ISSN 2616-5805 Vol. 5, Issue 1: 89-95, DOI: 10.25236/AJMS.2024.050113

The Primitive Matrix Representation and Symmetric Matrix Representation of Finite Fields

Yuying Ou[1,a], Wenbin Zhang[1,b,*]

[1]Department of Applied Mathematics, Guangzhou Huashang College, Guangzhou, China
[a]1079141032@qq.com, [b]wenb.zh@gmail.com
[*]Corresponding author

Abstract: *In this paper, we consider the matrix representations of the finite field, and show some conclusions of the primitive matrix representation of the finite field on the ground field by using the properties of the cyclotomic polynomial. We obtain the symmetric matrix representation of the finite field $\mathbb{F}_q$ with characteristic 2 by constructing the symmetric matrix, and get the relationship between the symmetric matrix representation and the primitive matrix representation of the finite field $\mathbb{F}_q$.*

Keywords: *Finite field; Primitive matrix representation; Cyclotomic polynomial; Primitive polynomial; Symmetric matrix representation*

1. Introduction

It is well established that the finite field $\mathbb{F}_q$ can be viewed as its ground field $\mathbb{F}_p{}'s$ extended field, where $q = p^n$, p is a prime number, n is a positive integer. Generally, the finite field $\mathbb{F}_q$ can be represented by polynomials and by vectors. Finite fields are widely used in coding theory and cryptography.

The Delsarte and Gabidulin rank metric codes in algebraic coding have been a major research hotspot in algebraic coding in recent decades. However, rank metric codes need to be considered matrices over finite fields and matrix representations over finite fields Willam P. Wardlaw provides a preliminary overview of matrix representations of finite fields recitation and examples [1], E M. Gabidulin and N. I. Pilipchuk elaborated on the matrix representation and primitive matrix representation of finite fields on the basis field preliminary concepts and lemmas also explain that finite fields with feature 2 can be represented by symmetric matrices [2].

In this connection, the article considers the primitive matrix representation of finite field $\mathbb{F}_q$ and the symmetric matrix representation of finite field $\mathbb{F}_{2^n}$. We are interested in the following questions:

Given a finite field $\mathbb{F}_\mathrm{q}$, how to find the primitive matrix representations and the symmetric matrix representations ?

How many primitive and symmetric matrix representations exist in a given finite field $\mathbb{F}_q$?

What is the relationship between its primitive matrix representation and symmetric matrix representation for a given finite field $\mathbb{F}_q$?

Throughout this paper, we note that $q = p^n$, where p is a prime number, n is a positive integer, $\boldsymbol{O_n}$ and I_n denote the $n \times n$ zero matrix and $n \times n$ identity matrix, respectively, and $\mathbb{F}_p^{n\times n}$ denote the $n \times n$ matrix over the finite field $\mathbb{F}_p$.

2. Preliminaries

In this section, we will give some preparatory knowledge, which will be used later in the proof of primitive matrix representation, symmetric matrix representation of finite fields.

2.1. Companion matrix of polynomial

Definition 1 Given the polynomial,

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n \tag{1}$$

the matrix

$$C(f(x)) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix} \tag{2}$$

is called companion matrix of polynomial $f(x)$[3].

2.2. Cyclotomic polynomial

As is well known, for a given positive integer n, $x^n - 1 = 0$ has n roots in the complex field which is of the form $e^{\frac{2k\pi i}{n}}(k = 1,2,\cdots,n)$. If we note $\varepsilon = e^{\frac{2\pi i}{n}}$, then $\varepsilon, \varepsilon^2, \cdots, \varepsilon^n$ are all complex roots of $x^n - 1 = 0$[5], thus

$$x^n - 1 = \prod_{k=1}^{n}(x - \varepsilon^k) \tag{3}$$

For the n-th unit root ω, the order of ω is defined as the smallest positive integer k that satisfies ω^k =1, and denoted by $\mathrm{ord}(\omega)$. Thus $\mathrm{ord}(\varepsilon) = n$, $\mathrm{ord}(\varepsilon^k) = \frac{n}{(n,k)}$. The n-th unit root of order n is called the n-th primitive unit root. Obviously, when $(n, k) = 1$, $\mathrm{ord}(\varepsilon^k) = n$, that is, ε^k is the n-th primitive unit root. Therefore there are $\varphi(n)$ of nth primitive unit roots, where $\varphi(n)$ is the Euler function.

Let $E_n = \{k\,|1 \le k \le d, (k,n) = 1\}$, $k \in E_n$,we can obtain $\mathrm{ord}\,(\varepsilon^k) = n$. We define the n order partial cyclotomic polynomial as the polynomial which is determined by all n-order primitive unit roots. That is,

$$\Phi_n(x) = \prod_{k\in E_n}(x - \varepsilon^k) \tag{4}$$

Since E_n is a set of positive integers which are prime to n and do not exceed n, therefore $\deg\Phi_n(x) = \varphi(n)$. According to the definition of $\Phi_n(x)$, it is easy to know

$$\Phi_1(x)=x - 1 \tag{5}$$

$$\Phi_2(x)=x + 1 \tag{6}$$

$$\Phi_3(x)=x^2 + x + 1 \tag{7}$$

$$\Phi_4(x)=x^2 + 1 \tag{8}$$

$$\Phi_6(x)=x^2 - x + 1 \tag{9}$$

The following theorem summarizes a straightforward property of the cyclotomic polynomial:

Theorem 1[4](Theorem 31.1)

$$x^n - 1 = \prod_{d|n}\Phi_d(x) \tag{10}$$

From this theorem, it can be immediately obtained,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,d<n}\Phi_d(x)} \tag{11}$$

$$\Phi_q(x)=\frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} \tag{12}$$

where $q = p^m$, p is a prime, m is a positive number.

From the definition of the cyclotomic polynomial, we knew the polynomial $\Phi_{q-1}(x) = \prod_{k\in E_{q-1}}(x - \varepsilon^k)$, which is determined by all $(q-1)$-th primitive unit roots. Assuming that $f(x)$ is an irreducible factor of $\Phi_{q-1}(x)$ and α is a root of $f(x)$.Then α is a $(q-1)$-th primitive unit root, as a consequence $f(x)$ is a primitive polynomial over the finite field $\mathbb{F}_q$.

2.3. Some auxiliary matrices

Let $D_n(x)$ and $H_n(x)$ be the three-diagonal $n \times n$ matrices over the finite field $\mathbb{F}_p$, and they are defined as follows:

$$D_n(x) = \begin{bmatrix} x & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & x & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & x & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & x & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & x & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & x \end{bmatrix} \tag{13}$$

$$H_n(x) = \begin{bmatrix} x & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & x & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & x & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & x & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & x & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & x+1 \end{bmatrix} \tag{14}$$

The determinant of the two matrices is denoted by $d_n(x)$ and $h_n(x)$ respectively. Obviously, $d_1(x) = x, h_1(x) = x + 1$, and set $d_0(x) = 1, h_0(x) = 1$.

3. Primitive matrix representation of finite fields

In this section, we give the concept of matrix representation and primitive matrix representation of finite fields through an example, and obtain two corollaries through Lemma 1 of [2].

Example 1 Matrix representation of the finite field $\mathbb{F}_8$.

Since $x^3 + x^2 + 1$ is an irreducible polynomial over $\mathbb{F}_2$, $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3 + x^2 + 1)$. Let θ is a root of $x^3 + x^2 + 1$, then $\theta^3 = \theta^2 + 1, \theta^4 = \theta^2 + \theta + 1, \theta^5 = \theta + 1, \theta^6 = \theta^2 + \theta, \theta^7 = 1$.

Accordingly,

$$\begin{aligned} \mathbb{F}_8 &= \{0,1,\theta,\theta^2,\theta^3,\theta^4,\theta^5,\theta^6\} \\ &= \{0,1,\theta,\theta^2,\theta^2+1,\theta^2+\theta+1,\theta+1,\theta^2+\theta\} \end{aligned} \tag{15}$$

Take $\{1,\theta,\theta^2\}$ as a basis of $\mathbb{F}_8$ and any element a in $\mathbb{F}_8$. The element a's right multiplication linear transformation is denoted as $\mathrm{R_a}$, then we can calculate the corresponding matrix of each element a in $\mathbb{F}_8$ under the basis $\{1,\theta,\theta^2\}$ and the action of the right multiplication linear transformation $\mathrm{R_a}$. When we take the elements of $\mathbb{F}_8$ in turn, the corresponding matrix is obtained as below:

$$\boldsymbol{M}_0 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \boldsymbol{M}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \boldsymbol{M}_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \boldsymbol{M}_3 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$
$$\boldsymbol{M}_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \boldsymbol{M}_5 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \boldsymbol{M}_6 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \boldsymbol{M}_7 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

In view of the right multiplication linear transformation $R_a\colon\ a \to M$, where M is a 3×3 matrix over the finite field $\mathbb{F}_2$, is injective function and keep it addition and multiplication, the right multiplication linear transformation $\mathrm{R_a}$ is an isomorphic mapping. Thus $\{M_i | 0 \le i \le 7\} \cong \mathbb{F}_8$. We obtain a matrix representation of finite field $\mathbb{F}_8$.

Then we can give the definition of the matrix representation of the extended field $\mathbb{F}_q$ over its ground field $\mathbb{F}_p$ below.

Definition 1 The finite field $\mathbb{F}_\mathrm{q}$ is isomorphism to $\mathbb{F}_p[A] = \{f(A) | f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0 \in \mathbb{F}_p[x], A \in \mathbb{F}_p^{n\times n}\}$, the matrix A is called the matrix representation of the finite field $\mathbb{F}_q$.

Note that in Example 1 above, if we let $\boldsymbol{A} = \boldsymbol{M}_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$,then

$$\boldsymbol{A}^2 = \boldsymbol{M}_3, \boldsymbol{A}^3 = \boldsymbol{M}_4, \boldsymbol{A}^4 = \boldsymbol{M}_5, \boldsymbol{A}^5 = \boldsymbol{M}_6, \boldsymbol{A}^6 = \boldsymbol{M}_7, \boldsymbol{A}^7 = \boldsymbol{M}_1 = \boldsymbol{I}_3.$$

Therefore,

$$\{\boldsymbol{M}_i | 0 \le i \le 7\} = \{\boldsymbol{O}_3, \boldsymbol{I}_3, \boldsymbol{A}, \boldsymbol{A}^2, \boldsymbol{A}^3, \boldsymbol{A}^4, \boldsymbol{A}^5, \boldsymbol{A}^6\}$$
$$\cong \{0, 1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6\} = \mathbb{F}_8 \tag{16}$$

Naturally, as way as the definition of primitive elements of finite fields, we can give the primitive matrix representation of the extended field $\mathbb{F}_q$ over its ground field $\mathbb{F}_p$.

Definition 2 $\mathbb{F}_q^*$ is isomorphic to $\{\boldsymbol{I}_n, \boldsymbol{A}, \boldsymbol{A}^2, \cdots, \boldsymbol{A}^{q-1}\}$, where $\boldsymbol{A}$ is a $n \times n$ matrix over $\mathbb{F}_p$, the matrix $\boldsymbol{A}$ is called the primitive representation of the extended field $\mathbb{F}_q$.

From the matrix representation of finite fields and the definition of primitive matrix representation, the following conclusion can be obtained.

Theorem 2 If $\boldsymbol{A}$ is a primitive matrix representation of $\mathbb{F}_q$, then a matrix similar to $\boldsymbol{A}$ must be a matrix representation of $\mathbb{F}_q$.

Proof Assume that $\boldsymbol{A}$ is similar to $\boldsymbol{B}$, then there is an invertible matrix $\boldsymbol{Q} \in \mathbb{F}_p^{n\times n}$, such that $\boldsymbol{A} = \boldsymbol{Q}^{-1}\boldsymbol{B}\boldsymbol{Q}$. Since A is the primitive matrix representation of finite field $\mathbb{F}_q$, then

$$\mathbb{F}_q^* \cong \langle \boldsymbol{A} \rangle = \{\boldsymbol{I}, \boldsymbol{A}, \boldsymbol{A}^2, \cdots, \boldsymbol{A}^{q-2}\} = \{\boldsymbol{I}, \boldsymbol{Q}^{-1}\boldsymbol{B}\boldsymbol{Q}, \boldsymbol{Q}^{-1}\boldsymbol{B}^2\boldsymbol{Q}, \cdots, \boldsymbol{Q}^{-1}\boldsymbol{B}^{q-2}\boldsymbol{Q}\} \tag{17}$$

Hence, $\mathbb{F}_q \cong \{\boldsymbol{O}, \boldsymbol{I}, \boldsymbol{Q}^{-1}\boldsymbol{B}\boldsymbol{Q}, \boldsymbol{Q}^{-1}\boldsymbol{B}^2\boldsymbol{Q}, \cdots, \boldsymbol{Q}^{-1}\boldsymbol{B}^{q-2}\boldsymbol{Q}\}$. Thus, B is a matrix representation of $\mathbb{F}_q$.

Theorem 3 ((Gabidulin & Pilipchuk, 2004), Lemma 1) A representation of $\mathbb{F}_q$ by $\boldsymbol{A}$ is primitive if and only if its characteristic polynomial $\det(x\boldsymbol{I_n} - \boldsymbol{A})$ coincides with a primitive polynomial $f(x)$ of degree n over $\mathbb{F}_p$, where

$$f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0 \tag{18}$$

Corollary 1 Assume that $\boldsymbol{A}$ is a matrix representation of the finite field $\mathbb{F}_q$, then $\boldsymbol{A}$ is the primitive representation of the finite field $\mathbb{F}_q$ if and only if $\boldsymbol{A}$ is a companion matrix of monic polynomial $f(x)$ of degree n,where $f(x)$ is an irreducible factor of $\Phi_{q-1}(x)$.

Proof Let $f(x)$ is a monic polynomial of degree n and a irreducible factor of $\Phi_{q-1}(x)$. The form of $f(x)$ is

$$f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0 \tag{19}$$

then $f(x)$ is a primitive polynomial of the finite field $\mathbb{F}_q$,whose companion matrix is

$$C(f(x)) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -f_{n-2} \\ 0 & 0 & \cdots & 1 & -f_{n-1} \end{bmatrix} \tag{20}$$

It's easy to see

$$\det\left(xI_n - C(f(x))\right) = f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0 = f(x) \tag{21}$$

Thus, from the necessary and sufficient condition of theorem 3, we obtain this proposition.

If the similar primitive matrix representations of the finite field $\mathbb{F}_q$ are regarded as one, the following corollary can be obtained.

Corollary 2 The number of the primitive matrix representations of the finite field $\mathbb{F}_q$ is $\frac{1}{n}\varphi(q-1)$.

Proof From theorem 3,it can be known that the primitive matrix representation of the finite field

$\mathbb{F}_q = \mathbb{F}_{p^n}$ has a one-to-one correspondence with the primitive polynomial of degree n in the ring $\mathbb{F}_p[x]$. There are $\frac{1}{n}\varphi(q-1)$ primitive polynomials of degree n in the ring $\mathbb{F}_p[x]$.The proposition is proved.

4. Symmetric matrix representation of finite field $\mathbb{F}_q$

In this section, we investigate the calculation method of the symmetric matrix representation of finite field $\mathbb{F}_q$ and the relationship between symmetric matrix representation and primitive matrix representation. The characteristic of the finite field $\mathbb{F}_p$ in this section is two.

Definition 3 An $n \times n$ symmetric matrix $\boldsymbol{A}$ over $\mathbb{F}_p$ can represent a finite field $\mathbb{F}_q$, $\boldsymbol{A}$ is called to be a symmetric matrix representation of the finite field $\mathbb{F}_q$.

Theorem 4[2] (, Theorem 1)

Let
$$f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0 \tag{22}$$
be an arbitrary monic polynomial of degree n over $\mathbb{F}_p$, then there exists a symmetric matrix $\boldsymbol{A} \in \mathbb{F}_p^{n\times n}$ for which $f(x)$ is the characteristic polynomial.

Corollary 3 Let $\boldsymbol{A} \in \mathbb{F}_p^{n\times n}$, if the characteristic polynomial of a symmetric matrix $\boldsymbol{A}$ is a primitive polynomial over $\mathbb{F}_p$, then $\boldsymbol{A}$ is the primitive matrix representation of the finite field $\mathbb{F}_q$, and $\boldsymbol{A}$ is similar to the companion matrix of its characteristic polynomial.

Proof Assume that $f(x)$ is a primitive polynomial of degree n over $\mathbb{F}_p$, where
$$f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0 \tag{23}$$
From theorem 2, when $\det(x\boldsymbol{I}_n - \boldsymbol{A})$ is equal to $f(x)$, then $\boldsymbol{A}$ is the primitive matrix representation of the finite field $\mathbb{F}_q$.

From Corollary 1, $\det\left(x\boldsymbol{I}_n - C\big(f(x)\big)\right)$ is equal to $f(x)$. In this way, $\det(x\boldsymbol{I}_n - \boldsymbol{A})$ is equal to $\det\left(x\boldsymbol{I}_n - C\big(f(x)\big)\right)$. Since $f(x)$ is a primitive polynomial, the invariant factors of the matrix $x\boldsymbol{I}_n - \boldsymbol{A}$ and the companion matrix $x\boldsymbol{I}_n - C\big(f(x)\big)$ are the same, and are $1,1,\cdots,1,f(x)$. Thus $\boldsymbol{A}$ is similar to $C\big(f(x)\big)$. The proposition is proved.

For example, the 3×3 symmetric matrix $\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ over $\mathbb{F}_2$, its characteristic polynomial is $x^3 + x + 1$.We know the polynomial $x^3 + x + 1$ is a primitive polynomial of degree two over $\mathbb{F}_2$. Consequently, $\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ is a symmetric representation and a primitive representation of $\mathbb{F}_{2^3} = \mathbb{F}_8$.

Nevertheless, there is great uncertainty by judging whether the characteristic polynomial of a symmetric matrix is a primitive polynomial or not. Hence, we need a more direct method to find the symmetric matrix representation of a finite field.

In line with the proof of theorem 4, the symmetric matrix representation $\boldsymbol{A}$ of the finite field $\mathbb{F}_q$ has the following form:

$$\boldsymbol{A} = \begin{bmatrix} a_{n-1} & b_{n-2} & b_{n-3} & b_{n-4} & \cdots & b_2 & b_1 & b_0 \\ b_{n-2} & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ b_{n-3} & 1 & 0 & 1 & \cdots & 0 & 0 & 0 \\ b_{n-4} & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b_2 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ b_1 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 \\ b_0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{bmatrix} \tag{24}$$

Where $a_{n-1}, a_{n-2} = b_{n-2}^2, a_{n-3} = b_{n-3}^2, \cdots, a_0 = b_0^2 \in \mathbb{F}_p$, and satisfy the following two equations,

$$\begin{aligned}(xh_{n-1}(x), h_{n-1}(x), h_{n-2}(x), d_1(x)h_{n-3}(x), \dots, d_{n-3}(x)h_1(x), d_{n-2}(x))^T \\ = L_{n+1}(x^n, x^{n-1}, x^{n-2}, \dots, x, 1)^T\end{aligned} \tag{25}$$

$$(1, a_{n-1}, a_{n-2}, \dots, a_1, a_0) = (1, f_{n-1}, f_{n-2}, \dots, f_1, f_0)L_{n+1}^{-1} \tag{26}$$

Here L_{n+1} is a $(n+1) \times (n+1)$ matrix over $\mathbb{F}_p$, and the elements of each row consist of the coefficients of the corresponding polynomial on the left side of equation (22).

In particular, when $\mathbb{F}_p = \mathbb{F}_2$, since the square of any element on $\mathbb{F}_2$ is equal to itself, then

$$a_{n-2} = b_{n-2}, a_{n-3} = b_{n-3}, \cdots, a_0 = b_0 \tag{27}$$

Thus, for a given primitive polynomial over the finite field $\mathbb{F}_p$,

$$f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_2x^2 + f_1x + f_0 \tag{28}$$

We get the way to compute the symmetric matrix representation of the finite field $\mathbb{F}_q$:

The first step, compute the determinant

$$|xh_{n-1}(x), h_{n-2}(x), \dots, h_1(x), h_0(x), d_1(x), d_2(x), \dots, d_{n-2}(x)| \tag{29}$$

the second step, by formula (22) the matrix L_{n+1} can be obtained, and L_{n+1}^{-1} is also obtained; the third step, by formula (23) we obtain $a_{n-1}, a_{n-2}, \dots, a_1, a_0$; the fourth step, get the symmetric matrix $\boldsymbol{A}$ according to $a_{n-1}, a_{n-2}, \dots, a_1, a_0$ obtained in the third step.

Simultaneously, we can also give the number of symmetric matrix representations of finite field obtained by the above method.

Theorem 5 The number of the symmetric matrix representations of the finite field $\mathbb{F}_q$ is $\frac{1}{n}\varphi(q-1)$.

Proof From theorem 4, for a given polynomial there is a uniquely determined symmetric matrix corresponding to it, and when the polynomial is a primitive polynomial of $\mathbb{F}_p$, the corresponding symmetric matrix is a symmetric matrix representation of the finite field $\mathbb{F}_q$. The different polynomial has different companion matrices, and from Corollary 2, the corresponding symmetric matrices are also dissimilar to each other.

In this way, the symmetric matrix representation of the finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$ has a one-to-one correspondence with the primitive polynomial with degree of$n$ in the polynomial ring $\mathbb{F}_p[x]$. There are $\frac{1}{n}\varphi(q-1)$ primitive polynomials with degree n the polynomial ring $\mathbb{F}_p[x]$, and the proposition is proved.

From Theorem 5, we can calculate the number of symmetric matrix representations of some finite field $\mathbb{F}_q$ when $p = 2$, and show in table 1.

Table 1: The number of symmetric matrix representations of finite field $\mathbb{F}_{2^n}$.

n	The number of symmetric matrix representations $\frac{1}{n}\varphi(2^n-1)$	n	The number of symmetric matrix representations $\frac{1}{n}\varphi(2^n-1)$
2	1	7	18
3	2	8	16
4	2	9	48
5	6	10	60
6	6	20	24000

5. Conclusion

In this paper, we give the primitive matrix representation of a finite field over its ground field by using the cyclotomic polynomial. The obtained conclusions are quite convenient. The method can be used to calculate the symmetric matrix representation of any finite field with characteristic 2. At the same time, the relationship between the symmetric matrix representation and the primitive matrix representation is showed. These provide a convenient way for further research on Delsarte and Gabidulin rank metric codes.

Acknowledgment

This paper was supported by the "Guangzhou Huashang College 2021 Linear Algebra First-Class Offline Course in 2021" (HS2021YLKC05) and "School level Quality Project for Higher Education Teaching Reform" (HS2021ZLGC31).

References

[1] Wardlaw, W.P. Matrix Representation of Finite Fields [J]. Mathematics Magazine, 1994, 67(4): 289-293.

[2] Gabidulin, E.M. and Pilipchuk, N.I. Symmetric Rank Codes [J]. Problems of Information Transmission, 2004, 40(2): 104-117.

[3] Gallian, J. A. Contemporary Abstract Algebra (Tenth edition) [M]. Crc press, 2021.

[4] Augot, D., Loidreau, P., and Robert, G. Generalized Gabidulin codes over fields of any characteristic [J], Des. Codes Cryptogr, 2018, 86(8): 1807–1848.

[5] Wan, Z.X. Lectures on Finite Fields and Galois Rings [M]. Penguin, 2003.