),$$

where $\vec{a}^i \in \mathfrak{R}^\beta$ for $i = 1, \ldots, \alpha$. If $\pi_\alpha(\mathcal{C}) = \mathcal{C}$, the code $\mathcal{C}$ is said to be quasi-cyclic of length $N$ and index $\alpha$ over $\mathfrak{R}$.

In the light of map $\Pi$ and Definition 2.1, we determine quasi-cyclic codes over $\mathbb{F}_{p^3}$ based on Gray images of cyclic codes over $\mathfrak{R}$.

**Theorem 2.2:** *Let $\mathcal{C} \subseteq \mathfrak{R}^N$ be a linear code. Then, $\mathcal{C}$ is cyclic if and only if $\Pi(\mathcal{C}) \subseteq \mathbb{F}_{p^3}^{3N}$ is quasi-cyclic with index* 3.

***Proof:*** It is verified analogous to [10, Theorem 4].

## 3. Cyclic codes over $\mathfrak{R}$

This section aims to explore cyclic codes (Theorem 3.3 to Proposition 3.6), and their properties that are used to get some optimal linear codes in the next section. For computation purposes, we restrict ourselves to cyclic codes of length $N$ satisfying $\gcd(N,p)=1$, that is, $p \nmid N$. We define a map $\tau : \mathfrak{R}[x] \to \mathbb{F}_{p^3}[x]$ by

$$\tau\left(\sum_{i=0}^{N} \tilde{s}_i x^i\right) = \sum_{i=0}^{N} \overline{\tau}(\tilde{s}_i) x^i,$$

where $\overline{\tau}(\tilde{s})$ is the polynomial reduction of $\tilde{s}$ modulo $e$. A monic polynomial $f(x) \in \mathfrak{R}[x]$ is defined to a basic irreducible polynomial, if $\tau(f(x)) \in \mathbb{F}_{p^3}[x]$ is irreducible. The next two results (Lemma 3.1 and Lemma 3.2) help to obtain cyclic codes over $\mathfrak{R}$.

**Lemma 3.1:** *For $p \nmid N$, let $x^N - 1 = \prod_{s=1}^{m} f_s$, where $\gcd(f_i, f_j) = 1$ for $i \neq j$ and $f_i$'s are irreducible polynomials in $\mathbb{F}_{p^3}[x]$. Then,*

$$\frac{\mathfrak{R}[x]}{\langle x^N - 1\rangle} = \bigoplus_{s=1}^{m} \frac{\mathfrak{R}[x]}{\langle f_s\rangle} = \bigoplus_{s=1}^{m} \mathfrak{R}_{f_s},$$

*where $\mathfrak{R}_{f_s} = \frac{\mathfrak{R}[x]}{\langle f_s\rangle}$ is right $\mathfrak{R}$-module for $1 \le s \le m$.*

***Proof:*** It is straightforward by applying the Chinese Remainder Theorem on the right $\mathfrak{R}$-module $\mathfrak{R}[x]/\langle x^N - 1\rangle$ (see [20, 28]).

**Lemma 3.2:** *Consider an irreducible polynomial $f \in \mathbb{F}_{p^3}[x]$. Then, $\langle 0\rangle, \langle 1\rangle, \langle e\rangle, \langle e^2\rangle$ and $\langle e + e^2 h_f\rangle$, constitute the complete set of right $\mathfrak{R}$-submodules of $\mathfrak{R}_f = \frac{\mathfrak{R}[x]}{\langle f\rangle}$, where $h_f$ is a unit in $\mathbb{F}_{p^3}[x]$.*

***Proof:*** Let $I$ be a non-trivial right $\mathfrak{R}$-submodule of $\mathfrak{R}_f = \frac{\mathfrak{R}[x]}{\langle f\rangle}$ and $g \in I$. Then, we have that $g \notin \langle f\rangle$. Let $g + \langle f\rangle = \tilde{g}_1 + e\tilde{g}_2 + e^2\tilde{g}_3 + \langle f\rangle$, where $\tilde{g}_i \in \mathbb{F}_{p^3}[x]$ with $1 \le i \le 3$.

**Case A:** Let $\gcd(f, \tau(g)) = 1$, that is, $\gcd(f, \tilde{g}_1) = 1$. Then, $\tilde{g}_1$ is invertible in $\mathbb{F}_{p^3}[x]/\langle f\rangle$ and $g$ is invertible in $\mathfrak{R}_f$. Hence, $I = \langle g\rangle = \langle 1\rangle = \mathfrak{R}_f$.

**Case B:** Let $\gcd(f, \tilde{g}_1) = f$. Then,

$$g + \langle f\rangle = e\tilde{g}_2 + e^2\tilde{g}_3 + \langle f\rangle. \tag{1}$$

Thus, $I \subseteq \langle e \rangle$. Now, we consider the following two sub-cases:

(1) Let $\gcd(f, \tilde{g}_2) = f$. Then, by equation (1), we have

$$g + \langle f \rangle = e^2 \tilde{g}_3 + \langle f \rangle. \tag{2}$$

Therefore, $I \subseteq \langle e^2 \rangle$. Also, $g$ is non-zero in $I$, $\gcd(f, \tilde{g}_3) = 1$. Hence, $\tilde{g}_3^{-1}$ exists in $\mathbb{F}_{p^3}[x]/\langle f \rangle$. Now, by equation (2), $e^2 + \langle f \rangle = g\tilde{g}_3^{-1} + \langle f \rangle \in I$. Thus, $\langle e^2 \rangle \subseteq I$ and $I = \langle e^2 \rangle$.

(2) Let $\gcd(f, \tilde{g}_2) = 1$. Then $\tilde{g}_2^{-1}$ exists in $\mathbb{F}_{p^3}[x]/\langle f \rangle$. Again, we have two choices as below:

(a) If $\gcd(f, \tilde{g}_3) = f$, then from equation (1), we have

$$g + \langle f \rangle = e\tilde{g}_2 + \langle f \rangle, \text{ this implies that}$$
$$e + \langle f \rangle = g\tilde{g}_2^{-1} + \langle f \rangle \in I.$$

Therefore, $\langle e \rangle \subseteq I$. Hence, $I = \langle e \rangle$.

(b) If $\gcd(f, \tilde{g}_3) = 1$, then $\tilde{g}_3^{-1}$ exists in $\mathbb{F}_{p^3}[x]/\langle f \rangle$. From equation (1), we have

$$g + \langle f \rangle = e\tilde{g}_2 + e^2\tilde{g}_3 + \langle f \rangle,$$
$$\text{that is,} \quad e + e^2\tilde{g}_3\tilde{g}_2^{-1} + \langle f \rangle = e + e^2 h_f + \langle f \rangle = g\tilde{g}_2^{-1} + \langle f \rangle \in I,$$

with a unit $h_f = \tilde{g}_3\tilde{g}_2^{-1}$ in $\mathbb{F}_{p^3}[x]$. Now, we have either $\langle e + e^2 h_f \rangle = I$ or $\langle e + e^2 h_f \rangle \subset I$. If $\langle e + e^2 h_f \rangle \subset I$, we have $e + e^2 h_{f'} \in I$ such that $e + e^2 h_{f'} \notin \langle e + e^2 h_f \rangle$, with a unit $h_{f'}$ in $\mathbb{F}_{p^3}[x]$. Thus, we have that $e^2(h_f - h_{f'}) \in I$ with $h_f \neq h_{f'}$, and hence $e^2 \in I$. Again, by equation (1),

$$e\tilde{g}_2 + \langle f \rangle = g - e^2\tilde{g}_3 + \langle f \rangle \in I,$$
$$\text{this implies that} \quad e + \langle f \rangle = (g - e^2\tilde{g}_3)\tilde{g}_2^{-1} + \langle f \rangle \in I.$$

Therefore, $\langle e \rangle \subseteq I$. Hence, $I = \langle e \rangle$.

Taking into account all the factors discussed above, we reach to the conclusion that all possible $\mathfrak{R}$-submodules of $\mathfrak{R}_f = \mathfrak{R}[x]/\langle f \rangle$ are $\langle 0 \rangle, \langle 1 \rangle, \langle e \rangle, \langle e^2 \rangle$ and $\langle e + e^2 h_f \rangle$, with a unit $h_f$ in $\mathbb{F}_{p^3}[x]$.

Now, by using Lemma 3.1 and Lemma 3.2, we prepare Theorem 3.3 which gives all right $\mathfrak{R}$-submodules (cyclic codes) of $\frac{\mathfrak{R}[x]}{\langle x^N - 1 \rangle}$.

**Theorem 3.3:** *Assume* $x^N-1=\prod_{s=1}^{m} f_s$, *with* $\gcd(f_i,f_j)=1$ *for* $i\neq j$ *and* $f_i$*'s are irreducible polynomials in* $\mathbb{F}_{p^3}[x]$. *Denote* $\hat{f}_s=\frac{x^N-1}{f_s}$, *for* $1\leq s\leq m$. *Then, any right* $\mathfrak{R}$*-submodule of* $\mathfrak{R}[x]/\langle x^N-1\rangle$ *is the sum of the right* $\mathfrak{R}$*-submodules* $\langle \hat{f}_s+\langle x^N-1\rangle\rangle$, $\langle e\hat{f}_s+\langle x^N-1\rangle\rangle$, $\langle e^2\hat{f}_s+\langle x^N-1\rangle\rangle$, *and* $\langle (e+e^2h_f)\,\hat{f}_s+\langle x^N-1\rangle\rangle$, *for* $1\leq s\leq m$ *and a unit* $h_f$ *in* $\mathbb{F}_{p^3}[x]$.

***Proof:*** Using the fact given by Lemma 3.1 & Lemma 3.2, it is verified.

**Theorem 3.4:** *Let* $\mathcal{C}\subseteq\mathfrak{R}^N$ *be a cyclic code. Then*

$$\mathcal{C}=\langle \hat{F}_1\rangle\oplus\langle e\hat{F}_2\rangle\oplus\langle e^2\hat{F}_3\rangle\oplus\langle (e+e^2h_f)\hat{F}_4\rangle$$

*and* $|\mathcal{C}|=p^{9\sum_{i=1}^{4}\deg F_i}$, *for a unit* $h_f$ *in* $\mathbb{F}_{p^3}[x]$ *and* $\gcd(F_i,F_j)=1$ *for* $i\neq j$, *monic polynomials* $F_i$*'s in* $\mathbb{F}_{p^3}[x]$ *satisfying* $x^N-1=\prod_{s=0}^{4} F_s$ *with* $\hat{F}_s=\frac{x^N-1}{F_s}$ *and* $0\leq s\leq 4$.

***Proof:*** First, assume that $x^N-1=\prod_{s=1}^{m} f_s$, with $\gcd(f_i,f_j)=1$ for $i\neq j$ and $f_i$*'s* are irreducible polynomials in $\mathbb{F}_{p^3}[x]$. Now, let $\mathcal{C}\subseteq\mathfrak{R}^N$ be cyclic. By Theorem 3.3, $\mathcal{C}$ can be formed by the addition of the right $\mathfrak{R}$-submodules $\langle \hat{f}_s+\langle x^N-1\rangle\rangle$, $\langle e\hat{f}_s+\langle x^N-1\rangle\rangle$, $\langle e^2\hat{f}_s+\langle x^N-1\rangle\rangle$, and $\langle (e+e^2h_f)\,\hat{f}_s+\langle x^N-1\rangle\rangle$, $1\leq s\leq m$. We consider (without loss of generality)

$$\begin{aligned}\mathcal{C}=&\langle \hat{f}_{k_1+1}\rangle\oplus\cdots\oplus\langle \hat{f}_{k_1+k_2}\rangle\oplus\langle e\hat{f}_{k_1+k_2+1}\rangle\oplus\cdots\oplus\langle e\hat{f}_{k_1+k_2+k_3}\rangle\\&\oplus\langle e^2\hat{f}_{k_1+k_2+k_3+1}\rangle\oplus\cdots\oplus\langle e^2\hat{f}_{k_1+k_2+k_3+k_4}\rangle\oplus\langle (e+e^2h_f)\\&\hat{f}_{k_1+k_2+k_3+k_4+1}\rangle\oplus\cdots\oplus\langle (e+e^2h_f)\hat{f}_{k_1+k_2+k_3+k_4+k_5}\rangle,\end{aligned}$$

where $k_i\geq 0$ for $1\leq i\leq 5$ and $\sum_{i=1}^{4}k_i+1\leq m$. Take $k_0=0$ and $k_1+k_2+k_3+k_4+k_5=m$. Also, let

$$\begin{aligned}&F_0=f_{k_0+1}\cdots f_{k_0+k_1};\ F_1=f_{k_1+1}\cdots f_{k_1+k_2};\\&F_2=f_{k_1+k_2+1}\cdots f_{k_1+k_2+k_3};\ F_3=f_{k_1+k_2+k_3+1}\cdots f_{k_1+k_2+k_3+k_4};\\&F_4=f_{k_1+k_2+k_3+k_4+1}\cdots f_{k_1+k_2+k_3+k_4+k_5}.\end{aligned}$$

It is easy to see that $F_0,\ldots,F_4$ are pairwise coprime, monic polynomials satisfying $x^N-1=\prod_{s=0}^{4}F_s$ and $\mathcal{C}=\langle \hat{F}_1\rangle\oplus\langle e\hat{F}_2\rangle\oplus\langle e^2\hat{F}_3\rangle\oplus\langle (e+e^2h_f)\hat{F}_4\rangle$.

Also, $|\langle \hat{F}_1\rangle| = p^{9\deg F_1}, |\langle e\hat{F}_2\rangle| = p^{9\deg F_2}, |\langle e^2\hat{F}_3\rangle| = p^{9\deg F_3}$, and $|\langle (e+e^2h_f)\hat{F}_4\rangle| = p^{9\deg F_4}$. Thus, $|\mathcal{C}| = |\langle \hat{F}_1\rangle| \cdot |\langle e\hat{F}_2\rangle| \cdot |\langle e^2\hat{F}_3\rangle| \cdot |\langle (e+e^2h_f)\hat{F}_4\rangle| = p^{9\sum_{i=1}^{4}\deg F_i}$.

**Proposition 3.5:** *Let $\mathcal{C} \subseteq \mathfrak{R}^N$ be a cyclic code. Then, there exist factors F, G of $x^N - 1$ in $\mathbb{F}_{p^3}[x]$ satisfying $\mathcal{C} = \langle F\rangle_I \oplus e\langle F\rangle_I \oplus e^2\langle F\rangle_I \oplus (e+e^2h_f)\langle G\rangle_I$ and $|\mathcal{C}| = p^{6N-3\deg F-3\deg G}$, where $\langle F\rangle_I$ is an ideal generated by F in $I = \mathbb{F}_{p^3}[x]/\langle x^N-1\rangle$ and $\langle x^N-1\rangle$ is an ideal of $\mathbb{F}_{p^3}[x]$.*

***Proof:*** Let $\mathcal{C} \subseteq \mathfrak{R}^N$ be cyclic. Then by Theorem 3.4 we have $\mathcal{C} = \langle \hat{F}_1\rangle \oplus \langle e\hat{F}_2\rangle \oplus \langle e^2\hat{F}_3\rangle \oplus \langle (e+e^2h_f)\hat{F}_4\rangle$, with $\gcd(F_i, F_j) = 1$ for $i \neq j$ and monic polynomials $F_i$s in $\mathbb{F}_{p^3}[x]$ satisfying $x^N - 1 = \prod_{s=0}^{4} F_s$ with $\hat{F}_s = \frac{x^N-1}{F_s}$ and a unit $h_f$ in $\mathbb{F}_{p^3}[x]$. Further, we know $\langle \hat{F}_s\rangle = \langle \hat{F}_s\rangle_I + e\langle \hat{F}_s\rangle_I + e^2\langle \hat{F}_s\rangle_I$ for $1 \le s \le 4$. Therefore,

$$\begin{aligned}\mathcal{C} &= \langle \hat{F}_1\rangle_I + e\langle \hat{F}_1\rangle_I + e^2\langle \hat{F}_1\rangle_I + e\langle \hat{F}_2\rangle_I + e^2\langle \hat{F}_2\rangle_I + \langle \hat{F}_2\rangle_I + e^2\langle \hat{F}_3\rangle_I + \langle \hat{F}_3\rangle_I + \\ &\quad e\langle \hat{F}_3\rangle_I + (e+e^2h_f)\langle \hat{F}_4\rangle_I + \langle \hat{F}_4\rangle_I + e\langle \hat{F}_4\rangle_I + e^2\langle \hat{F}_4\rangle_I \\ &= \langle \hat{F}_1\rangle_I + \langle \hat{F}_2\rangle_I + \langle \hat{F}_3\rangle_I + \langle \hat{F}_4\rangle_I + e(\langle \hat{F}_1\rangle_I + \langle \hat{F}_2\rangle_I + \langle \hat{F}_3\rangle_I + \langle \hat{F}_4\rangle_I) + \\ &\quad e^2(\langle \hat{F}_1\rangle_I + \langle \hat{F}_2\rangle_I + \langle \hat{F}_3\rangle_I + \langle \hat{F}_4\rangle_I) + (e+e^2h_f)\langle \hat{F}_4\rangle_I.\end{aligned}$$

Take $F = \hat{F}_1 + \hat{F}_2 + \hat{F}_3 + \hat{F}_4$ and $G = \hat{F}_4$. Now, we show $\langle F\rangle = \langle \hat{F}_1\rangle_I + \langle \hat{F}_2\rangle_I + \langle \hat{F}_3\rangle_I + \langle \hat{F}_4\rangle_I$. Clearly, $\langle F\rangle \subseteq \langle \hat{F}_1\rangle_I + \langle \hat{F}_2\rangle_I + \langle \hat{F}_3\rangle_I + \langle \hat{F}_4\rangle_I$. For any $s \neq t$, we know $\hat{F}_s\hat{F}_t \equiv 0 \bmod (x^N - 1)$, $0 \le s, t \le 4$. Since, $F_s$ and $\hat{F}_s$ are pairwise coprime, there exist $a_s, b_s \in \mathbb{F}_{p^3}[x]$ such that $a_sF_s + b_s\hat{F}_s = 1$, $1 \le s \le 4$. Also, $\prod_{s=2}^{4}(a_sF_s + b_s\hat{F}_s) = 1$, which implies that there exist some polynomials $w_1, w_2, w_3, w_4 \in \mathbb{F}_{p^3}[x]$ such that $w_1F_2F_3F_4 + w_2\hat{F}_2F_3F_4 + w_3F_2\hat{F}_3F_4 + w_4F_2F_3\hat{F}_4 = 1$, therefore, $\hat{F}_1 = w_1\hat{F}_1F_2F_3F_4$. Again, we have $w_1FF_2F_3F_4 = w_1\hat{F}_1F_2F_3F_4 = \hat{F}_1$. Hence, $\hat{F}_1 \in \langle F\rangle$. Similarly, we can show that $\hat{F}_i \in \langle F\rangle$ for $1 = 2, 3, 4$. Hence, $\langle \hat{F}_1\rangle_I + \langle \hat{F}_2\rangle_I + \langle \hat{F}_3\rangle_I + \langle \hat{F}_4\rangle_I \subseteq \langle F\rangle$. Therefore, $\langle F\rangle = \langle \hat{F}_1\rangle_I + \langle \hat{F}_2\rangle_I + \langle \hat{F}_3\rangle_I + \langle \hat{F}_4\rangle_I$. Consequently, $\mathcal{C} = \langle F\rangle_I \oplus e\langle F\rangle_I \oplus e^2\langle F\rangle_I \oplus (e+e^2h_f)\langle G\rangle_I$.

Further, $|\langle F\rangle_I| = p^{3N-3\deg F}, |\langle G\rangle_I| = p^{3N-3\deg G}$ and hence, $|\mathcal{C}| = p^{6N-3\deg F-3\deg G}$.

**Proposition 3.6:** *Let $\mathcal{C} \subseteq \mathfrak{R}^N$ be a cyclic code. Then, there is a polynomial $F \in \mathfrak{R}[x]$ satisfying $\mathcal{C} = \langle F\rangle$.*

***Proof:*** Let $\mathcal{C} \subseteq \mathfrak{R}^N$ be cyclic. By Theorem 3.4, we have

$$\mathcal{C} = \langle \hat{F}_1 \rangle \oplus \langle e\hat{F}_2 \rangle \oplus \langle e^2\hat{F}_3 \rangle \oplus \langle (e + e^2 h_f)\hat{F}_4 \rangle,$$

for $\gcd(F_i, F_j) = 1, i \neq j$, monic polynomials $F_i$'s in $\mathbb{F}_{p^3}[x]$ satisfying $x^N - 1 = \prod_{s=0}^{4} F_s$ with $\hat{F}_s = \frac{x^N - 1}{F_s}$ and a unit $h_f$ in $\mathbb{F}_{p^3}[x]$. Take $F = \hat{F}_1 + e\hat{F}_2 + e^2\hat{F}_3 + (e + e^2 h_f)\hat{F}_4$. Now, we show $C = \langle F \rangle$. Clearly, $\langle F \rangle \subseteq \mathcal{C}$. Note that for $s \neq t$, $\hat{F}_s \hat{F}_t \equiv 0 \bmod (x^N - 1)$ and $F_s \hat{F}_s \equiv 0 \bmod (x^N - 1)$, $0 \leq s, t \leq 4$. Again, since $F_s$ and $\hat{F}_s$ are coprime, so there exist $a_s, b_s \in \mathbb{F}_{p^3}[x]$ such that $a_s F_s + b_s \hat{F}_s = 1$, for $s = 1, 2, 3, 4$. Also,

$$\begin{aligned} &\prod_{s=1}^{3} (a_s F_s + b_s \hat{F}_s) = 1, \text{which implies that} \\ &(c_1 F_1 F_2 F_3 + c_2 \hat{F}_1 F_2 F_3 + c_3 F_1 \hat{F}_2 F_3 + c_1 F_1 F_2 \hat{F}_3) = 1, \end{aligned} \tag{3}$$

where $c_i$, for $i = 1, 2, 3, 4$ are some polynomials in $\mathbb{F}_{p^3}[x]$. By performing multiplication on the both sides of equation (3) by $\hat{F}_4$, we obtain $c_1 F_1 F_2 F_3 \hat{F}_4 = \hat{F}_4$. Also, $Fc_1 F_1 F_2 F_3 = (e + e^2 h_f)\, c_1 F_1 F_2 F_3 \hat{F}_4 = (e + e^2 h_f)\hat{F}_4$. Thus, $(e + e^2 h_f)\, \hat{F}_4 \in \langle F \rangle$. Continuing the same procedure, we show that $e\hat{F}_1$, $e^2\hat{F}_1 \in \langle F \rangle$. Hence, $\mathcal{C} \subseteq \langle F \rangle$ and $\mathcal{C} = \langle F \rangle$.

## 4. Examples

There is a well-known online database [6] which gives bounds on the parameters of several linear codes over $\mathbb{F}_q$, where $q = p^n \leq 9$. It is one of the most popular and reliable platforms to judge whether a linear code is good. Here, based on the database [6], we derive numerous optimal, best-known (briefly, BKLC) as well as near to optimal (good) linear $\mathbb{F}_8$-codes induced from $\mathbb{F}_8$-images of cyclic codes over $\mathfrak{R}$. We call $[n, k, d]_q$ is *Near Optimal* (good) or *Near BKLC* $[n, k, d']_q$ code, given by the database [6], if $d' - d \leq 2$. We use the Magma software [4] to carry out the computation for these examples. We represent a polynomial $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ briefly by its coefficient sequence $a_n a_{n-1} \ldots a_0$.

**Example 4.1:** Let $\mathbb{F}_8 = \mathbb{F}_2[\omega]$ be the field of size 8, where $\omega^3 - \omega - 1 = 0$. Then in $\mathbb{F}_8[x]$,

(1) if $N = 7$, we have

$$x^7 - 1 = (11)(1\omega)(1\omega^2)(1(\omega+1))(1(\omega^2+1))(1(\omega+\omega^2))(1(\omega^2+\omega+1))$$
$$= f_1 f_2 f_3 f_4 f_5 f_6 f_7 \text{ (say).}$$

(2) if $N = 9$, we have

$$x^9 - 1 = (11)(111)(1\omega 1)(1\omega^2 1)(1\omega^4 1)$$
$$= g_1 g_2 g_3 g_4 g_5 \text{ (say).}$$

By following Theorem 3.4, the generator polynomials for cyclic codes of length 7 and 8 over $\mathfrak{R} = M_3(\mathbb{F}_2)$ are given in $2^{nd}$ column of Table 1 and their $\mathbb{F}_8$-Gray images which include many optimal codes (as per the database [6]) are given by $3^{rd}$ column.

**Table 1**

**Optimal linear codes induced from $\mathbb{F}_8$-images of cyclic codes of length *N* over $M_3(\mathbb{F}_2)$**

| N | Generators of cyclic codes | $\Pi(\mathcal{C})$ | Remarks |
|---|---|---|---|
| 7 | $\langle f_5, e^2 f_1 f_2 \rangle$ | [21,16,4] | BKLC |
| 7 | $\langle f_5, e f_1 f_2, e^2 f_4 \rangle$ | [21,20,2] | Optimal |
| 7 | $\langle f_3 f_4, e f_1 f_2 \rangle$ | [21,19,2] | Optimal |
| 7 | $\langle f_3 f_4, e^2 f_1 f_2 \rangle$ | [21,17,3] | Near Optimal |
| 9 | $\langle g_3, e^2 g_1 g_2 \rangle$ | [27,23,4] | Optimal |
| 9 | $\langle e^2 g_3, g_1 \rangle$ | [27,25,2] | Optimal |
| 9 | $\langle e^2 g_1, (e+e^2) g_2 g_4 \rangle$ | [27,18,5] | Near BKLC |
| 9 | $\langle g_3, e g_1 g_4, (e+e^2) g_2 \rangle$ | [27,24,3] | Optimal |

**Table 2**

**Optimal linear codes induced from $\mathbb{F}_8$-images of cyclic codes of length *N* over $M_3(\mathbb{F}_2)$**

| *N* | Generators of cyclic codes | $\Pi(\mathcal{C})$ | Remarks |
|---|---|---|---|
| 15 | $\langle e^2 f_3, (e+e^2) f_5 f_2 \rangle$ | [45,42,3] | Optimal |
| 15 | $\langle f_1 f_3, e f_2, (e+e^2) f_4 f_5 \rangle$ | [45,44,2] | Optimal |
| 15 | $\langle e^2 f_3 f_2, (e+e^2) f_5 f_1 f_4 \rangle$ | [45,40,4] | Optimal |
| 17 | $\langle e g_2, (e+e^2) g_1 \rangle$ | [51,43,7] | Optimal |

*Contd...*

| | | | |
|---|---|---|---|
| 17 | $\langle eg_2, (e+e^2)g_1g_3\rangle$ | [51,39,8] | BKLC |
| 19 | $\langle h_1h_2, eh_4\rangle$ | [57,51,5] | Optimal |
| 19 | $\langle eh_3, e^2h_4, (e+e^2)h_1h_2\rangle$ | [57,53,3] | Near Optimal |
| 39 | $\langle k_2k_4, e^2k_7, (e+e^2)k_8k_{11}\rangle$ | [117,112,4] | Optimal |
| 39 | $\langle ek_1k_2k_4, (e+e^2)k_3k_8k_9k_{10}\rangle$ | [117,108,5] | BKLC |
| 39 | $\langle k_4k_7, e^2k_1k_2, (e+e^2)k_6k_9k_{10}\rangle$ | [117,109,6] | Optimal |

**Example 4.2:** Let $\mathcal{C}$ be a cyclic code over $M_3(\mathbb{F}_2)$ of length $N$, and $\mathbb{F}_8 = \mathbb{F}_2[\omega]$, where $\omega^3 - \omega - 1 = 0$. In $\mathbb{F}_8[x]$,

(1) if $N = 15$, then

$$\begin{aligned} x^{15} - 1 &= (11)(111)(10011)(11001)(11111) \\ &= f_1f_2f_3f_4f_5 \text{ (say).} \end{aligned}$$

(2) if $N = 17$, then

$$\begin{aligned} x^{17} - 1 &= (11)(100111001)(111010111) \\ &= g_1g_2g_3 \text{ (say).} \end{aligned}$$

(3) if $N = 19$, then

$$\begin{aligned} x^{19} - 1 &= (11)(1\omega^3\omega^6\omega^6\omega^6\omega^3 1)(1\omega^5\omega^3\omega^3\omega^3\omega^5 1)(1\omega^6\omega^5\omega^5\omega^5\omega^6 1) \\ &= h_1h_1h_3h_4 \text{ (say).} \end{aligned}$$

(4) if $N = 39$, then

$$\begin{aligned} x^{39} - 1 &= (11)(111)(11\omega\omega^2 1)(11\omega^2\omega^4 1)(11\omega^4\omega 1)(1\omega\omega^4 11)(1\omega^2\omega 11)\times \\ &\quad (1\omega^3\omega^5\omega^3 1)(1\omega^4\omega^2 11)(1\omega^5\omega^6\omega^5 1)(1\omega^6\omega^3\omega^6 1) \\ &= k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11} \text{ (say).} \end{aligned}$$

Cyclic codes of length $N = 15, 17, 19$ and 39 over $M_3(\mathbb{F}_2)$ and optimal linear codes over $\mathbb{F}_8$ induced from the Gray images are enlisted in Table 2.

## 5. Conclusion

The paper gives an extensive study on algebraic properties of cyclic codes of length $N$ satisfying $\gcd(N, p) = 1$ over $M_3(\mathbb{F}_p)$. By defining a Gray map from $M_3(\mathbb{F}_p)$ to $\mathbb{F}_{p^3} + e\mathbb{F}_{p^3} + e^2\mathbb{F}_{p^3}$, we derive numerous optimal and good linear codes over $\mathbb{F}_{p^3}$ for $p = 2$. In future, one may find interesting

to study $(i)$ self-dual cyclic codes of arbitrary length over $M_3(\mathbb{F}_p)$ for a prime $p$, and $(ii)$ cyclic codes of arbitrary length over $M_4(\mathbb{F}_p)$, for odd $p$.

**Acknowledgement**

The second author acknowledged the funding of the Department of Science and Technology (DST) (under project CRG/2020/005927, vide Diary No. SERB/F/6780/ 2020-2021 dated 31 December 2020). Also, all authors express their gratitude to the anonymous referee(s) and the Editor for their detailed comments while evaluating the manuscript, which improves its presentation.

**References**

[1] A. Alahmadi, H. Sboui, P. Solé and O. Yemen, Cyclic codes over $M_2(\mathbb{F}_2)$, *J. Franklin Inst.* 350, pp. 2837-2847 (2013).

[2] C. Bachoc, Applications of coding theory to the construction of modular lattices, *IEEE Trans. Inf. Theory* 78(1) , pp. 92-119 (1997).

[3] S. Bhowmick, S. Bagchi and R. K. Bandi, Self-dual cyclic codes over $M_2(\mathbb{Z}_4)$, arXiv:1807.04913 (2018).

[4] W. Bosma and J. Cannon, Handbook of Magma Functions, Univ. of Sydney, Sydney (1995).

[5] D. F. Falcunit and V. Sison, Cyclic codes over matrix ring $M_2(\mathbb{F}_p)$ and their isometric images over $\mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$, arXiv:1409.7228 (2014).

[6] M. Grassl, Code Tables: Bounds on the parameters of codes, online, http://www.codetables.de.

[7] M. Greferath, Cyclic codes over finite rings, *Discrete Math*. 177(1-2), pp. 273-277 (1997).

[8] M. Greferath and S. E. Schmidt, Linear Codes and Rings of Matrices, Proceedings of AAECC 13 Hawaii Springer LNCS 1719, pp. 160-169 (1999).

[9] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Coethals, and related codes, *IEEE Trans. Inform. Theory* 40(2), pp. 301-319 (1994).

[10] H. Islam and O. Prakash, A study of cyclic and constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, *Int. J. Inf. Coding Theory* 5(2), pp. 155-168 (2018).

[11] H. Islam and O. Prakash, A class of constacyclic codes over the ring $\mathbb{Z}_4[u,v]/\langle u^2, v^2, uv-vu\rangle$ and their Gray images, *Filomat* 33(8), pp. 2237-2248 (2019).

[12] H. Islam, T. Bag and O. Prakash, A class of constacyclic codes over $\mathbb{Z}_4[u]/\langle u^k\rangle$, *J. Appl. Math. Comput.* 60(1-2), pp. 237-251 (2019).

[13] H. Islam, O. Prakash and D. K. Bhunia, On the structure of cyclic codes over $M_2(\mathbb{F}_p + u\mathbb{F}_p)$, *Indian J. Pure Appl. Math.* 53(1), pp. 153-161 (2022).

[14] H. Islam, E. Martínez-Moro and O. Prakash, Cyclic codes over a non-chain ring $R_{e,q}$ and their application to LCD codes, *Discrete Math.* 344(10), Paper No. 112545 (2021).

[15] H. Islam and O. Prakash, New $\mathbb{Z}_4$ codes from constacyclic codes over a non-chain ring, *Comp. Appl. Math.* 40(1), pp. 1-17 (2021).

[16] H. Islam and O. Prakash, Construction of reversible cyclic codes over $\mathbb{Z}_{p^k}$, *J. Discrete Math. Sci. Cryptogr.* 25(6), pp. 1817-1830 (2022). https://doi.org/10.1080/09720529.2020.1815341.

[17] P. Kanwar and S. Lopez-Permouth, Cyclic codes over the integers modulo $p^m$, *Finite Fields Appl.* 3(4), pp. 334-352 (1997).

[18] R. Luo and P. Udaya, Cyclic codes over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$, *Cryptogr. Commun.* 10(6), pp. 1109-1117 (2018).

[19] M. A. Mohammed, A. J. Munshid and M. Alaeiyan, Cyclic codes of length $p^n$ over $(\mathbb{Z}_p)^m$, *J. Discrete Math. Sci. Cryptogr.*, 24(2), 579-588 (2021).

[20] F. Oggier, P. Solé and J. C. Belfiore, Codes over matrix rings for space-time coded modulations, *IEEE Trans. Inf. Theory* 58(2), pp. 734-746 (2012).

[21] J. Pal, S. Bhowmick and S. Bagchi, Cyclic codes over $M_4(\mathbb{F}_2)$, *J. Appl. Math. Comput.* 60(1-2), pp. 749-756 (2019).

[22] Pankaj and M. Pruthi, Cyclic codes of prime power length from generalized cyclotomic classes of order $2r$, *Journal of Information and Optimization Sciences*, 39(4), 965-971 (2018).

[23] S. Patel, O. Prakash and H. Islam, Cyclic codes over $M_4(\mathbb{F}_2 + u\mathbb{F}_2)$, *Cryptogr. Commun* 14(5), pp. 1021-1034 (2022).

[24] O. Prakash, H. Islam and S. Das, On Cyclic Codes with Minimal Generating Sets over the Ring $\mathbb{Z}_{p^k}$, *Southeast Asian Bulletin of Mathematics* 45(4), pp. 521-532 (2021).

[25] V. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* 42(5), pp. 1594-1600 (1996).

[26] W. Scharlau, Quadratic and Hermitian Forms, New York: Springer-Verlag (1985).

[27] B. A. Sethuraman, B. S. Rajan and V. Shashidhar, Full-diversity, high-rate space-time block codes from division algebras, *IEEE Trans. Inform. Theory* 49(10), pp. 2596-2616 (2003).

[28] R. Wisbauer, Foundations of Module and Ring Theory. Gordon and Breach (1991).

[29] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* 45(7), pp. 2527-2532 (1999).

*Received September 2022*