Palestine Journal of Mathematics

Vol 14(2)(2025) , 180–193 © Palestine Polytechnic University-PPU 2025

On Cyclic Codes over $M_3(\mathbb{F}_3)$

Xuesong Si and Chuanze Niu

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 11T71; Secondary 94B05, 94B15.

Keywords and phrases: Cyclic codes, Cyclic algebra, Matrix rings, Gray map.

The authors would like to thank the anonymous reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Corresponding Author: Chuanze Niu

Abstract This paper studies the structure of cyclic codes of length n over $M_3(\mathbb{F}_3)$. We define the Gray map ϕ from $M_3(\mathbb{F}_3)$ to $\mathbb{F}_{3^3}^3$ and investigate the structural properties of cyclic codes over $M_3(\mathbb{F}_3)$ by using cyclic algebra. It is shown that cyclic codes of length n over $M_3(\mathbb{F}_3)$ are principal ideals of $\mathcal{R}[x]/\langle x^n-1\rangle$. Meanwhile, a linear code of length n over $M_3(\mathbb{F}_3)$ can be regarded as a linear code of length $3n$ over $\mathbb{F}_{3^3}$ under the Gray map ϕ. Furthermore, we prove that $M_3(\mathbb{F}_p)$ is isomorphic to the cyclic algebra $(\mathbb{F}_q/\mathbb{F}_p, \tau, 1)$ and discuss the structure of linear codes over $M_3(\mathbb{F}_p)$ with $q=p^3$, when $p\equiv 1(\mathrm{mod}6)$.

1 Introduction

In recent three decades, the theory of error-correcting codes over finite rings has gained a great deal of attention since Hammons et al. [13] showed that some good nonlinear binary codes can be represented as Gray images of linear codes on $\mathbb{Z}_4$. Numerous linear codes over commutative rings have been built (see [1, 5–9, 21, 22, 24, 25, 31]).

Codes on non-commutative rings in theory of error-correcting codes are becoming more important. Many researchers wonder about the structure of cyclic codes over finite non-commutative rings owing to the rich algebraic structure of cyclic codes over finite fields and commutative rings. Linear codes over matrix rings have been a widely studied topic since Wood [30] proved that finite Frobenius rings are suitable as linear coded alphabets. The ring $M_2(\mathbb{F}_2)$ as a linear coded alphabet appeared first in the algebraic construction for modular lattices in [3]. Greferath et al. considered the role of the matrix rings in coding theory in [12]. In 2012, Oggier et al. [19] constructed space-time codes over $M_2(\mathbb{F}_2)$. In 2013, Alahmadi et al. [2] studied cyclic codes over $M_2(\mathbb{F}_2)$ and explored self-dual $\mathbb{F}_4$-codes. The structure of cyclic codes over $M_2(\mathbb{F}_p)$ was built in 2014 by Falcunit and Sison [11]. In 2018, Luo and Parampalli [18] investigated cyclic codes over the matrix ring $M_2(\mathbb{F}_2+u\mathbb{F}_2)$ and obtained some optimal $\mathbb{F}_4$-codes. In 2019, Pal et al. [20] constructed cyclic codes over $M_4(\mathbb{F}_2)$. Bhowmick et al. [4] studied self-dual cyclic codes over $M_2(\mathbb{Z}_4)$ and Islam et al. [15] extended the results of [11] to $M_2(\mathbb{F}_p+u\mathbb{F}_p)$ in 2022. Patel et al. [23] considered the structure of cyclic codes over $M_4(\mathbb{F}_2+u\mathbb{F}_2)$. The structure of skew cyclic codes over $M_2(\mathbb{F}_2)$ was studied by Si and Niu [28]. Dinh et al [10] derived the structure theorem for cyclic codes of odd length n over the ring $\mathcal{A}=M_2(\mathbb{F}_2[u]/\langle u^k\rangle)$ with the help of isometry map from $\mathcal{A}$ to $\mathbb{F}_4[u,v]/\langle u^k, v^2, uv-vu\rangle$.

This paper uses cyclic algebra introduced in [3, 27] to consider the structure of cyclic codes over $M_3(\mathbb{F}_3)$ and defines the Gray map ϕ from $M_3(\mathbb{F}_3)$ to $\mathbb{F}_{3^3}^3$. The cyclic codes over $M_3(\mathbb{F}_3)$ are corresponding to the linear codes over the finite field $\mathbb{F}_{3^3}$ by using Gray map ϕ. We also study linear codes over $M_3(\mathbb{F}_p)$ when $p\equiv 1(\mathrm{mod}6)$.

The structure of the article is as follows: In Section 2, this paper will introduce some essential basic facts. This section proves that $M_3(\mathbb{F}_3)$ is isomorphic to the finite chain ring $\mathcal{R}=\mathbb{F}_{3^3}\oplus u\mathbb{F}_{3^3}\oplus u^2\mathbb{F}_{3^3}, u^3=0$. Meanwhile, the parameters of the Gray images of the linear codes of length n over $\mathcal{R}$ are given in this section. In Section 3, the structural theorems of cyclic codes of length n over $M_3(\mathbb{F}_3)$ are obtained. The structure of linear codes over $M_3(\mathbb{F}_p)$ is studied in Section 4. Section 5 concludes this work.

2 Frobenius Rings and Cyclic Algebras

Let R be a finite ring with identity $1 \neq 0$. An ideal I of R is called principal, denoted by $I = \langle a \rangle$, if it is generated by an element $a \in R$. If all the ideals of R are principal, then R is called a principal ideal ring. R is called a local ring if R has a unique right (resp. left) maximal ideal. A ring R is called a right (resp. left) chain ring if the set of all right (resp. left) ideals of R is linearly ordered under the set inclusion. Unless otherwise explained, all rings mentioned in this paper have a multiplication identity.

We define the Jacobson radical as the intersection of all maximal ideals in R, denoted by $\mathrm{Rad}(R)$. It is a two side ideal. The left(resp. right) socle of a ring R, denoted by $\mathrm{Soc}({}_RR)$ (resp. $\mathrm{Soc}(R_R)$), is the sum of all minimal left (resp. right) ideals. A finite ring R is a Frobenius ring if and only if ${}_R(R/\mathrm{Rad}(R)) \simeq \mathrm{Soc}({}_RR)$ [14]. The ring $M_n(R)$ of $n \times n$ matrices over a Frobenius ring R is also Frobenius [29]. Next, we give the definition of cyclic algebra. Lemma 2.2 describes the relation between the Frobenius ring $M_3(\mathbb{F}_3)$ and cyclic algebra.

Let R^n be the set of all n-tuples over R. A nonempty subset C of R^n is called a code of length n over R. A code C of length n over R is called right (resp. left) linear if it is a right (resp. left) R-submodule of R^n. Elements of C are said to be codewords. Each codeword c in the code C is an n-tuple of the form $c = (c_0, c_1, \cdots, c_{n-1}) \in C$.

Definition 2.1. Let ${}^L/_K$ be a cyclic extension of degree n, with Galois group $\mathrm{Gal}({}^L/_K) = \langle \sigma \rangle$, where σ is the generator of the cyclic group. Let $({}^L/_K, \sigma, \gamma)$ be its corresponding cyclic algebra of degree n, that is

$$({}^L/_K, \sigma, \gamma) \simeq L \oplus eL + e^2L \oplus \cdots \oplus e^{n-1}L$$

with $e \in ({}^L/_K, \sigma, \gamma)$ such that $le = e\sigma(l)$ for all $l \in L$ and $e^n = \gamma \in K, \gamma \neq 0$.

Lemma 2.2. *A split algebra $M_n(K)$ can be considered as a cyclic algebra if there is a cyclic extension ${}^L/_K$ of degree n because L can be embedded in $M_n(K) \simeq \mathrm{End}_K(L)$ by using the regular representation.*

We consider the cyclic algebra $\mathcal{A} = ({}^{\mathbb{F}_{3^3}}/_{\mathbb{F}_3}, \sigma, 1)$, where $\mathbb{F}_{3^3} \simeq \mathbb{F}_3[\alpha]$ with $\alpha^3 - \alpha + 1 = 0$. Its cyclic Galois group $\mathrm{Gal}({}^{\mathbb{F}_{3^3}}/_{\mathbb{F}_3})$ is generated by the Frobenius automorphism $\sigma(a) = a^3$. If we consider the map $\mu : \mathcal{A} \to M_3(\mathbb{F}_3)$,

$$e \mapsto \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \alpha \mapsto \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

then it is easy to check that μ is a isomorphism by [19] and [26, Lemma 12.6]. Therefore, we have

$$\mathcal{A} \simeq M_3(\mathbb{F}_3) \simeq \mathbb{F}_{3^3} \oplus e\mathbb{F}_{3^3} \oplus e^2\mathbb{F}_{3^3},$$

where the multiplication is given by $ae = e\sigma(a)$ for all $a \in \mathbb{F}_{3^3}$. The cyclic algebra $\mathcal{A}$ contains the finite field $\mathbb{F}_{3^3}$ and has an $\mathbb{F}_{3^3}$-basis $\{1, e, e^2\}$. It is a central simple algebra over $\mathbb{F}_3$ and $\dim\mathcal{A} = 9$ by [26, Theorem 12.1]. Note that $(e-1)^3 = 0$, then $e - 1$ is a nilpotent element of order 3. Let $u = e - 1$, and do a change of basis to get

$$\mathcal{A} \simeq \mathbb{F}_{3^3} \oplus u\mathbb{F}_{3^3} \oplus u^2\mathbb{F}_{3^3}. \tag{2.1}$$

Let $\mathcal{R} = \mathbb{F}_{3^3} \oplus u\mathbb{F}_{3^3} \oplus u^2\mathbb{F}_{3^3}$. It is a finite local ring with the unique maximal ideal $\langle u \rangle$. Notice that the ring $\mathcal{R}$ is non-commutative for multiplication. The multiplication and the ideals mentioned in this paper are always right.

Let C be a code of length n over $\mathcal{R}$. The Hamming weight $w_{Ham}(c)$ of a codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ is the number of nonzero components. The minimum weight $w_{Ham}(c)$ of the code C is the smallest weight among all its nonzero codewords. For $x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1}) \in C$, $d_{Ham} = \#\{i | x_i \neq y_i\}$ is called the Hamming distance between x and y. It is denoted by $d_{Ham}(x, y) = w_{Ham}(x - y)$. The minimum Hamming distance between distinct pairs of codewords of C is called the minimum distance of C and denoted by $d_{Ham}(C)$.

For any $r = r_0 + ur_1 + u^2r_2 \in \mathcal{R}$, the Lee weight of r is defined as

$$w_L(r) = w_{Ham}(r_2) + w_{Ham}(r_1 + r_2) + w_{Ham}(r_0 + r_1 + r_2), \tag{2.2}$$

where $w_{Ham}(*)$ holds the usual Hamming weight on $\mathbb{F}_{3^3}$. Let $c = (c_0, c_1, \cdots, c_{n-1}) \in C$. Then the Lee weight of c is the rational sum of Lee weights of its components, that is, $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$. For $x, y \in C$, the Lee distance $d_L(x, y)$ between x and y is the Lee weight of $x - y$, i.e. $d_L(x, y) = w_L(x - y)$. The minimum Lee weight of C is the smallest nonzero Lee weight among all codewords. The minimum Lee distance of C is the smallest nonzero Lee distance between all pairs of distinct codewords. If C is linear, then the minimum Lee distance is same as the minimum Lee weight.

Define the Gray map ϕ from $\mathcal{R}$ to $\mathbb{F}_{3^3}^3$ following the method in [6],

$$\phi(r_0 + ur_1 + u^2 r_2) = (r_2, r_1 + r_2, r_0 + r_1 + r_2).$$

The map ϕ is a linear distance-preserving bijection and can be extended to $\mathcal{R}^n$. From [20] and the linearity of the map ϕ, we have the following theorem.

Theorem 2.3. *Let n be an integer that is not divisible by 3. If $\mathcal{C}$ is a linear code over $\mathcal{R}$ of length n with size $\mathcal{M}$ and the minimum Lee distance d_{Lee}, then $\phi(\mathcal{C})$ is a linear code over $\mathbb{F}_{3^3}$ of length $3n$ with size $\mathcal{M}$ and the minimum Hamming distance d_{Ham}.*

3 Cyclic Codes over $M_3(\mathbb{F}_3)$

Let n be an integer that is not divisible by 3. We set $\mathcal{R}[x]$ is the ring of polynomials over $\mathcal{R}$ and $\mathcal{R}_n = \mathcal{R}[x]/\langle x^n - 1\rangle$. Then a linear code of length n over $\mathcal{R}$ is a right $\mathcal{R}$-submodule of $\mathcal{R}^n$. Let $\mathcal{C}$ be a linear code of length n over $\mathcal{R}$. The linear code $\mathcal{C}$ is called cyclic if for any codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, its cyclic shift $(c_{n-1}, c_0, c_1, \cdots, c_{n-2})$ is also in $\mathcal{C}$.

This section shows that every cyclic code of length n over $\mathcal{R}$ is a right principal ideal of $\mathcal{R}_n$. Theorem 3.1 describes the sufficient and necessary conditions for a linear code over $\mathcal{R}$ to be a cyclic code. Theorems 3.6 and 3.8 illustrate the structure of cyclic codes over $\mathcal{R}$.

Theorem 3.1. *A linear code $\mathcal{C} = \mathcal{C}_0 + u\mathcal{C}_1 + u^2\mathcal{C}_2$ of length n over $\mathcal{R}$ is cyclic if and only if $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ are cyclic codes of length n over $\mathbb{F}_{3^3}$.*

Proof. Let θ be the standard cyclic shift map on $\mathcal{R}^n$, i.e., for any $c \in \mathcal{C}$, we have that $\theta(c) \in \mathcal{C}$ and θ is linear. If $c_0 + uc_1 + u^2c_2 \in \mathcal{C}$, where $c_i \in \mathcal{C}_i$, $i = 0, 1, 2$, then $\theta(c_0 + uc_1 + u^2c_2) = \theta(c_0) + u\theta(c_1) + u^2\theta(c_2) \in \mathcal{C}$. Thus, $\theta(c_i) \in \mathcal{C}_i$, $i = 0, 1, 2$, i.e., $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ are cyclic.

Conversely, if $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ are cyclic codes over $\mathbb{F}_{3^3}$. Then for every $c_0 + uc_1 + u^2c_2 \in \mathcal{C}$, where $c_i \in \mathcal{C}_i$, $i = 1, 2, 3$, we have $\theta(c_0) \in \mathcal{C}_0$, $\theta(c_1) \in \mathcal{C}_1$ and $\theta(c_2) \in \mathcal{C}_2$. Therefore, $\theta(c_0 + uc_1 + u^2c_2) = \theta(c_0) + u\theta(c_1) + u^2\theta(c_2) \in \mathcal{C}$, i.e., $\mathcal{C}$ is cyclic over $\mathcal{R}$. □

There exists a natural homomorphic map from $\mathcal{R}$ to the Galois field $\mathbb{F}_{3^3}$. For any $r \in \mathcal{R}$, let $\bar{r}$ denote the element reduction modulo u. Define the polynomial reduction map $\delta : \mathcal{R}[x] \to \mathbb{F}_{3^3}[x]$ such that

$$f(x) = \sum_{i=0}^{n-1} r_i x^i \mapsto \sum_{i=0}^{n-1} \bar{r}_i x^i = \bar{f}(x).$$

Definition 3.2. A monic polynomial f over $\mathcal{R}[x]$ is called a basic irreducible polynomial if its image $\bar{f}$ under the map δ is irreducible.

Since the characteristic of $\mathcal{R}$ is 3 and n is not divisible by 3, then it implies that $x^n - 1$ has a unique decomposition as a product of basic irreducible pairwise coprime polynomials in $\mathcal{R}[x]$ from [8, Proposion 2.7].

Lemma 3.3. *Let $x^n - 1 = \prod_{i=1}^{t} f_i$, where $f_i's$, $i = 1, 2, \cdots t$, are basic irreducible polynomials in $\mathcal{R}[x]$. Then*

$$\mathcal{R}_n = \mathcal{R}[x]/\langle x^n - 1\rangle = \bigoplus_{i=1}^{t} \mathcal{R}[x]/\langle f_i\rangle.$$

Proof. The proof is obtained easily from the Chinese Remainder Theorem. □

Lemma 3.4. *Let g be a basic irreducible polynomial in $\mathcal{R}[x]$. Then the right ideals of $\mathcal{R}_g = \mathcal{R}[x]/\langle g\rangle$ are $\langle 0\rangle$, $\langle 1\rangle$, $\langle u\rangle$, and $\langle u^2\rangle$.*

Proof. First, we assert that these four ideals are not equal to each other. They can be rewritten as $\langle u^i + \langle g\rangle\rangle$, $i = 0, 1, 2, 3$. Let $\langle u^i + \langle g\rangle\rangle = \langle u^j + \langle g\rangle\rangle$, $0 \le i < j \le 3$. Then there exist $r(x) \in \mathcal{R}[x]$ with $\deg(r(x)) < \deg(g(x))$ such that $u^i + \langle g\rangle = u^j r(x) + \langle g\rangle$. This shows that $u^i - u^j r(x) \in \langle g(x)\rangle$. Since,

$$\deg(u^j r(x) - u^i) \le \deg(r(x)) \le \deg(g(x)),$$

it follows that $u^j r(x) - u^i = 0$. Multiplying above equation by u^{3-j}, we have $u^{3+i-j} = 0$. Thus, $3 + i - j = 0$, i.e. $i = j$. Next, we prove that $\mathcal{R}/\langle g\rangle$ has only four ideals.

Let N be a nonzero right $\mathcal{R}$-submodule of $\mathcal{R}_g$ and $h(x)$ be a nonzero element in N with $h \notin \langle g\rangle$. Then $h(x) = h_0(x) + uh_1(x) + u^2h_2(x)$, where $h_i(x) \in \mathbb{F}_{3^3}[x]$ for $i = 0, 1, 2$, and

$$\gcd(g(x), h_i(x)) = 1 \text{ or } g(x).$$

If $\gcd(g, h_0) = 1$, i.e. $g(x)$ and $h_0(x)$ are coprime in $\mathcal{R}[x]$, then there exist s_0, t_0 such that $gs_0 + h_0t_0 = 1$. That implies

$$(h_0 + \langle g\rangle)(t_0 + \langle g\rangle) = 1 + \langle g\rangle,$$

where $\langle h_0 + \langle g\rangle\rangle$ is an unit in $\mathcal{R}[x]/\langle g\rangle$. Therefore, $N = \mathcal{R}[x]/\langle g\rangle = \langle 1\rangle$.

If $\gcd(g, h_0) = g$, $\gcd(g, h_1) = 1$, then $h + \langle g\rangle = uh_1 + u^2h_2 + \langle g\rangle$. That means $N = \langle u\rangle$.

If $\gcd(g, h_0) = g$, $\gcd(g, h_1) = g$ and $\gcd(g, h_2) = 1$ then $h + \langle g\rangle = u^2h_2 + \langle g\rangle$, i.e. $N = \langle u^2\rangle$.

If $\gcd(g, h_i) = g$ for $i = 1, 2, 3$, then it's obvious that $N = \langle 0\rangle$. □

Lemma 3.4 shows that the right ideals of $\mathcal{R}_g = \mathcal{R}[x]/\langle g\rangle$ form a chain.

Lemma 3.5. *Let $x^n - 1 = \prod_{i=1}^{t} f_i$, where the $f_i's$ are pairwise coprime monic basic irreducible polynomials in $\mathcal{R}[x]$. Let $\hat{f}_i = \frac{x^n-1}{f_i}$. Then any right ideal of $\mathcal{R}[x]/\langle x^n - 1\rangle$ is a direct sum of the ideals $\langle \hat{f}_i\rangle$, $\langle u\hat{f}_i\rangle$ and $\langle u^2\hat{f}_i\rangle$.*

Proof. By Lemma 3.3, we have

$$\mathcal{R}[x]/\langle x^n - 1\rangle = \mathcal{R}[x]/\cap_{i=1}^{t}\langle f_i\rangle \simeq \bigoplus_{i=1}^{t} \mathcal{R}[x]/\langle f_i\rangle. \tag{3.1}$$

Thus, any ideal of $\mathcal{R}[x]/\langle x^n - 1\rangle$ is one of the form $\oplus_{i=1}^{t}\mathcal{I}_i$, where $\mathcal{I}_i$ is a nonzero ideal of $\mathcal{R}[x]/\langle f_i\rangle$. By Lemma 3.4, we have $\mathcal{I}_i \in \{\langle f_i\rangle, \langle 1 + \langle f_i\rangle\rangle, \langle u + \langle f_i\rangle\rangle, \langle u^2 + \langle f_i\rangle\rangle\}$, $1 \le i \le t$. Hence $\mathcal{I}_i$ corresponds to one of the forms $\langle x^n - 1\rangle$, $\langle \hat{f}_i + \langle x^n - 1\rangle\rangle$, $\langle u\hat{f}_i + \langle x^n - 1\rangle\rangle$, $\langle u^2\hat{f}_i + \langle x^n - 1\rangle\rangle$ in $\mathcal{R}[x]/\langle x^n - 1\rangle$. □

The following theorems describe the structure of cyclic codes over $M_3(\mathbb{F}_3)$.

Theorem 3.6. *Let $x^n - 1 = \prod_{i=1}^{t} f_i$, where the $f_i's$ are pairwise coprime monic basic irreducible polynomials in $\mathcal{R}[x]$. If $\mathcal{C}$ is a cyclic code of length n over $\mathcal{R}$, then there exists a range of pairwise coprime monic polynomials $p_i(x) \in \mathbb{F}_{3^3}[x]$, $i = 0, 1, 2, 3$, such that $x^n - 1 = \prod_{i=0}^{3} p_i(x)$ and $\mathcal{C} = \langle \hat{p}_1\rangle \oplus \langle u\hat{p}_2\rangle \oplus \langle u^2\hat{p}_3\rangle$. Furthermore $|\mathcal{C}| = 27^{3\deg(p_1)+2\deg(p_2)+\deg(p_3)}$.*

Proof. Since $\mathcal{C}$ is a cyclic code of length n over $\mathcal{R}$, then it can be seen as a direct sum of the form of an array of ideals $\langle u^j\hat{f}_i + \langle x^n - 1\rangle\rangle$, $0 \le j \le 3$, $1 \le i \le t$ by Lemma 3.5.

Without loss of generality, we make the following assumption,

$$\begin{aligned}\mathcal{C} = {} & \langle \hat{f}_{s_1+1}\rangle \oplus \cdots \oplus \langle \hat{f}_{s_1+s_2}\rangle \\ & \oplus \langle u\hat{f}_{s_1+s_2+1}\rangle \oplus \cdots \oplus \langle u\hat{f}_{s_1+s_2+s_3}\rangle \\ & \oplus \langle u^2\hat{f}_{s_1+s_2+s_3+1}\rangle \oplus \cdots \oplus \langle u^2\hat{f}_t\rangle,\end{aligned}$$

where $s_i \geq 0$ and $s_1 + s_2 + s_3 + 1 \leq t$. For $s_1 + s_2 + s_3 + s_4 = t$, define

$$\begin{aligned} p_0 &= f_1 f_2 \cdots f_{s_1}, \\ p_1 &= f_{s_1+1} \cdots f_{s_1+s_2}, \\ p_2 &= f_{s_1+s_2+1} \cdots f_{s_1+s_2+s_3}, \\ p_3 &= f_{s_1+s_2+s_3+1} \cdots f_{s_1+s_2+s_3+s_4}. \end{aligned}$$

By our construction, it is clear that p_0, p_1, p_2, p_3 are pairwise coprime and $x^n - 1 = \prod_{i=0}^{3} p_i$. Thus, $\mathcal{C} = \langle \hat{p}_1 \rangle \oplus \langle u\hat{p}_2 \rangle \oplus \langle u^2 \hat{p}_3 \rangle$.

By [8, Theorem 3.4], we have $|\mathcal{C}| = |\langle \hat{p}_1 \rangle| \cdot |\langle u\hat{p}_2 \rangle| \cdot |\langle u^2 \hat{p}_3 \rangle|$ and

$$|\langle u^i \hat{p}_{i+1} \rangle| = \left(\frac{|\mathcal{R}|}{|\langle u^{3-i} \rangle|} \right)^{(n-\deg(\hat{p}_{i+1}))} = \left(\frac{|\overline{\mathcal{R}}|^3}{|\overline{\mathcal{R}}|^i} \right)^{\deg(p_{i+1})} = \left(|\overline{\mathcal{R}}| \right)^{(3-i)\deg(p_{i+1})},$$

$i = 0, 1, 2$, where $\overline{\mathcal{R}} = \mathcal{R}/\langle u \rangle$. Thus, $|\mathcal{C}| = 27^{3\deg(p_1)+2\deg(p_2)+\deg(p_3)}$. □

By Theorem 3.6, we obtain the following corollary.

Corollary 3.7. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{R}$. There exist polynomials $q_0(x)$, $q_1(x)$, $q_2(x)$ in $\mathbb{F}_{3^3}[x]$ such that $\mathcal{C} = \langle q_0 \rangle \oplus \langle uq_1 \rangle \oplus \langle u^2 q_2 \rangle$ and $q_2(x)|q_1(x)|q_0(x)|x^n - 1$.*

Proof. By Theorem 3.6, there exists a family of pairwise coprime monic polynomials $p_i(x) \in \mathbb{F}_{3^3}[x]$, $i = 0, 1, 2, 3$ and $\prod_{i=0}^{3} p_i(x) = x^n - 1$, such that $\mathcal{C} = \langle \hat{p}_1 \rangle \oplus \langle u\hat{p}_2 \rangle \oplus \langle u^2 \hat{p}_3 \rangle$.

Define $q_0 = p_0 p_2 p_3$, $q_1 = p_0 p_3$, $q_2 = p_0$. On the one hand, it is obvious that $q_2(x)|q_1(x)|q_0(x)|x^n - 1$. It should be noticed that $u^i \hat{p}_{i+1} = u^i p_0 \cdots p_i p_{i+2} \cdots p_3 = u^i q_i p_1 \cdots p_i$, $i = 0, 1, 2$. Thus, $\mathcal{C} \subseteq \langle q_0 \rangle \oplus \langle uq_1 \rangle \oplus \langle u^2 q_2 \rangle$.

On the other hand, note that $\gcd(\hat{p}_1(x), p_1(x)) = 1$ and $\gcd(p_1(x), p_2(x)) = 1$, then there exist $\varphi(x)$, $\psi(x) \in \mathbb{F}_{3^3}[x]$ such that $\varphi(x)p_1(x) + \psi(x)p_2(x) = 1$. Meanwhile,

$$\begin{aligned} q_1 &= p_0 p_3 \\ &= (\varphi p_1 + \psi p_2) p_0 p_3 \\ &= \varphi p_0 p_1 p_3 + \psi p_0 p_2 p_3 \\ &= \varphi \hat{p}_2 + \psi q_0. \end{aligned}$$

Therefore, $uq_1(x) = u\varphi\hat{p}_2(x) + u\psi q_0(x) \in \mathcal{C}$. Similarly, it can also be proved that $u^2 q_2(x) \in \mathcal{C}$, i.e. $\mathcal{C} \supseteq \langle q_0 \rangle \oplus \langle uq_1 \rangle \oplus \langle u^2 q_2 \rangle$. The proof is complete. □

Theorem 3.8. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{R}$. The generator of $\mathcal{C}$ is $P = \hat{p}_1(x) + u\hat{p}_2(x) + u^2 \hat{p}_3(x)$.*

Proof. It is obvious that $\langle P \rangle$ is contained in $\mathcal{C}$. By Theorem 3.6, we have that $\mathcal{C} = \langle \hat{p}_1, u\hat{p}_2, u^2 \hat{p}_3 \rangle$ and $\prod_{i=0}^{3} p_i = x^n - 1$, where $p_i \in \mathbb{F}_{3^3}[x]$, $i = 0, 1, 2, 3$, are pairwise coprime monic polynomials and $p_i \hat{p}_i = x^n - 1$.

For every $i, j \in \{0, 1, 2, 3\}$, $i \neq j$, it is clear that $\hat{p}_i \hat{p}_j \equiv 0 (\mathrm{mod} x^n - 1)$ and $\gcd(p_i, \hat{p}_i) = 1$. Therefore, there exist $\alpha_i(x)$ and $\beta_i(x)$ in $\mathbb{F}_{3^3}[x]$ such that for any $i \in \{0, 1, 2, 3\}$,

$$\alpha_i(x) p_i(x) + \beta_i(x) \hat{p}_i(x) = 1.$$

Multiplying them separately, we have

$$\prod_{i=1}^{k} \alpha_i(x) p_i(x) + \beta_i(x) \hat{p}_i(x) = 1 \tag{3.2}$$

where $k \in \{1, 2, 3\}$. Let $k = 2$. By Eq.(3.2), we get

$$\begin{aligned} (\alpha_1 p_1 + \beta_1 \hat{p}_1)(\alpha_2 p_2 + \beta_2 \hat{p}_2) &\equiv \alpha_1 \alpha_2 p_1 p_2 + \beta_1 \alpha_2 \hat{p}_1 p_2 + \alpha_1 \beta_2 p_1 \hat{p}_2 \\ &\equiv 1 (\mathrm{mod} x^n - 1). \end{aligned} \tag{3.3}$$

Multiplying both sides of Eq.(3.3) by $u^2\hat{p}_3$, we have

$$u^2\hat{p}_3(\alpha_1\alpha_2p_1p_2 + \beta_1\alpha_2\hat{p}_1p_2 + \alpha_1\beta_2p_1\hat{p}_2) \equiv u^2\alpha_1\alpha_2p_1p_2\hat{p}_3 \equiv u^2\hat{p}_3(\mathrm{mod}x^n - 1),$$

and

$$\alpha_1\alpha_2p_1p_2 \equiv 1(\mathrm{mod}x^n - 1). \tag{3.4}$$

By Eq.(3.4) and $P = \hat{p}_1 + u\hat{p}_2 + u^2\hat{p}_3$, we have

$$\alpha_1\alpha_2p_1p_2P \equiv u^2\alpha_1\alpha_2p_1p_2\hat{p}_3 \equiv u^2\hat{p}_3(\mathrm{mod}x^n - 1),$$

thus, $u^2\hat{p}_3 \in \langle P\rangle$.

We can prove that $\hat{p}_1, u\hat{p}_2 \in \langle P\rangle$ similarly. Therefore, $\mathcal{C} = \langle P\rangle$. □

From Theorem 3.8, we get the following corollary immediately.

Corollary 3.9. *The quotient ring $\mathcal{R}_n = \mathcal{R}[x]/\langle x^n - 1\rangle$ is a principal ideal ring.*

Let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{R}$. Then $\mathcal{C}$ has the form $\mathcal{C} = \langle\hat{p}_1\rangle \oplus \langle u\hat{p}_2\rangle \oplus \langle u^2\hat{p}_3\rangle$ by Theorem 3.6. We give the examples below.

Example 3.10. Suppose $n = 2$. The factorization of $x^2 - 1$ over $\mathbb{F}_{3^3}$ is given by $(x + 1)(x - 1)$. Let $f_1 = x + 1$, $f_2 = x - 1$. This paper considers the cyclic code $\mathcal{C}_1 = \langle f_1, uf_2\rangle$ over $\mathcal{R}$. From Lemma 3.5 and Theorem 3.6, we know that $\mathcal{C}_1 = \langle f_1\rangle \oplus \langle uf_2\rangle$.

Next, we determine the parameters of the Gray image code $\phi(\mathcal{C}_1)$ of $\mathcal{C}_1$ by MAGMA. The code $\phi(\mathcal{C}_1)$ is a linear $[6, 4, 2]$ code over $\mathbb{F}_{3^3}$. A generator matrix of $\phi(\mathcal{C}_1)$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{pmatrix}.$$

Example 3.11. Let $n = 4$. It is easy to check that $x^4 - 1 = (x + 1)(x - 1)(x^2 + 1)$. We set $f_1 = x + 1$, $f_2 = x - 1$, $f_3 = x^2 + 1$ and consider the cyclic code $\mathcal{C}_2 = \langle f_1f_2, uf_3\rangle$ over $\mathcal{R}$. Let

$$p_0 = 1, p_1 = f_3, p_2 = f_1f_2, p_3 = 1.$$

Then we have that $\mathcal{C}_2 = \langle\hat{p}_1\rangle \oplus \langle u\hat{p}_2\rangle$ by Lemma 3.5 and Theorem 3.6. The code $\phi(\mathcal{C}_2)$ is a linear $[12, 8, 2]$ code over $\mathbb{F}_{3^3}$. A generator matrix of $\phi(\mathcal{C}_2)$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

4 Linear codes over $M_3(\mathbb{F}_p)$, $p \equiv 1(\mathrm{mod}6)$

In this section, we discuss the structure of linear codes of length n over $M_3(\mathbb{F}_p)$, where p is prime and $p \equiv 1(\mathrm{mod}6)$. The relationship between cyclic algebra and the Froebnius ring $M_3(\mathbb{F}_p)$ should be determined. Eq.(4.2) shows that the cyclic algebra $\mathcal{A} = (\mathbb{F}_q/\mathbb{F}_p, \tau, 1)$ is isomorphic to $M_3(\mathbb{F}_p)$, where τ is the Frobenius map of the finite field $\mathbb{F}_p$. Meanwhile, Theorems 4.6-4.8 depict the structural properties of linear codes of length n over $M_3(\mathbb{F}_p)$.

Lemma 4.1. *[17, Theorem 6.1, König-Rados Theorem] Let* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{q-2}x^{q-2} \in \mathbb{F}_q[x]$. *We associate* f *with the* $(q-1)\times(q-1)$ *matrix* A *given by*

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \cdots & a_{q-2} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{q-2} & a_0 & \cdots & a_{q-4} & a_{q-3} \end{pmatrix},$$

then the number of nonzero solutions of $f(x) = 0$ *in* $\mathbb{F}_q$ *is equal to* $q - 1 - rank(A)$.

The matrix A is a left-circulant matrix, in which each row is obtained from the preceding row by a left cyclic shift of entries.

Definition 4.2. A polynomial $f \in R[x_1, x_2, \cdots, x_n]$ is called symmetric if $f(x_{i_1}, x_{i_2}, \cdots, x_{i_n}) = f(x_1, x_2, \cdots, x_n)$ for any permutation $i_1, i_2, \cdots, i_n$ of the integers $1, 2, \cdots, n$.

Let

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \cdots + x_n, \\ \sigma_2 &= \sum_{1\le i_1<i_2\le n} x_{i_1}x_{i_2}, \\ &\cdots\cdots\cdots \\ \sigma_{n-1} &= \sum_{1\le i_1<\cdots<i_{n-1}\le n} \prod_{r=1}^{n-1} x_{i_r}, \\ \sigma_n &= x_1x_2\cdots x_n. \end{aligned}$$

The polynomial $\sigma_k (k = 1, 2, \cdots, n)$ is called the k-th elementary symmetric polynomial in the indeterminates $x_1, x_2, \cdots, x_n$ over R.

Lemma 4.3. *[17, Theorem 1.76, Waring's Formula] Let* $s_0 = n \in \mathbb{Z}$ *and* $s_k = s_k(x_1, x_2, \cdots, x_n) = x_1^k + x_2^k + \cdots + x_n^k \in R[x_1, x_2, \cdots, x_n]$ *for* $k \ge 1$. *Then*

$$s_k = \sum (-1)^{i_2+i_4+\cdots} \frac{(i_1 + i_2 + \cdots + i_n - 1)!k}{i_1!i_2!\cdots i_n!} \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n},$$

where the summation is extended over all n*-tuples* $(i_1, i_2, \cdots, i_n)$ *of nonnegative integers with* $i_1 + 2i_2 + \cdots + ni_n = k$. *The coefficient of* $\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$ *is always an integer.*

Theorem 4.4 gives the necessary and sufficient condition that the polynomial $f(x) = x^3 + x - 1$ is irreducible in $\mathbb{F}_p[x]$. The best choice of $f(x)$ is the Conway polynomial, which is used in computational algebra systems such as MAGMA and GAP to represent finite fields. However, since the choice of p is different, then the Conway polynomial is also different. Therefore, this paper chooses a simple polynomial $x^3 + x - 1$.

Theorem 4.4. *Let* $p \equiv 1 (\mathrm{mod} 6)$. *Then* $f(x) = x^3 + x - 1$ *is irreducible on* $\mathbb{F}_p$ *if and only if*

$$\sum_{s=0}^{\frac{p-1}{6}} (-1)^{3s+1} \frac{C_{\frac{p-1}{3}+s}^{3s}}{\frac{p-1}{3}+s} + \sum_{t=0}^{\frac{p-1}{3}} \frac{C_{\frac{p-1}{3}+2t}^{3t}}{\frac{p-1}{3}+2t} \neq 0 \tag{4.1}$$

in the finite field $\mathbb{F}_p$.

Since the proof of Theorem 4.4 is too long, we place it at the end of the paper so as not to affect the coherence of the contents of this section.

Considering the Frobenius map $\tau(x) = x^p$ of $\mathbb{F}_q$ and the cyclic algebra $\mathcal{A} = (\mathbb{F}_q/\mathbb{F}_p, \tau, 1)$, we have that

$$M_3(\mathbb{F}_p) \simeq \mathcal{A} \simeq \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q, \tag{4.2}$$

with $q = p^3$, $v^3 = 1$, where $\mathbb{F}_q = \mathbb{F}_p[\omega]$ and $\omega^3 + \omega - 1 = 0$. The multiplication is given by $av = v\tau(a)$ for any $a \in \mathbb{F}_q$. From linear algebra, we know that

$$x^p = g(x)f(x) + ax^2 + bx + c \tag{4.3}$$

with $g(x) \in \mathbb{F}_q[x]$, $a, b, c \in \mathbb{F}_q$, i.e., $\omega^p = a\omega^2 + b\omega + c$. The isomorphism $\rho : \mathcal{A} \to M_3(\mathbb{F}_p)$ is given as follows:

$$v \mapsto \begin{pmatrix} 1 & c & c^2 + 2ab \\ 0 & b & a^2 - 2ab + 2bc \\ 0 & a & b^2 - a^2 + 2ac \end{pmatrix}, \omega \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Substituting the three roots $\alpha_1, \alpha_2, \alpha_3$ of $f(x)$ into Eq.(4.3), we get system of linear equations

$$\begin{pmatrix} \alpha_1^2 & \alpha_1 & 1 \\ \alpha_2^2 & \alpha_2 & 1 \\ \alpha_3^2 & \alpha_3 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} \alpha_1^p \\ \alpha_2^p \\ \alpha_3^p \end{pmatrix}.$$

By Cramer's Rule, we have

$$\begin{aligned} a &\equiv \frac{\alpha_1^p}{(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_2)} + \frac{\alpha_2^p}{(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_1)} + \frac{\alpha_3^p}{(\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)} (\mathrm{mod} p), \\ b &\equiv -\frac{\alpha_1^p(\alpha_2 + \alpha_3)}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)} - \frac{\alpha_2^p(\alpha_1 + \alpha_3)}{(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)} - \frac{\alpha_3^p(\alpha_1 + \alpha_2)}{(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_1)} (\mathrm{mod} p), \\ c &\equiv \frac{\alpha_1^{p-1}}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)} + \frac{\alpha_2^{p-1}}{(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)} + \frac{\alpha_3^{p-1}}{(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)} (\mathrm{mod} p). \end{aligned} \tag{4.4}$$

Eq.(4.4) gives explicit expressions of a, b, c as rational symmetric polynomials of $\alpha_1, \alpha_2, \alpha_3$. Table 4.1 shows the values of a, b, c, when $p = 7, 13, 19, 31$. All operations on symmetric polynomials can be done in MAGMA.

Let $\mathcal{R}_q = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$. Then $\mathcal{R}_q$ such that $v^3 - 1 = 0$ is a non-chain principal ideal ring with two maximal ideals $\langle v - 1 \rangle$ and $\langle v^2 + v + 1 \rangle$. The ideal lattice of $\mathcal{R}_q$ is given in the Figure 4.1.

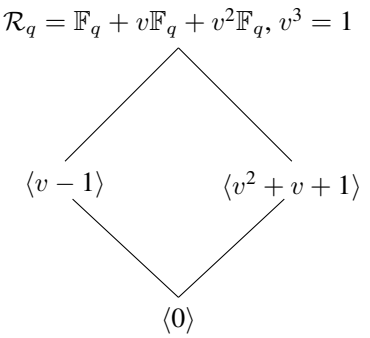

Figure 4.1. The ideal lattice of the ring $\mathcal{R}_q = \mathbb{F}_q[v]/\langle v^3 - 1 \rangle$

For a code C over $\mathcal{R}_q$, we define

$$\begin{aligned} C_1 &= \left\{ c \in \mathbb{F}_q^n \mid a + vb + v^2c \in C, \text{ for some } a, b \in \mathbb{F}_q^n \right\}, \\ C_2 &= \left\{ b - c \in \mathbb{F}_q^n \mid a + vb + v^2c \in C \right\}, \\ C_3 &= \left\{ a - c \in \mathbb{F}_q^n \mid a + vb + v^2c \in C \right\}. \end{aligned} \tag{4.5}$$

If C is a linear code of length n over $\mathcal{R}_q$, then C_1, C_2 and C_3 are all linear codes over length n over $\mathbb{F}_q$. Moreover, the linear code C of length n over $\mathcal{R}_q$ can be uniquely expressed as

$$C = (v^2 + v + 1)C_1 \oplus vC_2 \oplus C_3.$$

A generator matrix of C is a matrix whose rows generate C. Let $C = (v^2+v+1)C_1 \oplus vC_2 \oplus C_3$ be a linear code of length n over $\mathcal{R}_q$ with a generator matrix G. Then G can be written as

$$\begin{pmatrix} (v^2+v+1)G_1 \\ vG_2 \\ G_3 \end{pmatrix},$$

where G_1, G_2, G_3 are the generator matrices of C_1, C_2 and C_3, respectively.

The definitions of Hamming and Lee metric of $\mathcal{R}_q$ are similar to those of Section 2. Hence, we do not repeat them in this section. The Gray map φ from $\mathcal{R}_q$ to $\mathbb{F}_q^3$ is defined by $\varphi(a+vb+v^2c) = (c, b-c, a-c)$. It can be easily checked that φ is a linear map. The Gray map φ can be extended to $\mathcal{R}_q^n$ in a natural way, that is, $\varphi : \mathcal{R}_q^n \to \mathbb{F}_q^{3n}$ such that $\varphi : (r_0, r_1, \cdots, r_{n-1}) \mapsto (a_0, b_0 - c_0, a_0 - c_0, \cdots, a_{n-1}, b_{n-1} - c_{n-1}, a_{n-1} - c_{n-1})$, where $r_i = a_i + vb_i + v^2c_i$ for $i = 0, 1, \cdots, n-1$.

There are some structural results on linear codes over $M_3(\mathbb{F}_p)$. Similarly to Lemma 1 of [16], we have Theorem 4.5. The proofs of Theorems 4.5-4.7 are similar to those of [16, 21]. Thus, we omit the proofs of the results.

Theorem 4.5. *The Gray map φ is a distance-preserving map or isometry from $\mathcal{R}_q^n$ (Lee distance) to $\mathbb{F}_q^{3n}$ (Hamming distance) and it is $\mathbb{F}_q$-linear.*

Theorem 4.6. *If $C = (v^2+v+1)C_1 \oplus vC_2 \oplus C_3$ is a linear code over $\mathcal{R}_q$, then $\varphi(C) = C_1 \otimes C_2 \otimes C_3$ and $|C| = |C_1||C_2||C_3|$.*

Corollary 4.7. *If $C = (v^2+v+1)C_1 \oplus vC_2 \oplus C_3$ is a linear code of length n over $\mathcal{R}_q$, where C_i is a linear code over $\mathbb{F}_q$ with dimension k_i and minimum Hamming distance $d_{Ham}(C_i)$ for $i = 1, 2, 3$, then $\varphi(C)$ is a linear $[3n, k_1+k_2+k_3, \min\{d_{Ham}(C_1), d_{Ham}(C_2), d_{Ham}(C_3)\}]$ code.*

In particular, we have the following result when C is cyclic over $\mathcal{R}_q$.

Theorem 4.8. *Let $C = (v^2+v+1)C_1 \oplus vC_2 \oplus C_3$ be a linear code of length n over $\mathcal{R}_q$. Then C is cyclic over $\mathcal{R}_q$ if and only if C_1, C_2, C_3 are cyclic over $\mathbb{F}_q$.*

Proof. Let $(c_0^{(1)}, c_1^{(1)}, \cdots, c_{n-1}^{(1)}) \in C_1$, $(c_0^{(2)}, c_1^{(2)}, \cdots, c_{n-1}^{(2)}) \in C_2$, $(c_0^{(3)}, c_1^{(3)}, \cdots, c_{n-1}^{(3)}) \in C_3$ and $c_i = (v^2+v+1)c_i^{(1)} + vc_i^{(2)} + c_i^{(3)}$ for $i = 0, 1, 2, \cdots, n-1$. Then the vector $(c_0, c_1, \cdots, c_{n-1}) \in C$. Since C is a cyclic code over $\mathcal{R}_q$, it implies that $(c_{n-1}, c_0, \cdots, c_{n-2}) \in C$. Notice that $(c_{n-1}, c_0, \cdots, c_{n-2}) = (v^2+v+1)(c_{n-1}^{(1)}, c_0^{(1)}, \cdots, c_{n-2}^{(1)}) + v(c_{n-1}^{(2)}, c_0^{(2)}, \cdots, c_{n-2}^{(2)}) + (c_{n-1}^{(3)}, c_0^{(3)}, \cdots, c_{n-2}^{(3)})$, then $(c_{n-1}^{(1)}, c_0^{(1)}, \cdots, c_{n-2}^{(1)}) \in C_1$, $(c_{n-1}^{(2)}, c_0^{(2)}, \cdots, c_{n-2}^{(2)}) \in C_2$ and $(c_{n-1}^{(3)}, c_0^{(3)}, \cdots, c_{n-2}^{(3)}) \in C_3$. It follows that C_1, C_2 and C_3 are cyclic codes over $\mathbb{F}_q$.

Conversely, let C_1, C_2 and C_3 are cyclic over $\mathbb{F}_q$. If $(c_0, c_1, \cdots, c_{n-1}) \in C$, where $c_i = (v^2+v+1)c_i^{(1)} + vc_i^{(2)} + c_i^{(3)}$ for $i = 0, 1, 2, \cdots, n-1$, then $(c_0^{(1)}, c_1^{(1)}, \cdots, c_{n-1}^{(1)}) \in C_1$, $(c_0^{(2)}, c_1^{(2)}, \cdots, c_{n-1}^{(2)}) \in C_2$ and $(c_0^{(3)}, c_1^{(3)}, \cdots, c_{n-1}^{(3)}) \in C_3$. Note that $(c_{n-1}, c_0, \cdots, c_{n-2}) = (v^2+v+1)(c_{n-1}^{(1)}, c_0^{(1)}, \cdots, c_{n-2}^{(1)}) + v(c_{n-1}^{(2)}, c_0^{(2)}, \cdots, c_{n-2}^{(2)}) + (c_{n-1}^{(3)}, c_0^{(3)}, \cdots, c_{n-2}^{(3)}) \in (v^2+v+1)C_1 \oplus vC_2 \oplus C_3 = C$. Therefore, C is cyclic over $\mathcal{R}_q$. □

Table 4.1: The values of a, b, c, when $p = 7, 13, 19, 31$

Finite Field	a, b, c	Elementary Symmetric Polynomials of a, b, c	Values
$\mathbb{F}_7$	a	$\tau_1^5 + 3\tau_1^3\tau_2 + 3\tau_1^2\tau_3 + 3\tau_1\tau_2^2 + 5\tau_2\tau_3$	-2
	b	$6\tau_1^4\tau_2 + \tau_1^3\tau_3 + 3\tau_1^2\tau_2^2 + 3\tau_1\tau_2\tau_3 + 6\tau_2^3 + \tau_3^2$	0
	c	$\tau_1^4\tau_3 + 4\tau_1^2\tau_2\tau_3 + 2\tau_1\tau_2^3 + \tau_2^2\tau_3$	1
$\mathbb{F}_{13}$	a	$\tau_1^{11} + 3\tau_1^9\tau_2 + 9\tau_1^8\tau_3 + 10\tau_1^7\tau_2^2 + 9\tau_1^6\tau_2\tau_3 + 9\tau_1^5\tau_2^3 + 8\tau_1^5\tau_3^2 + \tau_1^4\tau_2^2\tau_3 + 9\tau_1^3\tau_2^4 + 5\tau_1^3\tau_2\tau_3^2 + 5\tau_1^2\tau_2^3\tau_3 + 10\tau_1^2\tau_3^3 + 7\tau_1\tau_2^5 + 4\tau_1\tau_2^2\tau_3^2 + 5\tau_2^4\tau_3 + 9\tau_2\tau_3^3$	1
	b	$12\tau_1^{10}\tau_2 + \tau_1^9\tau_3 + 9\tau_1^8\tau_2^2 + 10\tau_1^7\tau_2\tau_3 + 11\tau_1^6\tau_2^3 + 7\tau_1^6\tau_3^2 + 11\tau_1^5\tau_2^2\tau_3 + 9\tau_1^4\tau_2^4 + 7\tau_1^4\tau_2\tau_3^2 + 11\tau_1^3\tau_2^3\tau_3 + 10\tau_1^3\tau_3^3 + 11\tau_1^2\tau_2^5 + 8\tau_1^2\tau_2^2\tau_3^2 + 12\tau_1\tau_2^4\tau_3 + 10\tau_1\tau_2\tau_3^3 + \tau_2^6 + 3\tau_2^3\tau_3^2 + \tau_3^4$	5

Continued on next page

Table 4.1 – continued from previous page

Finite Field	a, b, c	Elementary Symmetric Polynomials of a, b, c	Values
	c	$\tau_1^{10}\tau_3 + 4\tau_1^8\tau_2\tau_3 + 8\tau_1^7\tau_3^2 + 2\tau_1^6\tau_2^2\tau_3 + 10\tau_1^5\tau_2\tau_3^2 + 4\tau_1^4\tau_2^3\tau_3 + 2\tau_1^4\tau_3^3 + 8\tau_1^3\tau_2^2\tau_3^2 + 2\tau_1^2\tau_2^4\tau_3 + 9\tau_1^2\tau_2\tau_3^3 + 6\tau_1\tau_2^3\tau_3^2 + 4\tau_1\tau_3^4 + 12\tau_2^5\tau_3 + 6\tau_2^2\tau_3^3$	5
$\mathbb{F}_{19}$	a	$\tau_1^{17}+3\tau_1^{15}\tau_2+15\tau_1^{14}\tau_3+10\tau_1^{13}\tau_2^2+8\tau_1^{12}\tau_2\tau_3+16\tau_1^{11}\tau_2^3+2\tau_1^{11}\tau_3^2+3\tau_1^{10}\tau_2^2\tau_3+12\tau_1^9\tau_2^4+5\tau_1^9\tau_2\tau_3^2+15\tau_1^8\tau_2^3\tau_3+13\tau_1^8\tau_3^3+6\tau_1^7\tau_2^5+4\tau_1^7\tau_2^2\tau_3^2+11\tau_1^6\tau_2^4\tau_3+15\tau_1^6\tau_2\tau_3^3+6\tau_1^5\tau_2^6+7\tau_1^5\tau_2^3\tau_3^2+12\tau_1^5\tau_3^4+13\tau_1^4\tau_2^5\tau_3+6\tau_1^4\tau_2^2\tau_3^3+13\tau_1^3\tau_2^7+6\tau_1^3\tau_2^4\tau_3^2+5\tau_1^3\tau_2\tau_3^4+5\tau_1^2\tau_2^6\tau_3+10\tau_1^2\tau_2^3\tau_3^3+2\tau_1^2\tau_3^5+9\tau_1\tau_2^8+3\tau_1\tau_2^5\tau_3^2+10\tau_1\tau_2^2\tau_3^4+11\tau_2^7\tau_3+16\tau_2^4\tau_3^3+13\tau_2\tau_3^5$	2
	b	$18\tau_1^{16}\tau_2+\tau_1^{15}\tau_3+15\tau_1^{14}\tau_2^2+10\tau_1^{13}\tau_2\tau_3+4\tau_1^{12}\tau_2^3+13\tau_1^{12}\tau_3^2+6\tau_1^{11}\tau_2^2\tau_3+\tau_1^{10}\tau_2^4+11\tau_1^{10}\tau_2\tau_3^2+13\tau_1^9\tau_2^3\tau_3+17\tau_1^9\tau_3^3+18\tau_1^8\tau_2^5+2\tau_1^8\tau_2^2\tau_3^2+16\tau_1^7\tau_2^4\tau_3+14\tau_1^7\tau_2\tau_3^3+6\tau_1^6\tau_2^6+9\tau_1^6\tau_2^3\tau_3^2+8\tau_1^6\tau_3^4+8\tau_1^5\tau_2^5\tau_3+6\tau_1^5\tau_2^2\tau_3^3+18\tau_1^4\tau_2^7+9\tau_1^4\tau_2^4\tau_3^2+11\tau_1^4\tau_2\tau_3^4+18\tau_1^3\tau_2^6\tau_3+\tau_1^3\tau_2^3\tau_3^3+16\tau_1^3\tau_3^5+17\tau_1^2\tau_2^8+\tau_1^2\tau_2^5\tau_3^2+11\tau_1^2\tau_2^2\tau_3^4+12\tau_1\tau_2^7\tau_3+17\tau_1\tau_2^4\tau_3^3+2\tau_1\tau_2\tau_3^5+18\tau_2^9+9\tau_2^6\tau_3^2+3\tau_2^3\tau_3^4+\tau_3^6$	-7
	c	$\tau_1^{16}\tau_3 + 4\tau_1^{14}\tau_2\tau_3 + 14\tau_1^{13}\tau_3^2 + 15\tau_1^{12}\tau_2^2\tau_3 + 15\tau_1^{11}\tau_2\tau_3^2 + 18\tau_1^{10}\tau_2^3\tau_3 + 9\tau_1^{10}\tau_3^3 + 14\tau_1^9\tau_2^2\tau_3^2+\tau_1^8\tau_2^4\tau_3+18\tau_1^8\tau_2\tau_3^3+10\tau_1^7\tau_2^3\tau_3^2+6\tau_1^7\tau_3^4+13\tau_1^6\tau_2^5\tau_3+6\tau_1^6\tau_2^2\tau_3^3+6\tau_1^5\tau_2^4\tau_3^2+9\tau_1^5\tau_2\tau_3^4+\tau_1^4\tau_2^6\tau_3+13\tau_1^4\tau_2^3\tau_3^3+13\tau_1^4\tau_3^5+9\tau_1^3\tau_2^5\tau_3^2+9\tau_1^3\tau_2^2\tau_3^4+2\tau_1^2\tau_2^7\tau_3+2\tau_1^2\tau_2^4\tau_3^3+9\tau_1^2\tau_2\tau_3^5+18\tau_1\tau_2^6\tau_3^2+12\tau_1\tau_2^3\tau_3^4+6\tau_1\tau_3^6+\tau_2^8\tau_3+17\tau_2^5\tau_3^3+15\tau_2^2\tau_3^5$	-5
$\mathbb{F}_{31}$	a	$\tau_1^{29}+3\tau_1^{27}\tau_2+27\tau_1^{26}\tau_3+10\tau_1^{25}\tau_2^2+\tau_1^{24}\tau_2\tau_3+4\tau_1^{23}\tau_2^3+21\tau_1^{23}\tau_3^2+18\tau_1^{22}\tau_2^2\tau_3+2\tau_1^{21}\tau_2^4+4\tau_1^{21}\tau_2\tau_3^2+28\tau_1^{20}\tau_2^3\tau_3+4\tau_1^{20}\tau_3^3+28\tau_1^{19}\tau_2^5+27\tau_1^{19}\tau_2^2\tau_3^2+8\tau_1^{18}\tau_2^4\tau_3+4\tau_1^{18}\tau_2\tau_3^3+11\tau_1^{17}\tau_2^6+5\tau_1^{17}\tau_2^3\tau_3^2+2\tau_1^{17}\tau_3^4+24\tau_1^{16}\tau_2^5\tau_3+6\tau_1^{16}\tau_2^2\tau_3^3+18\tau_1^{15}\tau_2^7+24\tau_1^{15}\tau_2^4\tau_3^2+11\tau_1^{15}\tau_2\tau_3^4+24\tau_1^{14}\tau_2^6\tau_3+17\tau_1^{14}\tau_2^3\tau_3^3+3\tau_1^{14}\tau_3^5+6\tau_1^{13}\tau_2^8+14\tau_1^{13}\tau_2^5\tau_3^2+12\tau_1^{13}\tau_2^2\tau_3^4+19\tau_1^{12}\tau_2^7\tau_3+21\tau_1^{12}\tau_2^4\tau_3^3+30\tau_1^{12}\tau_2\tau_3^5+29\tau_1^{11}\tau_2^9+19\tau_1^{11}\tau_2^6\tau_3^2+21\tau_1^{11}\tau_2^3\tau_3^4+7\tau_1^{11}\tau_3^6+13\tau_1^{10}\tau_2^8\tau_3+9\tau_1^{10}\tau_2^5\tau_3^3+14\tau_1^{10}\tau_2^2\tau_3^5+29\tau_1^9\tau_2^{10}+2\tau_1^9\tau_2^7\tau_3^2+17\tau_1^9\tau_2^4\tau_3^4+24\tau_1^9\tau_2\tau_3^6+16\tau_1^8\tau_2^9\tau_3+8\tau_1^8\tau_2^6\tau_3^3+30\tau_1^8\tau_2^3\tau_3^5+18\tau_1^8\tau_3^7+13\tau_1^7\tau_2^{11}+30\tau_1^7\tau_2^8\tau_3^2+29\tau_1^7\tau_2^5\tau_3^4+8\tau_1^7\tau_2^2\tau_3^6+15\tau_1^6\tau_2^{10}\tau_3+9\tau_1^6\tau_2^7\tau_3^3+28\tau_1^6\tau_2^4\tau_3^5+\tau_1^6\tau_2\tau_3^7+19\tau_1^5\tau_2^{12}+10\tau_1^5\tau_2^9\tau_3^2+28\tau_1^5\tau_2^6\tau_3^4+7\tau_1^5\tau_2^3\tau_3^6+16\tau_1^5\tau_3^8+15\tau_1^4\tau_2^{11}\tau_3+10\tau_1^4\tau_2^8\tau_3^3+26\tau_1^4\tau_2^5\tau_3^5+10\tau_1^4\tau_2^2\tau_3^7+29\tau_1^3\tau_2^{13}+22\tau_1^3\tau_2^{10}\tau_3^2+5\tau_1^3\tau_2^7\tau_3^4+13\tau_1^3\tau_2^4\tau_3^6+4\tau_1^3\tau_2\tau_3^8+\tau_1^2\tau_2^{12}\tau_3+6\tau_1^2\tau_2^9\tau_3^3+14\tau_1^2\tau_2^6\tau_3^5+16\tau_1^2\tau_2^3\tau_3^7+24\tau_1^2\tau_3^9+15\tau_1\tau_2^{14}+24\tau_1\tau_2^{11}\tau_3^2+18\tau_1\tau_2^8\tau_3^4+5\tau_1\tau_2^5\tau_3^6+30\tau_1\tau_2^2\tau_3^8+17\tau_2^{13}\tau_3+7\tau_2^{10}\tau_3^3+14\tau_2^7\tau_3^5+20\tau_2^4\tau_3^7+21\tau_2\tau_3^9$	17
	b	$30\tau_1^{28}\tau_2+\tau_1^{27}\tau_3+27\tau_1^{26}\tau_2^2+10\tau_1^{25}\tau_2\tau_3+16\tau_1^{24}\tau_2^3+25\tau_1^{24}\tau_3^2+\tau_1^{23}\tau_2^2\tau_3+6\tau_1^{22}\tau_2^4+9\tau_1^{22}\tau_2\tau_3^2+26\tau_1^{21}\tau_2^3\tau_3+5\tau_1^{21}\tau_3^3+7\tau_1^{20}\tau_2^5+24\tau_1^{20}\tau_2^2\tau_3^2+7\tau_1^{19}\tau_2^4\tau_3+9\tau_1^{19}\tau_2\tau_3^3+14\tau_1^{18}\tau_2^6+10\tau_1^{18}\tau_2^3\tau_3^2+28\tau_1^{18}\tau_3^4+3\tau_1^{17}\tau_2^5\tau_3+20\tau_1^{17}\tau_2^2\tau_3^3+4\tau_1^{16}\tau_2^7+9\tau_1^{16}\tau_2^4\tau_3^2+17\tau_1^{16}\tau_2\tau_3^4+5\tau_1^{15}\tau_2^6\tau_3+13\tau_1^{15}\tau_2^3\tau_3^3+\tau_1^{15}\tau_3^5+30\tau_1^{14}\tau_2^8+7\tau_1^{14}\tau_2^5\tau_3^2+14\tau_1^{14}\tau_2^2\tau_3^4+26\tau_1^{13}\tau_2^7\tau_3+28\tau_1^{13}\tau_2^4\tau_3^3+21\tau_1^{13}\tau_2\tau_3^5+14\tau_1^{12}\tau_2^9+23\tau_1^{12}\tau_2^6\tau_3^2+20\tau_1^{12}\tau_2^3\tau_3^4+19\tau_1^{12}\tau_3^6+5\tau_1^{11}\tau_2^8\tau_3+15\tau_1^{11}\tau_2^5\tau_3^3+23\tau_1^{11}\tau_2^2\tau_3^5+29\tau_1^{10}\tau_2^{10}+8\tau_1^{10}\tau_2^7\tau_3^2+26\tau_1^{10}\tau_2^4\tau_3^4+23\tau_1^{10}\tau_2\tau_3^6+4\tau_1^9\tau_2^9\tau_3+8\tau_1^9\tau_2^6\tau_3^3+6\tau_1^9\tau_2^3\tau_3^5+14\tau_1^9\tau_3^7+14\tau_1^8\tau_2^{11}+22\tau_1^8\tau_2^8\tau_3^2+21\tau_1^8\tau_2^5\tau_3^4+8\tau_1^8\tau_2^2\tau_3^6+28\tau_1^7\tau_2^{10}\tau_3+4\tau_1^7\tau_2^7\tau_3^3+5\tau_1^7\tau_2^4\tau_3^5+10\tau_1^7\tau_2\tau_3^7+7\tau_1^6\tau_2^{12}+8\tau_1^6\tau_2^9\tau_3^2+26\tau_1^6\tau_2^6\tau_3^4+26\tau_1^6\tau_2^3\tau_3^6+11\tau_1^6\tau_3^8+5\tau_1^5\tau_2^{11}\tau_3+22\tau_1^5\tau_2^8\tau_3^3+21\tau_1^5\tau_2^5\tau_3^5+18\tau_1^5\tau_2^2\tau_3^7+9\tau_1^4\tau_2^{13}+4\tau_1^4\tau_2^{10}\tau_3^2+6\tau_1^4\tau_2^7\tau_3^4+17\tau_1^4\tau_2^4\tau_3^6+9\tau_1^4\tau_2\tau_3^8+25\tau_1^3\tau_2^{12}\tau_3+24\tau_1^3\tau_2^9\tau_3^3+10\tau_1^3\tau_2^6\tau_3^5+12\tau_1^3\tau_2^3\tau_3^7+10\tau_1^3\tau_3^9+12\tau_1^2\tau_2^{14}+\tau_1^2\tau_2^{11}\tau_3^2+15\tau_1^2\tau_2^8\tau_3^4+12\tau_1^2\tau_2^5\tau_3^6+26\tau_1^2\tau_2^2\tau_3^8+21\tau_1\tau_2^{13}\tau_3+29\tau_1\tau_2^{10}\tau_3^3+13\tau_1\tau_2^7\tau_3^5+3\tau_1\tau_2^4\tau_3^7+24\tau_1\tau_2\tau_3^9+30\tau_2^{15}+29\tau_2^{12}\tau_3^2+29\tau_2^9\tau_3^4+25\tau_2^6\tau_3^6+21\tau_2^3\tau_3^8+\tau_3^{10}$	11
	c	$\tau_1^{28}\tau_3 + 4\tau_1^{26}\tau_2\tau_3 + 26\tau_1^{25}\tau_3^2 + 15\tau_1^{24}\tau_2^2\tau_3 + 20\tau_1^{23}\tau_2\tau_3^2 + 25\tau_1^{22}\tau_2^3\tau_3 + 28\tau_1^{22}\tau_3^3 + 27\tau_1^{21}\tau_2^2\tau_3^2+24\tau_1^{20}\tau_2^4\tau_3+19\tau_1^{20}\tau_2\tau_3^3+13\tau_1^{19}\tau_2^3\tau_3^2+21\tau_1^{19}\tau_3^4+17\tau_1^{18}\tau_2^5\tau_3+25\tau_1^{18}\tau_2^2\tau_3^3+13\tau_1^{17}\tau_2^4\tau_3^2+23\tau_1^{17}\tau_2\tau_3^4+27\tau_1^{16}\tau_2^6\tau_3+25\tau_1^{16}\tau_2^3\tau_3^3+9\tau_1^{16}\tau_3^5+9\tau_1^{15}\tau_2^5\tau_3^2+9\tau_1^{15}\tau_2^2\tau_3^4+\tau_1^{14}\tau_2^7\tau_3+26\tau_1^{14}\tau_2^4\tau_3^3+16\tau_1^{14}\tau_2\tau_3^5+16\tau_1^{13}\tau_2^6\tau_3^2+15\tau_1^{13}\tau_2^3\tau_3^4+12\tau_1^{13}\tau_3^6+17\tau_1^{12}\tau_2^8\tau_3+6\tau_1^{12}\tau_2^5\tau_3^3+18\tau_1^{12}\tau_2^2\tau_3^5+30\tau_1^{11}\tau_2^7\tau_3^2+10\tau_1^{11}\tau_2^4\tau_3^4+20\tau_1^{11}\tau_2\tau_3^6+2\tau_1^{10}\tau_2^9\tau_3+11\tau_1^{10}\tau_2^6\tau_3^3+18\tau_1^{10}\tau_2^3\tau_3^5+10\tau_1^{10}\tau_3^7+15\tau_1^9\tau_2^8\tau_3^2+5\tau_1^9\tau_2^5\tau_3^4+21\tau_1^9\tau_2^2\tau_3^6+17\tau_1^8\tau_2^{10}\tau_3+\tau_1^8\tau_2^7\tau_3^3+9\tau_1^8\tau_2^4\tau_3^5+29\tau_1^8\tau_2\tau_3^7+14\tau_1^7\tau_2^9\tau_3^2+22\tau_1^7\tau_2^6\tau_3^4+15\tau_1^7\tau_2^3\tau_3^6+22\tau_1^7\tau_3^8+24\tau_1^6\tau_2^{11}\tau_3+16\tau_1^6\tau_2^8\tau_3^3+3\tau_1^6\tau_2^5\tau_3^5+12\tau_1^6\tau_2^2\tau_3^7+29\tau_1^5\tau_2^{10}\tau_3^2+15\tau_1^5\tau_2^7\tau_3^4+5\tau_1^5\tau_2^4\tau_3^6+27\tau_1^5\tau_2\tau_3^8+22\tau_1^4\tau_2^{12}\tau_3+7\tau_1^4\tau_2^9\tau_3^3+30\tau_1^4\tau_2^6\tau_3^5+18\tau_1^4\tau_2^3\tau_3^7+30\tau_1^4\tau_3^9+27\tau_1^3\tau_2^{11}\tau_3^2+13\tau_1^3\tau_2^8\tau_3^4+3\tau_1^3\tau_2^5\tau_3^6+15\tau_1^3\tau_2^2\tau_3^8+19\tau_1^2\tau_2^{13}\tau_3+23\tau_1^2\tau_2^{10}\tau_3^3+21\tau_1^2\tau_2^7\tau_3^5+3\tau_1^2\tau_2^4\tau_3^7+\tau_1^2\tau_2\tau_3^9+27\tau_1\tau_2^{12}\tau_3^2+23\tau_1\tau_2^9\tau_3^4+26\tau_1\tau_2^6\tau_3^6+13\tau_1\tau_2^3\tau_3^8+10\tau_1\tau_3^{10}+\tau_2^{14}\tau_3+15\tau_2^{11}\tau_3^3+30\tau_2^8\tau_3^5+3\tau_2^5\tau_3^7+14\tau_2^2\tau_3^9$	1

The proof of Theorem 4.4

Proof. According to Lemma 4.1, $f(x)$ is irreducible on $\mathbb{F}_p$ if and only if $\text{rank}(A) = p-1$, i.e. $\det(A) \not\equiv 0 (\text{mod} p)$, where A is the $(p-1)\times(p-1)$ matrix,

$$A = \begin{pmatrix} -1 & 1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 & -1 & 1 \\ 1 & 0 & 0 & 0 & 0 & \cdots & -1 & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & -1 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 1 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

Notice that the matrix A is a permutation of the circulant matrix B,

$$A = BP, \tag{4.6}$$

where P is a permutation matrix with ones on the anti-diagonal, and zeros in all other entries,

$$B = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 1 & -1 \\ -1 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 1 \\ 1 & -1 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 1 & -1 & 0 \end{pmatrix}$$

is a right circulant matrix.

Then

$$\det(A)=\det(BP)=\det(B)\det(P).$$

The determinant of the permutation matrix P is $(-1)^{\frac{p-1}{2}}$. Define the associated polynomial $g(x) = x^4 + x^2 - x$. By linear algebra, we have

$$\begin{aligned} \det(B) &= \prod_{j=1}^{p-1}(-\omega_j + \omega_j^2 + \omega_j^4) \\ &= \prod_{j=1}^{p-1}\omega_j \prod_{j=1}^{p-1}(-1 + \omega_j + \omega_j^3) \\ &= -\prod_{j=1}^{p-1}(-1 + \omega_j + \omega_j^3), \end{aligned}$$

where $\omega_j = e^{\frac{2\pi i j}{p-1}}$ and $i = \sqrt{-1}$. Thus,

$$\det(A) = (-1)^{\frac{p-1}{2}}\det(B) = (-1)^{\frac{p+1}{2}}\prod_{j=1}^{p-1}(-1 + \omega_j + \omega_j^3). \tag{4.7}$$

The determinant of A is not equal to 0 if and only if Eq.(4.7) is not zero. Let α_1, α_2 and α_3 be the three roots of $x^3 + x - 1 = 0$ in the algebraic closure $\overline{\mathbb{F}}_p$, then

$$\prod_{j=1}^{p-1}(-1 + \omega_j + \omega_j^3) \equiv \prod_{j=1}^{p-1}\prod_{i=1}^{3}(x_j - \alpha_i)(\text{mod} p). \tag{4.8}$$

By Vieta's Theorem, for $x^{p-1}-1=0$, we have

$$\begin{aligned}
&\sigma_1=\sum_{i=1}^{p-1}\omega_i=0,\\
&\sigma_2=\sum_{1\le i_1<i_2\le p-1}\omega_{i_1}\omega_{i_2}=0,\\
&\cdots\cdots\cdots\\
&\sigma_{p-2}=\sum_{1\le i_1<\cdots<i_{p-2}\le p-1}\prod_{r=1}^{p-2}\omega_{i_r}=0,\\
&\sigma_{p-1}=\omega_1\omega_2\cdots\omega_{p-1}=-1.
\end{aligned}$$

Consequently,

$$\begin{aligned}
\prod_{j=1}^{p-1}\prod_{i=1}^{3}(x_j-\alpha_i)&=\prod_{i=1}^{3}\prod_{j=1}^{p-1}(x_j-\alpha_i)\\
&=\prod_{i=1}^{3}(\sigma_{p-1}-\alpha_i\sigma_{p-2}-\alpha_i^2\sigma_{p-3}\cdots+(-1)^{p-1}\alpha_i^{p-1})\\
&=\prod_{i=1}^{3}(\alpha_i^{p-1}-1)\\
&=(\alpha_1^{p-1}+\alpha_2^{p-1}+\alpha_3^{p-1})-(\alpha_1^{p-1}\alpha_2^{p-1}+\alpha_1^{p-1}\alpha_3^{p-1}+\alpha_2^{p-1}\alpha_3^{p-1})
\end{aligned}\tag{4.9}$$

By Vieta's Theorem, for $x^3+x-1=0$, we have

$$\begin{aligned}
&\tau_1=\alpha_1+\alpha_2+\alpha_3=0,\\
&\tau_2=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=1,\\
&\tau_3=\alpha_1\alpha_2\alpha_3=1.
\end{aligned}$$

Let $\beta_1=\alpha_1\alpha_2,\beta_2=\alpha_1\alpha_3,\beta_3=\alpha_2\alpha_3$, then

$$\begin{aligned}
&\theta_1=\beta_1+\beta_2+\beta_3=1,\\
&\theta_2=\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3=0,\\
&\theta_3=\beta_1\beta_2\beta_3=1.
\end{aligned}$$

According to Lemma 4.3,

$$\begin{aligned}
s_{p-1}^{(1)}&=\alpha_1^{p-1}+\alpha_2^{p-1}+\alpha_3^{p-1}\\
&=\sum_{j_1+2j_2+3j_3=p-1}(-1)^{j_2+1}\frac{(j_1+j_2+j_3-1)!}{j_1!j_2!j_3!}\tau_1^{j_1}\tau_2^{j_2}\tau_3^{j_3}\\
&=\sum_{2j_2+3j_3=p-1}(-1)^{j_2+1}\frac{(j_2+j_3-1)!}{j_2!j_3!}\\
&=\sum_{s=0}^{\frac{p-1}{6}}(-1)^{3s+1}\frac{(\frac{p-1}{3}+s-1)!}{(3s)!(\frac{p-1}{3}-2s)!}\\
&=\sum_{s=0}^{\frac{p-1}{6}}(-1)^{3s+1}\frac{C_{\frac{p-1}{3}+s}^{3s}}{\frac{p-1}{3}+s}.
\end{aligned}\tag{4.10}$$

$$
\begin{aligned}
s_{p-1}^{(2)} &= \beta_1^{p-1} + \beta_2^{p-1} + \beta_3^{p-1} \\
&= \sum_{i_1+2i_2+3i_3=p-1} (-1)^{i_2+1} \frac{(i_1+i_2+i_3-1)!}{i_1!i_2!i_3!} \theta_1^{i_1}\theta_2^{i_2}\theta_3^{i_3} \\
&= \sum_{i_1+3i_3=p-1} (-1) \frac{(i_1+i_3-1)!}{i_1!i_3!} \\
&= -\sum_{t=0}^{\frac{p-1}{3}} \frac{(\frac{p-1}{3}+2t-1)!}{(3t)!(\frac{p-1}{3}-t)!} \\
&= -\sum_{t=0}^{\frac{p-1}{3}} \frac{C_{\frac{p-1}{3}+2t}^{3t}}{\frac{p-1}{3}+2t}.
\end{aligned}
\tag{4.11}
$$

Thus, $f(x) = x^3 + x - 1$ is irreducible over $\mathbb{F}_p[x]$ if and only if $s_{p-1}^{(1)}$ is not equal to $s_{p-1}^{(2)}$. The proof of Theorem 4.4 is done. □

5 Conclusion

In this paper, we prove that $M_3(\mathbb{F}_3)$ is isomorphic to the finite chain ring $\mathcal{R} = \mathbb{F}_{3^3} \oplus u\mathbb{F}_{3^3} \oplus u^2\mathbb{F}_{3^3}$, $u^3 = 0$ and investigate the structure of cyclic codes of length n over $M_3(\mathbb{F}_3)$ by using cyclic algebra. It is shown that every cyclic code of length n over $\mathcal{R}$ is a right principal ideal of $\mathcal{R}_n = \mathcal{R}[x]/\langle x^n - 1\rangle$. We also define the Gray map from $M_3(\mathbb{F}_3)$ to $\mathbb{F}_3^3$. The Gray images of linear codes of length n over $\mathcal{R}$ are linear codes of length $3n$ over $\mathbb{F}_3$ under the map ϕ. Moreover, this paper also studies the structural properties of linear codes over $M_3(\mathbb{F}_p)$, where p is prime and $p \equiv 1(\mathrm{mod}6)$.

Declarations

- **Author Contributions:** All authors contributed to the study conception and design. The idea of this paper is derived from Xuesong Si. The first draft of the manuscript was written by Xuesong Si and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.
- **Conflicts of Interest:** The authors declare no conflicts of interest.
- **Funding:** This work is supported by the Natural Science Foundation of Shandong Province, China (Grant number ZR2019BA011) and the National Natural Science Foundation of China (Grant number 11401285).

References

[1] T. Abualrub, I. Siap. Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. Designs, Codes and Cryptography, 2007, 42: 273-287.

[2] A. Alahmadi, H. Sboui, P. Solé, et al. Cyclic codes over $M_2(\mathbb{F}_2)$. Journal of the Franklin Institute, 2013, 350 (9): 2837-2847.

[3] C. Bachoc. Applications of coding theory to the construction of modular lattices. Journal of Combinatorial Theory, Series A, 1997, 78 (1): 92-119.

[4] S. Bhowmick, S. Bagchi, R. Bandi. Self-dual cyclic codes over $M_2(\mathbb{Z}_4)$. Discussiones Mathematicae - General Algebra and Applications, 2022, 42: 349-362.

[5] T. Blackford. Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discrete Applied Mathematics. 2001, 128 (1): 27-46.

[6] A. Bonnecaze, P. Udaya. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Transactions on Information Theory, 1999, 45 (4): 1250-1255.

[7] K. Chatouh. Linear codes over $\mathfrak{R} = \mathbb{Z}_7(\mathbb{Z}_7 + u\mathbb{Z}_7)(\mathbb{Z}_7 + v\mathbb{Z}_7 + w\mathbb{Z}_7 + vw\mathbb{Z}_7)$. Palestine Journal of Mathematics, 2024, 13(Special Issue III): 55-62.

[8] H. Dinh, S. López-Permouth. Cyclic and negacyclic codes over finite chain rings. IEEE Transactions on Information Theory, 2004, 50 (8): 1728-1744.

[9] H. Dinh, A. Singh, N. Kumar, et al. On constacyclic codes Over $\mathbb{Z}[v]/\langle v^2 - v\rangle$ and their Gray images. IEEE Communications Letters, 2018, 22 (9): 1758-1761.

[10] H. Dinh, A. Gaur, P. Kumar, et. al. Cyclic codes over rings of matrices. Advances in Mathematics of Communications, 2024, 18(4): 1100-1122.

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

[12] M. Greferath, S. Schmidt. Linear codes and rings of matrix. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, Springer, Berlin, 1999, 1719: 160-169.

[13] J. Hammons, P. Kumar, A. Calderbank, et al. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Transactions on Information Theory, 1994, 40: 301-319.

[14] T. Honold. Characterization of finite Frobenius rings. Archiv der Mathematik, 2001, 76 (6): 406-415.

[15] H. Islam, O. Prakash, D. Bhunia. On the structure of cyclic codes over $M_2(\mathbb{F}_p + u\mathbb{F}_p)$. Indian Journal of Pure and Applied Mathematics, 2022, 53 (1): 153-161.

[16] J. Gao. Some results on linear codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$. Journal of Applied Mathematics and Computing. 2015, 47: 473–485.

[17] R. Lidl, H. Niederreiter. Finite fields. Cambridge University Press, 1997.

[18] R. Luo, U. Parampalli. Cyclic codes over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$. Cryptography and Communications, 2018, 10: 1109-1117.

[19] F. Oggier, P. Sole, J. Belfiore. Codes over matrix rings for space-time coded modulations. IEEE Transactions on Information Theory, 2012, 58 (2): 734-746.

[20] J. Pal, S. Bhowmick, S. Bagchi. Cyclic codes over $M_4(\mathbb{F}_2)$. Journal of Applied Mathematics and Computing, 2019, 60, 749–756.

[21] M. Shi, T. Yao, A. Alahmadi, P. Solé. Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E 98. A (8): 1845-1848.

[22] S. Ali, G. Mohammad, P. Sharma, et.al. Structural properties of cyclic codes over the ring $\mathfrak{L}_q[\mathfrak{v}, \mathfrak{w}]/\langle \mathfrak{v}^2 - \alpha^2, \mathfrak{w}^2 - \beta^2\mathfrak{w}, \mathfrak{v}\mathfrak{w} - \mathfrak{w}\mathfrak{v}\rangle$. Palestine Journal of Mathematics, 2024, 13(Special Issue III): 9-19.

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

[24] S. Pattanayak, A. Singh. A class of cyclic codes over the ring $\mathbb{Z}_4[u]/\langle u^2\rangle$ and its Gray image. (preprint) arXiv:1507.04938, 2015.

[25] P. Rai, B. Singh, A. Gupta. Skew cyclic codes over $\mathbb{F}_q[u_1, u_2, \cdots, u_r]/\langle u_i^3 - u_i, u_iu_j - u_ju_i\rangle_{i,j=1}^r$. Palestine Journal of Mathematics, 2024, 13(Special Issue III): 216-229.

[26] W. Scharlau. Quadratic and Hermitian forms. Springer Science & Business Media, 2012.

[27] B. Sethuraman, B. Rajan, V. Shashidha. Full-diversity, high-rate space-time block codes from division algebras. IEEE Transactions on Information Theory, 2003, 49 (10): 2596-2616.

[28] X. Si, C. Niu. On skew cyclic codes over $M_2(\mathbb{F}_2)$. AIMS Mathematics, 2023, 8(10): 24434-24445.

[29] J. Wood. Duality for modules over finite rings and applications to coding theory. American Journal of Mathematics, 1999, 121 (3): 555-575.

[30] J. Wood. Code equivalence characterizes finite Frobenius rings. Proceedings of the American Mathematical Society, 2008, 136 (2): 699-706.

[31] B. Yildiz, S. Karadeniz. Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Designs, Codes and Cryptography, 2011, 58: 221-234.

Author information

Xuesong Si, School of Mathematical Sciences, Liaocheng University, P.R. China.
E-mail: sixuesong0825@163.com

Chuanze Niu, School of Mathematical Sciences, Liaocheng University, P.R. China.
E-mail: niuchuanze@lcu.edu.cn

Received: 2024-05-04
Accepted: 2024-11-07