N° d'ordre: 35/ 2022-C/ MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENNE

FACULTÉ DE MATHÉMATIQUES

THESE DE DOCTORAT

PRÉSENTÉE POUR L'OBTENTION DU GRADE DE DOCTEUR

En : Mathématiques

Spécialité : Arithmétique, codage et combinatoire

Présentée par : **BOUGUEBRINE SOUFYANE**

Intitulée :

Primitive Polynomials and Applications to BCH Codes

Soutenue publiquement le 22/03/2022, devant le jury composé de :

M.	Belbachir Hacène	Professeur à USTHB	Président
M.	Cherchem Ahmed	Professeur à USTHB	Directeur de thèse
Mme.	Benferhat Leila	Professeur à USTHB	Examinatrice
M.	Boumahdi Rachid	MCA à ESI	Examinateur
M.	Abchiche Mourad	MCB à USTHB	Invité
M.	Maouche Youcef	MCB à USTHB	Invité

Acknowledgment

First and foremost, I would like to express my sincere appreciation and respect to my supervisor, Professor ***Cherchem Ahmed****, for all of his assistance, patience, and moral support that he has shown me during this work. The words are certainly not enough to express my gratitude to him, for all the efforts of his.*
I express my deepest gratitude to Professor ***Belbachir Hacène****, for giving me the honor of chairing my jury for this thesis despite his business.*
I also express my sincere thanks to Professor ***Benferhat Leila****, for showing interest in my work by agreeing to examine and evaluate my thesis.*
My thanks also go to Doctor ***Boumahdi Rachid****, for being a member of my jury as my examiner.*
I want to express my gratitude to my teacher, Doctor ***Abchiche Mourad****, for accepting to be my guest of my thesis defense. He deserves to be thanked for all that he taught us, his encouragement and his precious advice. May he find my eternal respect here.*
I want to thank my colleague, Doctor ***Maouche Youcef****, for accepting to be my guest of my thesis defense.*
Big thank you to my brothers and colleagues at the university, in particular, Doctor ***Manaa Abderrahmen****,* ***Rehouma Imene****,* ***Mansouri Charaf Eddine****,* ***Souakri Roufaida****,* ***Cherih Nour El Houda****,* ***Zouilekh Belkacem*** *and* ***Salhi Celia****, for their invaluable support, sage advice and observations, as well as the precious moments we spent during our PhD journey. To my roommates,* ***Smati Ramzi*** *and* ***Ben Naidja Tarek****.*
Finally, my last words of thanks go naturally to my beloved family and friends.

CONTENTS

NOTATIONS

$\mathbb{Z}$	Ring of integers
$\mathbb{F}_q$	Finite field of q elements
$\mathbb{F}_q^*$	Cyclic group of nonzero elements of $\mathbb{F}_q$
$\mathbb{F}_q^n$	Vector space over $\mathbb{F}_q$ of dimension n
$\mathbb{F}_q[x]$	Polynomial ring over $\mathbb{F}_q$
$\mathbb{F}_q(\alpha)$	Smallest extension of $\mathbb{F}_q$ containing both $\mathbb{F}_q$ and α
$\mathbb{F}_q[\mathbf{U}]$	Smallest extension of $\mathbb{F}_q$ containing both $\mathbb{F}_q$ and the matrix $\mathbf{U}$
$\mathrm{ord}(\alpha)$	Multiplicative order of α in $\mathbb{F}_q^*$
$\mathrm{ord}_e(q)$	Multiplicative order of q modulo e
$\mathrm{Tr}_{q^m\|q}$	Trace function from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$
Tr_q	Absolute Trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$
φ	Frobenius automorphism
$\mathrm{Mat}_{r\times r}(\mathbb{F}_q)$	Ring of matrices of size $r \times r$ with coefficients in $\mathbb{F}_q$
$\mathrm{Min}(\alpha, \mathbb{F}_q)(x)$	Minimal polynomial of α over $\mathbb{F}_q$
$[\mathbb{F}_{q^n} : \mathbb{F}_q]$	Degree of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$

INTRODUCTION

The theory of finite fields is a branch of modern algebra that has applications in various areas of theoretical and applied mathematics. Its origins can be traced back into the 17th and 18th century, with the work of Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813), and Adrien-Marie Legendre (1752-1833) contributing to the structure of a special finite fields, the so-called finite prime fields. The general theory of finite fields may be said to begin with the work of Carl Friedrich Gauss (1777-1855) and Evariste Galois (1811-1832), but it only became of interest for applied mathematicians in recent decades with the emergence of discrete mathematics as a serious discipline.

The theory of polynomials over finite fields is important for investigating the algebraic structure of finite fields as well as for many applications. For example, every mapping of a finite field can be expressed as a polynomial, which is an immediate consequence of the Lagrange interpolation formula.

A central problem about polynomials over finite fields is to construct irreducible polynomials over a given finite field.

Irreducible polynomials, considered as the prime elements of the polynomial ring over a finite field, are fundamental objects in the theory of finite fields, since they are needed to construct extensions of finite fields and to compute with their elements.

A polynomial of positive degree is irreducible if it allows only trivial factorizations, other wise it is reducible. The reducibility or irreducibility of a given polynomial depends heavily on the field under consideration. For instance, the binomial $x^2 + 1$ is irreducible over the field of real numbers $\mathbb{R}$, but $x^2 + 1 = (x - i)(x + i)$ is reducible over the field of complex numbers $\mathbb{C}$.

Their interest in theoretical aspects often appears in number theory, combinatorics and algebraic geometry (see, e.g., [20],[24],[28],[38]). For example, every polynomial over a finite field can be written as a product of irreducible polynomials, over the same finite field, in an essentially unique manner. In practical applications, they are widely used in coding theory, cryptography, complexity theory and computer science (see, e.g., [22],[26],[37]). For instance, they are used to construct minimal and maximal cyclic codes. A good introduction to this topic is Reference [24], where a detailed survey can be found at the end of Chapter 3.

One class of irreducibles of great importance is that of primitive polynomials, that is polynomials which have as roots primitive elements of a finite field, or in other words, polynomials with maximum order. These polynomials are also widely used in cryptography and coding theory (see, e.g., [10],[17],[18],[19]). For example, they are related to linear recurring sequences with maximum period, and it is well known that this is important for cryptographic applications. They are also used to construct maximum distance separable (MDS) codes [12].

According to [28], known constructions of irreducible polynomials depend on the composition of an initial irreducible polynomial with a further polynomial or rational function.

Often this process can be iterated or continued recursively to produce an infinite sequence of irreducible polynomials of increasing degrees.

Irreducible composition of certain types were studied by many authors. Agou [3] has established a criterion for $f(g(x))$ to be irreducible over a finite field $\mathbb{F}_{p^s}$, where p is prime. This criterion was used in Agou([3],[4], [5],[6]) to characterize irreducible polynomials of special types such as $f(x^{p^r} - ax)$, $f(x^{p^{2r}} - ax^{p^r} - bx)$ and others. Such irreducible compositions of polynomials are also studied in Cohen ([15],[16]), Long [25], and Ore [30].

Irreducibility criteria for compositions of polynomials of the form $f(x^s)$ have been established by Agou ([2],[3]), Butler [11], Cohen [16], Pellet [31], Petterson [32], and Serret ([34],[35]).

Cohen [15] established a result to construct new irreducible poynomials using the compos ition method. More recently, various constructions and recurrent sequences of irreducible polynomials were established using this technique (see, e.g., [1],[7],[23],[27]).

It should be noted that these constructions involve only irreducible polynomials over the same finite field $\mathbb{F}_q$, while in the present work we are interested in the construction of irreducible polynomials over $\mathbb{F}_q$ from a given irreducible polynomial over an extension of $\mathbb{F}_q$.

As we pointed out before, finite fields have very important applications in error-correcting codes theory. This theory is considered to have originated in 1948 with Claude Shannon and his landmark paper: A mathematical theory of communication [36], that signified the beginning of both information theory and coding theory. Among all types of codes, cyclic codes, which are linear codes, are the most studied codes since they are easy to understand and to encode. They are the building blocks for many other codes, such as the Kerdock, Preparata and Justesen codes. We refer the reader to references [22] and [26] for basic concepts about these codes. Cyclic codes are first studied by Prange [33] in 1957. Since then, the study of these codes is experiencing enormous progress. They contain the most efficient codes, such as Hamming and Reed-Solomon codes. Another important cyclic codes are the BCH codes. These codes, were introduced by R. Bose and D.K. Ray-Chaudhuri [9] in 1960, and independently by A. Hocquenghem [21] in 1959 in the binary case, form an important class of cyclic error-correcting codes. They are very powerful codes since for any positive integer d, we can construct a BCH code of minimum distance greater or equal to d. BCH codes are of great practical importance for error correction in communication systems, storage devices and consumer electronics, particularly if the expected number of errors is small compared with the length of the code (see, e.g., [22], [26]). Since we are dealing with irreducible and primitive polynomials, we are led to investigate some applications to BCH codes.

The present work is devoted to two constructions of irreducible (resp. primitive) polynomials over $\mathbb{F}_q$ of degree rm from irreducible (resp. primitive) polynomials over $\mathbb{F}_{q^m}$ of degree r. As an application, a characterization of the generator polynomial of a BCH code is given. Then, we show how two BCH codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$,respectively, and their generator polynomials are related.

This thesis is structured as follows.

Chapter 1

This chapter contains the preliminaries and definitions that we will use throughout this work.

Chapter 2

In this chapter, we present the first construction of irreducible polynomials through the Frobenius automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. In fact, this coincides with the *spin of a polynomial* introduced by Mullin et al. in [29]. We would like to notice here that our representation turns out to be useful through the properties of the Frobenius automorphism extended to the ring of polynomials.

Chapter 3

In this chapter, we present the second construction which is based on the notion of companion matrix. This construction is basically the same as the one proposed in [13] for primitive polynomials. We show that this construction works also for irreducible polynomials, and in fact, it is the same as the first one. The advantage of this construction is that one can generate multiple irreducible polynomials over $\mathbb{F}_q$ of degree rm from an irreducible polynomial over $\mathbb{F}_{q^m}$ of degree r. Furthermore, all such polynomials can be obtained if a primitive polynomial over $\mathbb{F}_{q^m}$ of degree r is provided.

Chapter 4

As an application of our results, in this last chapter we obtain a characterization of the generator polynomial of a BCH code, and a relation between two BCH codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively. Then, we show how the generator polynomials of the previous two codes are related.

All computations in this work are done using the software SageMath Version 8.8.

CHAPTER 1

PRELIMINARIES

In this chapter, some concepts and definitions are introduced which can be found in [24]. Throughout this work, we consider only *monic polynomials*, i.e., the polynomials with leading coefficient is equal to 1.

1.1 Finite Fields

The theory of finite fields is a branch of modern algebra that has come to the fore in the last fifty years because of its diverse applications in combinatorics, coding theory and the mathematical study of switching circuits among others.

Definition 1.1. A *finite field* is a field with a finite number of elements.

Example 1.1. For every prime p, the residue class ring

$$\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$$

equipped with the usual addition and multiplication modulo p, forms a finite field with p elements which we denote by $\mathbb{F}_p$.

Theorem 1.1. (Fermat's Little Theorem) Let p be a prime which does not divide an integer a. Then,

$$a^{p-1} = 1 \mod p.$$

Proof. We list the first $p-1$ positive multiples of a :

$$a, 2a, \cdots, (p-1)a \mod p.$$

Suppose that ra and sa are the same modulo p. Then, $r = s \mod p$ and the $p-1$ multiples of a above are distinct and nonzero, that is, they must be congruent to $1, 2, \cdots, p-1$ in some order. Multiply all these congruences together and we find :

$$a(2a)\cdots((p-1)a) = 1.2\cdots(p-1) \mod p,$$

which is

$$a^{p-1}(p-1)! = (p-1)! \mod p.$$

Divide both side by $(p-1)!$ to complete the proof. □

Remark 1.1. Sometimes Fermat's Little Theorem is presented in the form

$$a^p = a \mod p,$$

for any integer a and a prime p.

Recall that for any two integers $0 \leq n$ and $0 \leq k \leq n$, the binomial coefficient C_k^n is defined by :

$$C_k^n = \frac{n!}{k!(n-k)!}.$$

Proposition 1.1. The prime p divides C_k^p for any $1 \leq k \leq p-1$.

Proof. We have

$$p! = k!(p-k)!C_k^p.$$

Then, p divides $k!(p-k)!C_k^p$. Since p is prime and

$$\gcd(p, k!) = \gcd(p, (p-k)!) = 1,$$

then p divides C_k^p. □

Remark 1.2. Fermat's Little Theorem along with Proposition 1.1 imply that, for any $a, b \in \mathbb{F}_p$, we have $a^p = a$ and

$$\begin{aligned}(a+b)^p = \sum_{k=0}^{p} C_k^p a^k b^{p-k} &= a^p + \sum_{k=1}^{p-1} C_k^p a^k b^{p-k} + b^p \\ &= a^p + b^p = a + b.\end{aligned}$$

Definition 1.2. Let $\mathbb{L}$ be a field. A subset $\mathbb{K}$ of $\mathbb{L}$ that is itself a field under the operations of $\mathbb{L}$ is called a *subfield* of $\mathbb{L}$. In this context, $\mathbb{L}$ is called an *extension* of $\mathbb{K}$.

Remark 1.3. If $\mathbb{K}$ is a subfield of the finite field $\mathbb{F}_p$, where p is prime, then $\mathbb{K}$ must contain the elements 0 and 1, and so all other elements of $\mathbb{F}_p$ by the closure of $\mathbb{K}$ under addition. It follows that $\mathbb{F}_p$ contains no proper subfields, and it is called *prime field*.

The prime field $\mathbb{F}_p$, also called the *Galois field* of order p, plays an important role in general field theory, since every field of characteristic p can be thought of as an extension of $\mathbb{F}_p$.

Definition 1.3. Let $\mathbb{K}$ be a subfield of $\mathbb{L}$ and $\alpha \in \mathbb{L}$. If α satisfies a nontrivial polynomial equation with coefficients in $\mathbb{K}$, that is, if $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$ with $a_i \in \mathbb{K}$ not all being 0, then α is said to be *algebraic* over $\mathbb{K}$. The extension $\mathbb{L}$ of $\mathbb{K}$ is called algebraic over $\mathbb{K}$ if every element of $\mathbb{L}$ is algebraic over $\mathbb{K}$.

Theorem 1.2. [24, Theorem 1.78] The prime subfield of a field $\mathbb{L}$ is isomorphic to either $\mathbb{F}_p$ or $\mathbb{Q}$. Therefore, the characteristic of $\mathbb{L}$ is a prime p or 0.

Theorem 1.3. [24, Theorem 2.2] Let $\mathbb{L}$ be a finite field. Then, $\mathbb{L}$ has p^n elements, where the prime p is the characteristic of $\mathbb{L}$ and n is the degree of $\mathbb{L}$ over its prime subfield $\mathbb{F}_p$.

Remark 1.4. The degree of $\mathbb{L}$ over its prime subfield $\mathbb{F}_p$ is the dimension of $\mathbb{L}$ considered as a vector space over $\mathbb{F}_p$.

Example 1.2. Consider the matrix

$$\mathbf{M} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{F}_2).$$

With the identification

$$\mathbb{F}_2 = \{0,1\} := \left\{ \mathbf{O} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{Mat}_{2\times 2}(\mathbb{F}_2),$$

the matrix $\mathbf{M}$ verifies the equation $\mathbf{M}^2 + \mathbf{M} + \mathbf{I} = 0$ over $\mathbb{F}_2$. Therefore, the matrix $\mathbf{M}$ is algebraic over $\mathbb{F}_2$, and the field

$$\mathbb{F}_2[\mathbf{M}] = \{\mathbf{O}, \mathbf{I}, \mathbf{M}, \mathbf{I} + \mathbf{M}\}$$

is an algebraic extension of $\mathbb{F}_2$ with $2^2 = 4$ elements. The degree of $\mathbb{F}_2[\mathbf{M}]$ over $\mathbb{F}_2$ is 2, considered as a vector space over $\mathbb{F}_2$ with a basis $\{\mathbf{I}, \mathbf{M}\}$.

We use the notation $\mathbb{F}_q$ for finite fields with $q = p^n$ elements. In order to construct $\mathbb{F}_q$, we need the notion of the *minimal polynomial* of an element $\alpha \in \mathbb{F}_q$ over $\mathbb{F}_p$ of degree n, which we introduce later.

Definition 1.4. For a multiplicative group G, the *order* of an element $a \in G$, if it exists, is the smallest positive integer n for which $a^n = 1$, and we write $n = \mathrm{ord}(a)$.

Theorem 1.4. [24, Theorem 2.8] For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.

Proof. We may assume $q \geq 3$. Let $h = p_1^{r_1} \cdots p_m^{r_m}$ be the prime factor decomposition of the order $h = q - 1$ of the group $\mathbb{F}_q^*$. For every $1 \leq i \leq m$, the polynomial $x^{h/p_i} - 1$ has at most h/p_i roots in $\mathbb{F}_q$. Since $h/p_i < h$, it follows that there are nonzero elements in $\mathbb{F}_q$ that are not roots of this polynomial. Let a_i be such an element and set

$$b_i = a_i^{h/p_i^{r_i}}.$$

We have $b_i^{p_i^{r_i}} = 1$, hence the order of b_i is a divisor of $p_i^{r_i}$ and is therefore of the form $p_i^{s_i}$ with $0 \leq s_i \leq r_i$. On the other hand, we have

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1,$$

and so the order of b_i is $p_i^{r_i}$. We claim that the element $b = b_1 \cdots b_m$ has order h. Suppose, on the contrary, that the order of b is a proper divisor of h and is therefore a divisor of at least one of the m integers h/p_j, $1 \leq j \leq m$, say of h/p_1. Then, we have

$$1 = b^{h/p_1} = b_1^{h/p_1} \cdots b_m^{h/p_1}.$$

Now, if $2 \leq i \leq m$, then $p_i^{r_i}$ divides h/p_1, and hence $b_i^{h/p_1} = 1$. Therefore $b_1^{h/p_1} = 1$. This implies that the order of b_1 must divide h/p_1, which is impossible since the order of b_1 is $p_1^{r_1}$. Thus, $\mathbb{F}_q^*$ is a cyclic group with generator b. □

Definition 1.5. A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

Example 1.3. The multiplicative group of the prime field $\mathbb{F}_7$ is

$$\mathbb{F}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \langle \bar{3} \rangle = \{\bar{3}^i : 0 \leq i \leq 5\},$$

and $\bar{3}$ is a primitive element of $\mathbb{F}_7$.

Remark 1.5. The order of a primitive element of $\mathbb{F}_q$ is maximal and is equal to $q - 1$.

Proposition 1.2. The field $\mathbb{F}_q$ contains $\phi(q-1)$ primitive elements, where

$$\phi(n) = \text{card}\{1 \leq i \leq n : \gcd(i, n) = 1\}$$

is Euler's function.

Proof. Let a be a primitive element of $\mathbb{F}_q$. Then, any other primitive element of $\mathbb{F}_q$ is of the form a^i for some $1 \leq i \leq q-1$. Thus, we must have $\text{ord}(a^i) = q - 1$, which is equivalent to $\gcd(i, q-1) = 1$. □

Example 1.4. The field $\mathbb{F}_7$ has $\phi(6) = 2$ primitive elements, which are $\bar{3}$ and $\bar{5}$.

Proposition 1.3. Let $\mathbb{F}_q$ be a finite field with q elements. Then, every $a \in \mathbb{F}_q$ satisfies $a^q = a$.

Proof. If $a = 0$, then $a^q = a$. On the other hand, the multiplicative group $\mathbb{F}_q^*$ has order $q - 1$. Then, $a^{q-1} = 1$ for all $a \in \mathbb{F}_q^*$, and the multiplication by a yields the desired result. □

Finite fields have the property that they are functionally complete. This means that every mapping of a finite field can be expressed as a polynomial, which is an immediate consequence of the Lagrange interpolation formula. To show that, let $f(x)$ be a map over $\mathbb{F}_q$, and consider the finite set

$$S = \left\{(a, f(a)) : a \in \mathbb{F}_q\right\}.$$

Recall that for a set of $k+1$ points $\{(x_i, y_i) : 0 \leq i \leq k\}$, where no two x_i are the same, the interpolation polynomial of the previous set in Lagrange form is the linear combination

$$L(x) = \sum_{i=0}^{k} y_i l_i(x),$$

of Lagrange basis polynomials

$$l_i(x) = \prod_{\substack{0 \leq m \leq k \\ i \neq m}} \frac{x - x_m}{x_i - x_m}.$$

The polynomial $L(x)$ verifies the equation $L(x_i) = y_i$, for all $0 \leq i \leq k$. Therefore, if we consider the interpolation polynomial $L(x)$ of the set S, then $L(x) \in \mathbb{F}_q[x]$ and $f(a) = L(a)$, for all $a \in \mathbb{F}_q$. Hence, the two functions $f(x)$ and $L(x)$ are identical over $\mathbb{F}_q$.

1.2 Frobenius Automorphism And Trace Function

A well known map over $\mathbb{F}_{p^s}$ is the so-called *Frobenius automorphism* defined by :

$$\begin{aligned} \varphi : \mathbb{F}_{p^s} &\to \mathbb{F}_{p^s} \\ a &\mapsto a^p. \end{aligned}$$

We can extend φ to the following map :

$$\begin{aligned} \varphi : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ a &\mapsto a^q, \end{aligned} \tag{1.1}$$

where q is a power of the prime p.

Proposition 1.4. The map φ is an automorphism of $\mathbb{F}_{q^m}$ called, for convenience, the Frobenius automorphism.

Proof. Suppose that $q = p^s$, for some integer $1 \leq s$. For all $a, b \in \mathbb{F}_{q^m}$, we have

$$\begin{aligned} \varphi(a+b) = (a+b)^q &= ((a+b)^p)^{p^{s-1}} \\ &= (a^p + b^p)^{p^{s-1}} \\ &\vdots \\ &= a^q + b^q \\ &= \varphi(a) + \varphi(b), \end{aligned}$$

and

$$\varphi(ab) = (ab)^q = a^q b^q = \varphi(a)\varphi(b).$$

Therefore, φ is a homomorphism of $\mathbb{F}_{q^m}$. On the other hand, we have

$$\ker(\varphi) = \{c \in \mathbb{F}_{q^m} : c^q = 0\} = \{0\},$$

and then φ is injective. Finally, let $c \in \mathbb{F}_{q^m}$, then

$$\left(c^{q^{m-1}}\right)^q = c^{q^m} = c$$

by Proposition 1.3. Hence, φ is surjective and thus an automorphism of $\mathbb{F}_{q^m}$. □

Remark 1.6. Note that, the surjection of φ in the proof above could also be deduced from the fact that $\mathbf{F}_{q^m}$ is finite and φ is injective.

Theorem 1.5. [28, Theorem 2.1.76] The distinct automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are given by the maps $\varphi_0, \cdots, \varphi_{m-1}$ where

$$\begin{aligned} \varphi_i : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ a &\mapsto a^{q^i}. \end{aligned}$$

Remark 1.7. The set of automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ forms a group under composition. This group is called the *Galois group* of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It is a cyclic group with generator φ, that is, $\varphi_i = \varphi^i$ for all $0 \leq i \leq m-1$.

Definition 1.6. We define the *trace function* from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$ as follows :

$$\begin{aligned} \mathrm{Tr}_{q^m|q} : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ a &\mapsto a + a^q + \cdots + a^{q^{m-1}}. \end{aligned}$$

Proposition 1.5. The trace function $\mathrm{Tr}_{q^m|q}$ verifies the following properties :

(i) $\mathrm{Tr}_{q^m|q}$ is linear ($\mathbb{F}_{q^m}$ is considered as a vector space over $\mathbb{F}_q$).

(ii) For all $a \in \mathbb{F}_{q^m}$, $\mathrm{Tr}_{q^m|q}(a^q) = \mathrm{Tr}_{q^m|q}(a)$.

(iii) The trace function is transitive, i.e. For all $a \in \mathbb{F}_{q^m}$ and a divisor d of m, we have

$$\mathrm{Tr}_{q^m|q}(a) = \mathrm{Tr}_{q^d|q}\left(\mathrm{Tr}_{q^m|q^d}(a)\right).$$

Proof. Let $a \in \mathbb{F}_{q^m}$. Note first that, since

$$\begin{aligned} \mathrm{Tr}_{q^m|q}(a)^q &= (a + a^q + \cdots + a^{q^{m-1}})^q \\ &= a^q + a^{q^2} + \cdots + a^{q^m} \\ &= a + a^q + \cdots + a^{q^{m-1}} \\ &= \mathrm{Tr}_{q^m|q}(a), \end{aligned}$$

then $\mathrm{Tr}_{q^m|q}(a) \in \mathbb{F}_q$.

(i) Let $b \in \mathbb{F}_{q^m}$ and $\lambda \in \mathbb{F}_q$. Then

$$\begin{aligned} \mathrm{Tr}_{q^m|q}(\lambda a + b) &= (\lambda a + b) + (\lambda a + b)^q + \cdots + (\lambda a + b)^{q^{m-1}} \\ &= \lambda(a + a^q + \cdots + a^{q^{m-1}}) + (b + b^q + \cdots + b^{q^{m-1}}) \\ &= \lambda \mathrm{Tr}_{q^m|q}(a) + \mathrm{Tr}_{q^m|q}(b). \end{aligned}$$

(ii) For all $a \in \mathbb{F}_{q^m}$, we have :

$$\begin{aligned}\mathrm{Tr}_{q^m|q}(a^q) &= a^q + a^{q^2} + \cdots + a^{q^m} \\ &= a + a^q + \cdots + a^{q^{m-1}} \\ &= \mathrm{Tr}_{q^m|q}(a).\end{aligned}$$

(iii) Let d be a divisor of m and $m = dn$. Then

$$\begin{aligned}\mathrm{Tr}_{q^{dn}|q}(a) &= a + \cdots + a^{q^{dn-1}} \\ &= \left(a + a^{q^d} + \cdots + a^{q^{d(n-1)}}\right) + \cdots + \left(a + a^{q^d} + \cdots + a^{q^{d(n-1)}}\right)^{q^{d-1}} \\ &= \left(\mathrm{Tr}_{q^{dn}|q^d}(a)\right) + \cdots + \left(\mathrm{Tr}_{q^{dn}|q^d}(a)\right)^{q^{d-1}} \\ &= \mathrm{Tr}_{q^d|q}\left(\mathrm{Tr}_{q^{dn}|q^d}(a)\right).\end{aligned}$$

□

When $q = p^m$, the *absolute trace*

$$\begin{aligned}\mathrm{Tr}_{q|p} : \mathbb{F}_q &\to \mathbb{F}_p \\ a &\mapsto a + a^p + \cdots + a^{p^{m-1}},\end{aligned}$$

is denoted by Tr_q.

Definition 1.7. The elements $a, a^q, \cdots, a^{q^{m-1}} \in \mathbb{F}_{q^m}$ are called the *conjugates* of a with respect to $\mathbb{F}_q$.

Remark 1.8. The conjugates of a are the elements to which a is sent by iterated applications of the Frobenius automorphism.

1.3 Companion Matrix And Characteristic Polynomial

There exist several ways of representing the elements of $\mathbb{F}_q$. One way to do that is to use matrices, for example the *companion matrix* of a polynomial.

Definition 1.8. The companion matrix of a monic polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_q[x]$ is given by the $n \times n$ matrix

$$\mathbf{C}_f = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{Mat}_{n\times n}(\mathbb{F}_q).$$

Remark 1.9. It is well known in linear algebra that $\mathbf{C}_f$ satisfies the equation $f(\mathbf{C}_f) = 0$, that is

$$f(\mathbf{C}_f) = \sum_{i=0}^{n} a_i \mathbf{C}_f^i = a_0 \mathbf{I}_n + a_1 \mathbf{C}_f + \cdots + a_{n-1} \mathbf{C}_f^{n-1} + \mathbf{C}_f^n = 0,$$

where $\mathbf{I}_n$ is the $n \times n$ identity matrix.

Example 1.5. The companion matrix of the polynomial $f(x) = 2 + x + x^3 \in \mathbb{F}_3[x]$ is

$$\mathbf{C}_f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{F}_3),$$

and we have

$$2\mathbf{I}_3 + \mathbf{C}_f + \mathbf{C}_f^3 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Definition 1.9. Let $\mathbf{M} \in \mathrm{Mat}_{n\times n}(\mathbb{F}_q)$. Then, the *characteristic polynomial* of $\mathbf{M}$ is

$$P_M(x) = \det(x\mathbf{I}_n - \mathbf{M}).$$

Remark 1.10. The polynomial $P_M(x)$ is monic over $\mathbb{F}_q$ of degree n, and verfies the equation $P_M(\mathbf{M}) = 0$.

Example 1.6. The characteristic polynomial of the matrix $\mathbf{C}_f$ obtained in Example 1.5 is

$$\det(x\mathbf{I}_3 - \mathbf{C}_f) = \begin{vmatrix} x & 0 & 2 \\ 2 & x & 1 \\ 0 & 2 & x \end{vmatrix} = 2 + x + x^3 = f(x).$$

Remark 1.11. For a monic polynomial $f(x) \in \mathbb{F}_q[x]$, the characteristic polynomial of its companion matrix $\mathbf{C}_f$ is equal to $f(x)$, that is, $f(x) = \det(x\mathbf{I} - \mathbf{C}_f)$, hence the property $f(\mathbf{C}_f) = 0$.

1.4 Irreducible Polynomials

A central question about polynomials over $\mathbb{F}_q$ is to find the *prime elements* of the ring $\mathbb{F}_q[x]$, which are usually called *irreducible polynomials*.

Definition 1.10. Let $f(x) \in \mathbb{F}_q[x]$ of degree $n \geq 1$. We say that $f(x)$ is irreducible over $\mathbb{F}_q$ if $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{F}_q[x]$ implies that either $g(x)$ or $h(x)$ is a constant polynomial.

Example 1.7. The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, since it has no roots in $\mathbb{F}_2$, that is, $f(x)$ has no linear factor over $\mathbb{F}_2$. However, the polynomial $x^2 + 1 = (x + 1)^2$ is reducible over $\mathbb{F}_2$.

Briefly stated, a polynomial of positive degree is irreducible over $\mathbb{F}_q$ if it allows only trivial factorizations over $\mathbb{F}_q$.

Theorem 1.6. [24, Corollary 2.11] For every finite field $\mathbb{F}_q$ and every positive integer n, there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.

Theorem 1.7. [24, Theorem 1.47] Let R be a commutative ring with identity. If R is a principal ideal domain, then $R/(c)$ is a field if and only if c is a prime element of R.

Since $\mathbb{F}_q$ is a field and the commutative ring $\mathbb{F}_q[x]$ is a principal ideal domain, we have the following result.

Theorem 1.8. [24, Theorem 1.61] Let $f(x) \in \mathbb{F}_q[x]$. The residue class ring $\mathbb{F}_q[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible over $\mathbb{F}_q$.

Proof. Note that the ring $\mathbb{F}_q[x]$ is a *Euclidean domain*. Therefore, the *Euclidean division* and the *Bézout's identity* for polynomials hold in $\mathbb{F}_q[x]$, i.e., for any nonzero polynomials $g(x), h(x) \in \mathbb{F}_q[x]$, there exist nonzero polynomials $u(x), v(x) \in \mathbb{F}_q[x]$ such that

$$u(x)g(x) + v(x)h(x) = \gcd(g(x), h(x)).$$

If $\mathbb{F}_q[x]/(f(x))$ is a field and $f(x) = g(x)h(x)$ is reducible, with $1 \leq \deg(g(x)), \deg(h(x)) \leq \deg(f(x)) - 1$, then both $g(x) + (f(x))$ and $h(x) + (f(x))$ are nonzero and not invertible in $\mathbb{F}_q[x]/(f(x))$, a contradiction. The other implication is a consequence of the Bézout's identity. □

Remark 1.12. As we have mentioned before, in order to construct $\mathbb{F}_{q^n}$, we need an irreducible polynomial over $\mathbb{F}_q$ of degree n. Then, let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n, Theorem 1.8 implies that

$$\mathbb{F}_q[x]/(f(x)) = \{h(x) \mod f(x) : h(x) \in \mathbb{F}_q[x], \deg(h) < n\}$$

is a field with q^n elements which we denote by $\mathbb{F}_{q^n}$.

Example 1.8. Consider the irreducible polynomial $f(x) = x^2 + x + 1$ over $\mathbb{F}_2$. Then, the field $\mathbb{F}_4 = \mathbb{F}_{2^2}$ can be represented by the field

$$\mathbb{F}_2[x]/(f(x)) = \{a + bx \mod f(x) : a, b \in \mathbb{F}_2\},$$

where the addition and multiplication tables for $\mathbb{F}_4$ are given by :

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Definition 1.11. If $f(x)$ is irreducible over $\mathbb{F}_q$ of degree n, then the field $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f(x))$ is called the *splitting field* of $f(x)$.

Theorem 1.9. [24, Lemma 1.58] If an irreducible polynomial $f(x) \in \mathbb{F}_q$ divides a product $f_1(x) \cdots f_k(x)$ of polynomials in $\mathbb{F}_q[x]$, then at least one of the factors $f_i(x)$ is divisible by $f(x)$.

Proof. Since $f(x)$ divides $f_1(x) \cdots f_k(x)$, then

$$(f_1(x) + (f(x)) \cdots (f_k(x) + (f(x)) = 0 + (f(x))$$

in the residue class ring $\mathbb{F}_q[x]/(f(x))$. Now $\mathbb{F}_q[x]/(f(x))$ is a field, then

$$f_i(x) + (f(x)) = 0 + (f(x))$$

for some $1 \leq i \leq k$, i.e., $f(x)$ divides $f_i(x)$. □

Irreducible polynomials over $\mathbb{F}_q$ are of fundamental importance for the structure of the ring $\mathbb{F}_q[x]$, since the polynomials in $\mathbb{F}_q[x]$ can be written as product of irreducible polynomials in an essentially unique manner.

Theorem 1.10. [24, Theorem 1.59] Any polynomial $h(x) \in \mathbb{F}_q[x]$ of positive degree can be written in the form

$$h(x) = af_1(x)^{e_1} \cdots f_k(x)^{e_k} \tag{1.2}$$

where $a \in \mathbb{F}_q$, $f_1(x), \ldots, f_k(x)$ are distinct monic irreducible polynomials in $\mathbb{F}_q[x]$, and $e_1, \ldots, e_k$ are positive integers.

Proof. The fact that any non constant polynomial $f(x) \in \mathbb{F}_q[x]$ can be represented in the form (1.2) is shown by induction on the degree of $f(x)$.
The case $\deg(f(x)) = 1$ is trivial, since any polynomial in $\mathbb{F}_q[x]$ of degree 1 is irreducible over $\mathbb{F}_q$. Now, suppose the desired factorization is established for all non constant polynomials in $\mathbb{F}_q[x]$ of degree less than n. If $\deg(f(x)) = n$ and $f(x)$ is irreducible over $\mathbb{F}_q$, then we are done since we can write $f(x) = a(a^{-1}f(x))$, where a is the leading coefficient of $f(x)$ and $a^{-1}f(x)$ is a monic irreducible polynomial over $\mathbb{F}_q$. Otherwise, $f(x)$ allows a factorization $f(x) = g(x)h(x)$ with $1 \leq \deg(g(x)), \deg(h(x)) < n$, and $g(x), h(x) \in \mathbb{F}_q[x]$. By the induction hypothesis, $g(x)$ and $h(x)$ can be factored in the form (1.2), and then $f(x)$ can be factored in this form. □

To determine all monic irreducible polynomials over $\mathbb{F}_p$ of degree n, one may first compute all monic reducible polynomials over $\mathbb{F}_p$ of degree n, and then eliminate them from the set of monic polynomials in $\mathbb{F}_p[x]$ of degree n.

Example 1.9. Find all irreducible polynomials over $\mathbb{F}_2$ of degree 4. Note that a nonzero polynomial over $\mathbb{F}_2$ is automatically monic. There are $2^4 = 16$ polynomials in $\mathbb{F}_2[x]$ of degree

4. Such a polynomial is reducible over $\mathbb{F}_2$ if and only if it has a divisor of degree 1 or 2. Therefore, we compute all products

$$(a_0 + a_1x + a_2x^2 + x^3)(b_0 + x) \quad \text{and} \quad (a_0 + a_1x + x^2)(b_0 + b_1x + x^2),$$

and obtain all reducible polynomials over $\mathbb{F}_2$ of degree 4. Comparison with the 16 polynomials of degree 4 leaves us with the irreducible polynomials

$$x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x].$$

Remark 1.13. If p or n is large, the above method is not feasible, and there are more powerful methods in the literature (see [24]).

For $a_1, a_2, \ldots, a_r \in \mathbb{F}_{q^n}$, we denote by $\mathbb{F}_q(a_1, a_2, \ldots, a_r)$ the smallest subfield of $\mathbb{F}_{q^n}$ containing both $\mathbb{F}_q$ and $a_1, a_2, \ldots, a_r$, that is, the extension of $\mathbb{F}_q$ obtained by adjoining $a_1, a_2, \ldots, a_r$ to $\mathbb{F}_q$. In particular, if α is a root of an irreducible polynomial $f(x)$, then we have

$$\mathbb{F}_q(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i\alpha^i : \ a_i \in \mathbb{F}_q \right\}.$$

Theorem 1.11. [24, Theorem 2.14] If $f(x)$ is irreducible over $\mathbb{F}_q$, then $f(x)$ has a root $\alpha \in \mathbb{F}_{q^n}$. Furthermore, all the roots of $f(x)$ are simple and are given by the n distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ of $\mathbb{F}_{q^n}$.

Proof. The theorem is trivial if $n = 1$, so assume $n > 1$. Note that $\alpha = x + (f(x))$ is a root of $f(x)$ in the field $\mathbb{F}_q[x]/(f(x))$, that is,

$$f(\alpha) = f\left(x + (f(x))\right) = f(x) + (f(x)) = 0 + (f(x)).$$

Then, we have the following ring isomorphism

$$\begin{aligned} \mathbb{F}_q[x]/(f(x)) &\to \mathbb{F}_q(\alpha) \\ h(x) + (f(x)) &\mapsto h(\alpha). \end{aligned}$$

Therefore, we have

$$\mathbb{F}_q(\alpha) \cong \mathbb{F}_q[x]/(f(x)) \cong \mathbb{F}_{q^n}.$$

Now, suppose that $f(x) = \sum_{i=0}^{n} a_i x^i$. Then, for all $0 \le j \le n-1$, we have

$$f(\alpha^{q^j}) = \sum_{i=0}^{n} a_i(\alpha^{q^j})^i = \left(\sum_{i=0}^{n} a_i\alpha^i \right)^{q^j} = (f(\alpha))^{q^j} = 0.$$

If $\alpha^{q^i} = \alpha^{q^j}$ with $0 \le j < i \le n-1$, then $\alpha^{(q^{i-j}-1)q^j} = 1$. Since $\gcd(\mathrm{ord}(\alpha), q^j) = 1$, so $\mathrm{ord}(\alpha)$ divides $q^{i-j} - 1$. Hence, $\alpha \in \mathbb{F}_{q^{i-j}} \subsetneq \mathbb{F}_{q^n}$, a contradiction. □

We use the notation $[\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ to mean the degree of α over $\mathbb{F}_q$, which is the degree of $f(x)$.

Remark 1.14. Theorem 1.11 implies that an irreducible polynomial $f(x)$ over a finite field of degree n must have n distinct roots $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$, and we have

$$f(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}).$$

With this information, we can deduce that polynomials of certain forms are never irreducible. For example, consider the polynomial $x^p + a \in \mathbb{F}_q$ and let α be its root. Then

$$(x - \alpha)^p = x^p - \alpha^p = x^p + a,$$

and α is the only root of $x^p + a$. Therefore, the polynomial $x^p + a$ is reducible over $\mathbb{F}_q$, since if it would be irreducible, it would have p distinct roots.

Definition 1.12. The irreducible polynomial $f(x)$ is called the *minimal polynomial* of α over $\mathbb{F}_q$, and we write $f(x) = \mathrm{Min}(\alpha, \mathbb{F}_q)(x)$.

Remark 1.15. The conjugates of $\alpha \in \mathbb{F}_{q^n}$ with respect to $\mathbb{F}_q$ are distinct if and only if the polynomial $\mathrm{Min}(\alpha, \mathbb{F}_q)(x)$ has degree n. Otherwise, the degree d of $\mathrm{Min}(\alpha, \mathbb{F}_q)(x)$ is a proper divisor of n, and then the conjugates of α with respect to $\mathbb{F}_q$ are the distinct elements $\alpha, \alpha^q, \cdots, \alpha^{q^{d-1}}$, each repeated n/d times.

Theorem 1.12. [24, Lemma 2.12] For a polynomial $h(x) \in \mathbb{F}_q[x]$, we have $h(\alpha) = 0$ if and only if $\mathrm{Min}(\alpha, \mathbb{F}_q)(x)$ divides $h(x)$.

Remark 1.16. Theorem 1.12 implies that two monic irreducible polynomials $h(x), g(x) \in \mathbb{F}_q[x]$ having a common root are equal.

Theorem 1.13. [24, Theorem 1.89] Let α and β be two roots of $f(x)$ that is irreducible over $\mathbb{F}_q$. Then, $\mathbb{F}_q(\alpha)$ and $\mathbb{F}_q(\beta)$ are isomorphic under the isomorphism

$$\begin{aligned} \mathbb{F}_q(\alpha) &\to \mathbb{F}_q(\beta) \\ \alpha &\mapsto \beta, \end{aligned}$$

keeping the elements of $\mathbb{F}_q$ fixed.

Remark 1.17. If $f(x)$ is irreducible over $\mathbb{F}_q$, then $\mathbf{C}_f$ can play the role of a root of $f(x)$. The polynomials in $\mathbf{C}_f$ over $\mathbb{F}_q$ of degree less than n yield a representation of the elements of $\mathbb{F}_{q^n}$, i.e.,

$$\mathbb{F}_q[\mathbf{C}_f] = \left\{ \sum_{i=0}^{n-1} a_i \mathbf{C}_f^i : \ a_i \in \mathbb{F}_q \right\} \cong \mathbb{F}_{q^n}.$$

Lemma 1.1. [24, Lemma 3.1] Let $f(x) \in \mathbb{F}_q[x]$ of degree $n \geq 1$ with $f(0) \neq 0$. Then, there exists a positive integer $e \leq q^n - 1$ such that $f(x)$ divides $x^e - 1$.

Proof. The residue class ring $\mathbb{F}_q[x]/(f(x))$ contains $q^n - 1$ nonzero elements. Since the q^n residue classes $x^i + (f(x))$, where $0 \leq i \leq q^n - 1$, are all nonzero, then there exist integers $0 \leq r < s \leq q^n - 1$ such that $x^s = x^r \mod f(x)$. Therefore, since x and $f(x)$ are relatively prime, we have $x^{s-r} = 1 \mod f(x)$, or equivalently, $f(x)$ divides $x^{s-r} - 1$ and $0 < s - r \leq q^n - 1$. □

An important integer attached to a nonzero polynomial over a finite field is its *order*.

Definition 1.13. Let $h(x) \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $h(0) \neq 0$, the least positive integer e for which $h(x)$ divides $x^e - 1$ is called the order of $h(x)$, and denoted by $\text{ord}(h(x))$. If $h(0) = 0$, then $h(x) = x^t g(x)$, where $t \in \mathbb{N}$ and $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$ are uniquely determined; $\text{ord}(h(x))$ is then defined to be $\text{ord}(g(x))$.

Remark 1.18. Any other integer s for which $h(x)$ divides $x^s - 1$ is then a multiple of e.

Proposition 1.6. [24, Theorem 2.18] The conjugates of $\alpha \in \mathbb{F}_{q^n}^*$ with respect to any subfield of $\mathbb{F}_{q^n}$ have the same order in the group $\mathbb{F}_{q^n}^*$.

Proof. The result follows from the fact that $\mathbb{F}_{q^n}^*$ is a cyclic group, and that every power of the characteristic of $\mathbb{F}_{q^n}$ is relatively prime to the order $q^n - 1$ of $\mathbb{F}_{q^n}^*$. □

Proposition 1.7. Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n having $\alpha \in \mathbb{F}_{q^n}$ as a root. Suppose that $f(0) \neq 0$. Then $\text{ord}(f(x)) = \text{ord}(\alpha)$.

Proof. First, we have

$$f(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}).$$

Let $e = \text{ord}(\alpha)$. Proposition 1.6 implies that $e = \text{ord}(\alpha^{q^i})$ for all $1 \leq i \leq n - 1$. Then, $f(x)$ divides $x^e - 1$, since $f(0) \neq 0$. Suppose that there exists some integer $0 < s < e$, such that $f(x)$ divides $x^s - 1$. Then, $\alpha^s - 1 = 0$ and $\text{ord}(\alpha) \leq s < e$, a contradiction. Therefore, $\text{ord}(f(x)) = \text{ord}(\alpha)$. □

Let $f(x) \in \mathbb{F}_q[x]$ of order e and let e' be the order of $f(x)$ viewed as a polynomial over some extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. This means that there exists a polynomial $g(x) \in \mathbb{F}_{q^m}$ such that $f(x)g(x) = x^{e'} - 1$. But, since the polynomials $f(x)$ and $x^{e'} - 1$ have their coefficients in $\mathbb{F}_q$, the polynomial $g(x)$ must have all its coefficients in $\mathbb{F}_q$, and then $e = e'$. It follows that the definition of the order of a polynomial does not depend on the choice of the field on which that polynomial is defined. This justifies the following remark.

Remark 1.19. Propositions 1.7 implies that, if $f(x)$ is irreducible over $\mathbb{F}_q$ and $V(x)$ is an irreducible factor of $f(x)$ over an extension of $\mathbb{F}_q$, then $\text{ord}(f(x)) = \text{ord}(V(x)) = \text{ord}(\alpha)$ for any root α of $f(x)$.

1.5 Primitive Polynomials

Definition 1.14. A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is called *primitive* over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^n}$

Thus, a primitive polynomial over $\mathbb{F}_q$ of degree n may be described as a monic polynomial that is irreducible over $\mathbb{F}_q$, and has a root $\alpha \in \mathbb{F}_{q^n}$ that generates the multiplicative group $\mathbb{F}_{q^n}^*$. Primitive polynomials can also be characterized as follows.

Theorem 1.14. [24, Theorem 3.16] A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is a primitive polynomial over $\mathbb{F}_q$ if and only if $f(x)$ is monic, $f(0) \neq 0$ and $\mathrm{ord}(f) = q^n - 1$.

Remark 1.20. The condition $f(0) \neq 0$ in the theorem above is to rule out the non primitive polynomial $f(x) = x$ in the case $q = 2$ and $n = 1$.

Example 1.10. Consider the polynomial $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Note that

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f(x),$$

where $x^2 + x + 1$ is the only irreducible polynomial of degree 2 over $\mathbb{F}_2$. Moreover, $f(x)$ has no roots in $\mathbb{F}_2$. Therefore, $f(x)$ is irreducible over $\mathbb{F}_2$. Let $\alpha \in \mathbb{F}_{16}$ be a root of $f(x)$. First, we have that $\mathbb{F}_{16}^*$ has order 15, then $\mathrm{ord}(\alpha) \in \{1, 3, 5, 15\}$. On the other hand, since $\alpha \neq 1$ we have $\mathrm{ord}(\alpha) \neq 1$, and also $\mathrm{ord}(\alpha) \neq 3$, for otherwise we would have $\alpha^3 + 1 = 0$, a contradiction, since $f(x) = \mathrm{Min}(\alpha, \mathbb{F}_2)(x)$ which is of degree 4. Finally

$$\alpha^5 = \alpha.\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha \neq 1,$$

since $\alpha^2 + \alpha + 1 \neq 0$ for the same reason as previously. Thus, $\mathrm{ord}(\alpha) = 15$ and α is a primitive element of $\mathbb{F}_{16}$. It follows that $f(x)$ is a primitive polynomial over $\mathbb{F}_2$.

Remark 1.21. Since the multiplicative group $\mathbb{F}_{q^n}^*$ of the field $\mathbb{F}_{q^n}$ is cyclic, then there exits always a primitive polynomial over $\mathbb{F}_q$ of degree n, which is the minimal polynomial of a primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Proposition 1.8. [24, Corollary 2.19] If α is a primitive element of $\mathbb{F}_{q^n}$, then so are all its conjugates with respect to any subfield of $\mathbb{F}_{q^n}$.

Proof. This follows from the fact that $\gcd(q^i, q^n - 1) = 1$, for all $0 \leq i$. □

Example 1.11. Let $\alpha \in \mathbb{F}_{16}$ be a root of the primitive polynomial $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ treated in the previous example. Then, the conjugates of α with respect to $\mathbb{F}_2$ are $\alpha, \alpha^2, \alpha^4 = \alpha + 1$ and $\alpha^8 = \alpha^2 + 1$, each of them being a primitive element of $\mathbb{F}_{16}$. The conjugates of α with respect to $\mathbb{F}_4$ are α and $\alpha^4 = \alpha + 1$.

Proposition 1.9. [28, Theorem 4.1.3] The number of primitive polynomials over $\mathbb{F}_q$ of degree n is $\frac{\phi(q^n-1)}{n}$.

Proof. We have that the number of primitive elements of $\mathbb{F}_{q^n}$ is equal to $\phi(q^n-1)$. Since each primitive element of $\mathbb{F}_{q^n}$ and its conjugates with respect to $\mathbb{F}_q$ have the same minimal polynomial over $\mathbb{F}_q$ of degree n, we list those primitive elements as follows :

$$\begin{aligned}
&\alpha_1, \alpha_1^q, \cdots, \alpha_1^{q^{n-1}},\\
&\alpha_2, \alpha_2^q, \cdots, \alpha_2^{q^{n-1}},\\
&\vdots\\
&\alpha_s, \alpha_s^q, \cdots, \alpha_s^{q^{n-1}},
\end{aligned}$$

where s is the number of primitive polynomials over $\mathbb{F}_q$ of degree n. Therefore, $sn = \phi(q^n - 1)$, or equivalently $s = \frac{\phi(q^n-1)}{n}$. □

Example 1.12. Since the polynomial $f(x) = x^2 + x + 1$ is the only irreducible polynomial over $\mathbb{F}_2$ of degree 2, and $\frac{\phi(2^2-1)}{2} = 1$, then $f(x)$ is primitive over $\mathbb{F}_2$.

Remark 1.22. One way of obtaining a primitive polynomial over $\mathbb{F}_q$ of degree n is to construct a primitive element of $\mathbb{F}_{q^n}$, and then determining the minimal polynomial of this element over $\mathbb{F}_q$.

1.6 Linear And Cyclic Codes

Information coming from some source is transmitted over a noisy communication channel to a receiver. For example: storage devices, wires, air, etc. There are a lot of important messages to be sent down those channels, and they must be sent as quickly and reliably as possible. In 1948, Claude Shannon published a landmark paper: A mathematical theory of communication [36], that signified the beginning of both information theory and coding theory. Shannon said that information can be encoded before transmission so that the corrupted data can be decoded. The fundamental problem in coding theory is to determine what message was sent on the basis of what is received. The purpose is to add redundancy to the information in order to recover it as accurately as possible after transmitting.
Among all types of codes, *linear code* are the most important for practical applications and are the simplest to understand.

Definition 1.15. A linear code C of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$.

Example 1.13. Consider the set

$$C = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\} \subset \mathbb{F}_2^3.$$

It is easy to check that C is a 2-dimensional subspace of $\mathbb{F}_2^3$ with $B = \{(1,1,0), (0,1,1)\}$ as a basis. Therefore, C is a linear code of length 3 over $\mathbb{F}_2$. We call the vectors in C codewords.

Definition 1.16. The *Hamming distance* $d(x,y)$ between two vectors $x, y \in \mathbb{F}_q^n$ is the number of coordinates in which x and y differ. That is

$$d(x,y) = |\{i : \ x_i \neq y_i, \ 1 \leq i \leq n\}|,$$

and the *weight* of x is $w(x) = d(x,0)$.

Proposition 1.10. [22, Theorem 1.4.1] For all $x, y, z \in \mathbb{F}_q^n$, the Hamming distance satisfies the following properties:

(i) (non-negativity) $d(x,y) \geq 0$.

(ii) $d(x,y) = 0$ if and only if $x = y$.

(iii) (symmetry) $d(x,y) = d(y,x)$.

(iv) (triangle inequality) $d(x,z) \leq d(x,y) + d(y,z)$.

An important parameter of a code C is the *minimum distance* between *codewords* which is given by

$$d = \min\{d(x,y) : \ x, y \in C, \ x \neq y\}.$$

For a linear code C, its minimum distance d is equal to its *minimum weight*, i.e.,

$$d = \min\{w(x) : \ x \in C, \ x \neq 0\}.$$

This distance is very important in determining the error-correcting capability of C. As we will see in the following proposition, the greater the minimum distance, the more errors the code can detect and correct.

Proposition 1.11. [22] A linear code C with a minimum distance d can detect up to $d-1$ errors and correct $\lfloor \frac{d-1}{2} \rfloor$ errors in a received message.

An extremely important class of linear codes are known as *cyclic codes*.

Definition 1.17. A linear code C of length n over $\mathbb{F}_q$ is called a cyclic code if

$$(c_0, c_1, \ldots, c_{n-1}) \in C \quad \text{implies that} \quad (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

We can identify a codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ with the polynomial

$$c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \in \frac{\mathbb{F}_q[x]}{(x^n - 1)}.$$

It is well-known that a linear code is cyclic if and only if the corresponding polynomial set is an ideal of the residue class ring $\frac{\mathbb{F}_q[x]}{(x^n-1)}$.

Definition 1.18. The unique monic polynomial which generates a cyclic code C is called the *generator polynomial* of C.

Example 1.14. The linear code C described in Example 1.13 is cyclic. Indeed, we can identify the codewords of C as polynomials of $\frac{\mathbb{F}_2[x]}{(x^3-1)}$ as follows:

$$\begin{aligned}(0,0,0) &:= 0 &&= (1+x).0,\\ (1,1,0) &:= 1+x &&= (1+x).1,\\ (0,1,1) &:= x+x^2 &&= (1+x)x,\\ (1,0,1) &:= 1+x^2 &&= (1+x)(1+x).\end{aligned}$$

Then, C is a cyclic code with the generator polynomial $1+x$.

Let n be a positive integer with $\gcd(n,q) = 1$. Recall that the $q-$cyclotomic coset of s modulo n is the set

$$C_s = \{s, sq, \cdots, sq^{r-1}\} \mod n,$$

where r is the smallest positive integer such that $sq^r = s \mod n$. The representative of a coset is the smallest element in the coset.

Let α be a primitive nth root of unity over $\mathbb{F}_q$, i.e., n is the smallest integer for which $\alpha^n = 1$ over $\mathbb{F}_q$.

Lemma 1.2. Let C be a nonzero cyclic code of length n over $\mathbb{F}_q$, and let $g(x)$ be the generator polynomial of C. Then:

1. We have that
$$x^n - 1 = \prod_{i\in S} \mathrm{Min}(\alpha^i, \mathbb{F}_q)(x)$$
is the factorization of $x^n - 1$ into irreducible factors over $\mathbb{F}_q$, where S is a set of represent atives of the $q-$cyclotomic cosets modulo n.

2. $g(x)$ divides $x^n - 1$ over $\mathbb{F}_q$.

3. Furthermore,
$$g(x) = \prod_{i\in T} \mathrm{Min}(\alpha^i, \mathbb{F}_q)(x),$$
where T is a subset of S.

Proof. 1. Since the α^i are distinct for $0 \le i < n$ and $(\alpha^i)^n = 1$, then

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i),$$

or equivalently

$$x^n - 1 = \prod_{i\in S} \mathrm{Min}(\alpha^i, \mathbb{F}_q)(x),$$

where S is a set of representatives of the $q-$cyclotomic cosets modulo n.

2. Let $x^n - 1 = g(x)h(x) + r(x)$ in $\mathbb{F}_q[x]$, where $\deg(r(x)) < \deg(g(x))$. As $x^n - 1$ corresponds to the zero codeword in C and C is an ideal in $\frac{\mathbb{F}_q[x]}{(x^n-1)}$, then $r(x) \in C$, a contradiction unless $r(x) = 0$. Hence, $g(x)$ divides $x^n - 1$ over $\mathbb{F}_q$.

3. This part follows from Parts 1 and 2.

□

Definition 1.19. The roots of unity $\{\alpha^i : i \in \cup_{i\in T} C_i\}$ are called the *zeros* of the cyclic code C, and $\{\alpha^i : i \notin \cup_{i\in T} C_i\}$ are the *nonzeros* of C. The set $\cup_{i\in T} C_i$ is called the *defining* set of C.

There are several known lower bounds for the minimum distance of a cyclic code. The oldest of these is the so-called *BCH bound*.

Theorem 1.15. [22, Theorem 4.5.3] Let C be a cyclic code of length n over $\mathbb{F}_q$ with defining set J. Suppose that C has minimum distance d. Assume that J contains $\delta - 1$ consecutive elements for some integer δ. Then $d \geq \delta$.

Before proceeding with the proof of this theorem, we state a lemma about the determinant of a *Vandermonde matrix*. For $\alpha_1, \alpha_2, \cdots, \alpha_s \in \mathbb{F}_q$, the $s \times s$ matrix $V = (v_{ij})$, where $v_{ij} = \alpha_j^{i-1}$ is called a Vandermonde matrix. Note that the transpose of this matrix is also called a Vandermonde matrix.

Lemma 1.3. [22, Lemma 4.5.1] We have

$$\det(V) = \prod_{1\leq i<j\leq s} (\alpha_i - \alpha_j).$$

In particular, V is nonsingular if the elements $\alpha_1, \alpha_2, \cdots, \alpha_s$ are distinct.

Now, we can give the proof of Theorem 1.15.

Proof. By assumption, C has zeros that include $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$, for some integer b. Let $c(x)$ be a nonzero codeword in C of weight w. We write $c(x)$ as follows:

$$c(x) = \sum_{j=1}^{w} c_{i_j} x^{i_j}.$$

Assume to the contrary that $w < \delta$. As $c(\alpha^i) = 0$ for $b \leq i \leq b + \delta - 2$, then $Mu^T = 0$, where

$$M = \begin{pmatrix} \alpha^{i_1 b} & \alpha^{i_2 b} & \cdots & \alpha^{i_w b} \\ \alpha^{i_1 (b+1)} & \alpha^{i_2 (b+1)} & \cdots & \alpha^{i_w (b+1)} \\ & & \vdots & \\ \alpha^{i_1 (b+w-1)} & \alpha^{i_2 (b+w-1)} & \cdots & \alpha^{i_w (b+w-1)} \end{pmatrix}$$

and $u = (c_{i_1}, c_{i_2}, \cdots, c_{i_w})$. Since $u \neq 0$, then M is a singular matrix and hence $\det(M) = 0$. On the other hand, we have

$$M = V. \begin{pmatrix} \alpha^{i_1 b} & 0 & \dots & 0 \\ 0 & \alpha^{i_2 b} & \dots & 0 \\ & & \vdots & \\ 0 & 0 & \dots & \alpha^{i_w b} \end{pmatrix},$$

where V is the Vandermonde matrix

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_w} \\ & & \vdots & \\ \alpha^{i_1(w-1)} & \alpha^{i_2(w-1)} & \dots & \alpha^{i_w(w-1)} \end{pmatrix}.$$

Therefore, $\det(M) = \alpha^{(i_1+i_2+\cdots+i_w)b} \det(V)$. Since the α^{i_j} are distinct, then, by Lemma 1.3, $\det(V) \neq 0$, contradicting $\det(M) = 0$. □

Cyclic codes are the most studied of all codes, since they are easy to encode, and include the important family of BCH codes, which we devoted Chapter 5 for some applications. Furthermore, they are building blocks for many other codes, such as the Kerdock, Preparata, and Justesen codes. We refer the reader to references [22] and [26] for basic concepts about these codes.

CHAPTER 2

CONSTRUCTION THROUGH AUTOMORPHISM

In this chapter, we extend the Frobenius automorphism φ of $\mathbb{F}_{q^m}$ to a ring automorphism of $\mathbb{F}_{q^m}[x]$. This extended automorphism will be used in order to construct irreducible polynomials over $\mathbb{F}_q$ of degree rm from an irreducible polynomial over $\mathbb{F}_{q^m}$ of degree r.

2.1 The Extended Frobenius Automorphism Φ

Let $V(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{F}_{q^m}[x]$. We can extend φ given by expression (1.1) to the following ring automorphism

$$\begin{aligned} \Phi : \mathbb{F}_{q^m}[x] &\to \mathbb{F}_{q^m}[x] \\ V(x) &\mapsto \Phi(V(x)) = \Phi(V)(x) = \sum_{i=0}^{r} \varphi(a_i) x^i = \sum_{i=0}^{r} a_i^q x^i. \end{aligned} \tag{2.1}$$

The automorphism Φ has some interesting properties as we will see in the next lemma, which will be useful later when we present a construction of irreducible polynomials over $\mathbb{F}_q$ through Φ.

Lemma 2.1. Let d be an integer such that $1 \leq d \leq m-1$. Then :

(i) We have

$$\Phi^d(V)(x) = \sum_{i=0}^{r} a_i^{q^d} x^i,$$

and $\Phi^d(V)(x) = V(x)$ if and only if $V(x) \in \mathbb{F}_{q^d}[x]$.

(ii) Let $\alpha \in \mathbb{F}_{q^{rm}}$. Then, $V(\alpha) = 0$ if and only if $\Phi^d(V)(\alpha^{q^d}) = 0$.

(iii) $V(x)$ is irreducible over $\mathbb{F}_{q^m}$ if and only if $\Phi^d(V)(x)$ is irreducible over $\mathbb{F}_{q^m}$.

(iv) Assume that $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$ (i.e., $\mathbb{F}_{q^m}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficients of $V(x)$). If j and k are two integers such that $0 \leq j < k \leq m-1$, then $\Phi^j(V)(x) \neq \Phi^k(V)(x)$.

Proof. (i) We have

$$\Phi^d(V)(x) = \Phi\left(\Phi^{d-1}(V)(x)\right) = \Phi\left(\sum_{i=0}^{r} a_i^{q^{d-1}} x^i\right) = \sum_{i=0}^{r} a_i^{q^d} x^i.$$

Therefore, $\Phi^d(V)(x) = V(x)$ if and only if $\sum_{i=0}^{r} a_i^{q^d} x^i = \sum_{i=0}^{r} a_i x^i$ if and only if $a_i^{q^d} = a_i$ for all $i = 0, \ldots, r$, which is equivalent to $V(x) \in \mathbb{F}_{q^d}[x]$.
(ii) Let $\alpha \in \mathbb{F}_{q^{rm}}$. Then, $V(\alpha) = 0$ if and only if $\sum_{i=0}^{r} a_i \alpha^i = 0$ if and only if

$$\left(\sum_{i=0}^{r} a_i \alpha^i\right)^{q^d} = \sum_{i=0}^{r} a_i^{q^d} (\alpha^{q^d})^i = \Phi^d(V)(\alpha^{q^d}) = 0.$$

(iii) Since Φ is an automorphism of $\mathbb{F}_{q^m}[x]$, then for any $Q(x), S(x) \in \mathbb{F}_{q^m}[x]$, $V(x) = Q(x)S(x)$ if and only if

$$\Phi^d(V)(x) = \Phi^d(Q \cdot S)(x) = \Phi^d(Q)(x) \cdot \Phi^d(S)(x).$$

Therefore, $V(x)$ is irreducible over $\mathbb{F}_{q^m}$ if and only if $\Phi^d(V)(x)$ is irreducible over $\mathbb{F}_{q^m}$.
(iv) Note that $\Phi^m(V)(x) = V(x)$. Then, for any two positive integers l and s with $0 \leq s \leq m-1$, we have

$$\Phi^{lm+s}(V)(x) = \Phi^{lm}\left(\Phi^s(V)(x)\right) = \Phi^s(V)(x).$$

Let j and k be two integers such that $0 \leq j < k \leq m-1$ and $\Phi^j(V)(x) = \Phi^k(V)(x)$. Then, $\Phi^{k-j}(V)(x) = V(x)$ and $V(x) \in \mathbb{F}_{q^{k-j}}[x]$, a contradiction, since $\mathbb{F}_{q^m}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficients of $V(x)$. □

2.2 A Construction Of Irreducible Polynomials Using Φ

It is useful to be able to decide whether an irreducible polynomial over a finite field remains irreducible over a certain finite extension field. For that, we have the following result.

Theorem 2.1. [24, Theorem 3.46] Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n and let k be a positive integer. Then, $f(x)$ factors into d irreducible polynomials in $\mathbb{F}_{q^k}[x]$ of the same degree n/d, where $d = \gcd(n, k)$.

Remark 2.1. Theorem 2.1 implies that, if $f(x)$ is irreducible over $\mathbb{F}_q$ of degree n and $\gcd(n, k) = 1$, then $f(x)$ remains irreducible over $\mathbb{F}_{q^k}$.

The following proposition is a restatement of Lemma 1 in [23], but we will give a somewhat different proof using the properties of the automorphism Φ. We would like to notice here that our representation, which is different from the one used in [23], turns out to be useful through the properties, stated previously, of the Frobenius automorphism extended to the ring of polynomials. Notice as well that the first implication is well known as a consequence

of Theorem 2.1, and the converse has been also proved in [29], where the authors introduced, for a given polynomial $V(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{F}_{q^m}[x]$, the notion of the *spin* of $V(x)$ by

$$\prod_{s=0}^{m-1} V^{(s)}(x),$$

where

$$V^{(s)}(x) = \sum_{i=0}^{r} a_i^{q^s} x^i,$$

which coincides with the product $\prod_{i=0}^{m-1} \Phi^i(V)(x)$ below.

Proposition 2.1. [14, Proposition 3.1] A monic polynomial $f(x)$ of degree rm is irreducible over $\mathbb{F}_q$ if and only if there exists a monic irreducible polynomial

$$V(x) = \sum_{i=0}^{r} a_i x^i$$

over $\mathbb{F}_{q^m}$ of degree r, such that $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$ and

$$f(x) = \prod_{i=0}^{m-1} \Phi^i(V)(x).$$

Proof. Let $V(x) = \sum_{i=0}^{r} a_i x^i$ be a monic irreducible polynomial over $\mathbb{F}_{q^m}$ of degree r and set $f(x) = \prod_{i=0}^{m-1} \Phi^i(V)(x)$. Since

$$\Phi(f)(x) = \prod_{i=0}^{m-1} \Phi^{i+1}(V)(x) = \prod_{i=1}^{m} \Phi^i(V)(x) = \prod_{i=0}^{m-1} \Phi^i(V)(x) = f(x),$$

then, by Part (i) of Lemma 2.1, $f(x)$ is a monic polynomial over $\mathbb{F}_q$ of degree rm. Let $\alpha \in \mathbb{F}_{q^{rm}}$ be a root of $V(x)$ and let $h(x) = \mathrm{Min}(\alpha, \mathbb{F}_q)(x)$. We will show that, if $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$, then $f(x) = h(x)$. Parts (ii) and (iii) of Lemma 2.1 imply that, for all $d \in \{0, 1, \ldots, m-1\}$,

$$\Phi^d(V)(x) = \prod_{i=0}^{r-1} (x - \alpha^{q^{im+d}}),$$

and

$$f(x) = \prod_{i=0}^{rm-1} (x - \alpha^{q^i}) = \prod_{i=0}^{m-1} \Phi^i(V)(x).$$

If $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$, by Part (iv) of Lemma 2.1, the elements α^{q^i} are distinct for all $i \in \{0, 1, \ldots, rm-1\}$. Therefore, $f(x) = h(x)$.
Conversely, let $f(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree rm. Let $\beta \in \mathbb{F}_{q^{rm}}$ be

a root of $f(x)$ and let $V(x) = \mathrm{Min}(\beta, \mathbb{F}_{q^m})(x)$. Since

$$\mathbb{F}_q(\beta) = \mathbb{F}_{q^{rm}} = \mathbb{F}_{q^m}(\beta),$$

then

$$\deg(V(x)) = [\mathbb{F}_{q^m}(\beta) : \mathbb{F}_{q^m}] = [\mathbb{F}_{q^{rm}} : \mathbb{F}_{q^m}] = r,$$

and $\mathbb{F}_{q^m}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficients of $V(x)$. Therefore, the first part of this proof implies that

$$f(x) = \prod_{i=0}^{m-1} \Phi^i(V)(x).$$

□

Example 2.1. Let $\theta \in \mathbb{F}_{3^2}$ be a primitive element such that $\theta^2 + 2\theta + 2 = 0$. We have $\mathbb{F}_3(\theta) = \mathbb{F}_{3^2}$. Consider the ring automorphism

$$\begin{aligned} \Phi : \mathbb{F}_{3^2}[x] &\to \mathbb{F}_{3^2}[x] \\ \sum_{i=0}^{n} a_i x^i &\mapsto \sum_{i=0}^{n} a_i^3 x^i. \end{aligned}$$

We take the irreducible polynomial $V(x) = x^3 + (2\theta + 2)x + \theta + 2 \in \mathbb{F}_{3^2}[x]$. Since $V(x) \notin \mathbb{F}_3[x]$, then according to Proposition 2.1, the polynomial

$$\begin{aligned} \Phi^0(V)(x) \cdot \Phi(V)(x) = V(x) \cdot \Phi(V)(x) &= (x^3 + (2\theta + 2)x + \theta + 2)(x^3 + (\theta + 1)x + 2\theta) \\ &= x^6 + 2x^3 + x^2 + x + 2 \end{aligned}$$

is irreducible over $\mathbb{F}_3$ of degree 6.

Remark 2.2. For an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree rm, if we can find an irreducible factor $V(x) \in \mathbb{F}_{q^m}[x]$ of $f(x)$, then, by Proposition 2.1, the remaining factors of $f(x)$ are $\Phi^i(V)(x)$, where $1 \leq i \leq m-1$.

Lemma 2.2. If $V(x) = \sum_{i=0}^{r} a_i x^i$ is primitive over $\mathbb{F}_{q^m}$, then $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$.

Proof. Suppose that $V(x)$ is primitive over $\mathbb{F}_{q^m}$ and $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^s} \subsetneq \mathbb{F}_{q^m}$. Then, $V(x)$ is irreducible over $\mathbb{F}_{q^s}$. Therefore, $\mathrm{ord}(V(x)) \leq q^{rs} - 1 < q^{rm} - 1$, a contradiction since $V(x)$ is primitive over $\mathbb{F}_{q^m}$. □

Proposition 2.1 can also be used to construct primitive polynomials, as we will see in the following corollary.

Corollary 2.1. [14, Corollary 3.1] A polynomial $f(x)$ of degree rm is primitive over $\mathbb{F}_q$ if and only if there exists a primitive polynomial $V(x)$ over $\mathbb{F}_{q^m}$ of degree r such that

$$f(x) = \prod_{i=0}^{m-1} \Phi^i(V)(x).$$

Proof. Using Proposition 2.1, Lemma 2.2 and the fact that the roots of $V(x)$ are also roots of $f(x)$, we obtain that $f(x)$ is primitive if and only if $V(x)$ is primitive. □

Example 2.2. Let $\theta \in \mathbb{F}_{2^2}$ be the primitive element verifying $\theta^2 + \theta + 1 = 0$. We have $\mathbb{F}_2(\theta) = \mathbb{F}_{2^2}$. Consider the ring automorphism

$$\begin{aligned} \Phi : \mathbb{F}_{2^2}[x] &\to \mathbb{F}_{2^2}[x] \\ \sum_{i=0}^{n} a_i x^i &\mapsto \sum_{i=0}^{n} a_i^2 x^i. \end{aligned}$$

Let $V(x) = x^4 + x^2 + (\theta+1)x + \theta \in \mathbb{F}_{2^2}[x]$ be a primitive polynomial over $\mathbb{F}_{2^2}$. Then, according to Corollary 2.1, the polynomial

$$\begin{aligned} \Phi^0(V)(x) \cdot \Phi(V)(x) = V(x) \cdot \Phi(V)(x) &= (x^4 + x^2 + (\theta+1)x + \theta)(x^4 + x^2 + \theta x + \theta + 1) \\ &= x^8 + x^5 + x^3 + x + 1 \end{aligned}$$

is primitive over $\mathbb{F}_2$ of degree 8.

2.3 Some Irreducible Polynomials Over $\mathbb{F}_q$

In this section, we will exploit Proposition 2.1 in order to produce irreducible polynomials over $\mathbb{F}_q$.

Theorem 2.2. [24, Theorem 3.75] Let $r \geq 2$ be an integer and $a \in \mathbb{F}_q^*$. Then, the binomial $x^r - a$ is irreducible over $\mathbb{F}_q$ if and only if the following two conditions are satisfied:

(i) each prime factor of r divides the order e of a in $\mathbb{F}_q^*$, but not $\frac{q-1}{e}$.

(ii) If $r \equiv 0 \bmod 4$, then $q \equiv 1 \bmod 4$.

Using this theorem, we obtain the following corollary.

Corollary 2.2. [14, Corollary 3.2] Let $a \in \mathbb{F}_{q^m}$ such that $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$, and let $r \geq 2$ be an integer. Then, the polynomial

$$f(x) = \prod_{i=0}^{m-1} (x^r - a^{q^i})$$

is irreducible over $\mathbb{F}_q$ of degree rm if and only if the following two conditions are satisfied:

(i) each prime factor of r divides the order e of a in $\mathbb{F}_{q^m}^*$, but not $\frac{(q^m-1)}{e}$.

(ii) If $r \equiv 0 \bmod 4$, then $q^m \equiv 1 \bmod 4$.

Proof. The condition $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$ implies that $\mathbb{F}_{q^m}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficents of the binomial $x^r - a$. Then, according to Proposition 2.1, we have that $f(x)$ is irreducible over $\mathbb{F}_q$ of degree rm if and only if $x^r - a$ is irreducible over $\mathbb{F}_{q^m}$ of degree r. Theorem 2.2 then yields the result. □

Remark 2.3. The polynomial $f(x)$ in Corollary 2.2 can never be primitive, since for any $r \geq 2$, we have

$$\mathrm{ord}(f(x)) = \mathrm{ord}(x^r - a).$$

On the other hand, if $\alpha \in \mathbb{F}_{q^{rm}}$ is a root of $x^r - a$, then $\alpha^r = a$ and

$$\alpha^{r(q^m-1)} = a^{q^m-1} = 1.$$

Therefore,

$$\mathrm{ord}(f(x)) = \mathrm{ord}(x^r - a) \leq r \cdot (q^m - 1) < q^{rm} - 1,$$

and the order of a primitive polynomial over $\mathbb{F}_q$ of degree rm is $q^{rm} - 1$.

Example 2.3. Take $q = m = 2$ and $a \in \mathbb{F}_4$ such that $a^2 + a + 1 = 0$. The order of a in $\mathbb{F}_4^*$ is 3. Then, by taking $r = 3^k$, where k is a positive integer, we obtain the well known class of irreducible polynomials over $\mathbb{F}_2$

$$(x^{3^k} + a) \cdot (x^{3^k} + a^2) = x^{2 \cdot 3^k} + x^{3^k} + 1.$$

In Table 2.1 (resp. Table 2.2), a is an element of $\mathbb{F}_{2^m}$ (resp. $\mathbb{F}_{3^m}$) with $\mathbb{F}_{q^m} = \mathbb{F}_q(a)$, $g(x) = \mathrm{Min}(a, \mathbb{F}_q)(x)$ and $f(x)$ is a monic irreducible polynomial over $\mathbb{F}_q$ of the form $\prod_{i=0}^{m-1}(x^r - a^{q^i})$.

Lemma 2.3. [24, Corollary 3.79] The trinomial $x^p - x - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if $\mathrm{Tr}_q(a) \neq 0$.

This lemma implies the following corollary.

Corollary 2.3. [14, Corollary 3.3] Let $a \in \mathbb{F}_{q^m}$ such that $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$. Then, the polynomial

$$f(x) = \prod_{i=0}^{m-1}(x^p - x - a^{q^i})$$

is irreducible over $\mathbb{F}_q$ of degree pm if and only if $\mathrm{Tr}_{q^m}(a) \neq 0$. Furthermore, $x^p - x - a$ is primitive over $\mathbb{F}_{q^m}$ if and only if $f(x)$ is primitive over $\mathbb{F}_q$.

Proof. The condition $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$ implies that $\mathbb{F}_{q^m}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficents of the trinomial $x^p - x - a$. Then, according to Proposition 2.1, we have that $f(x)$ is irreducible over $\mathbb{F}_q$ of degree pm if and only if $x^p - x - a$ is irreducible over $\mathbb{F}_{q^m}$ of degree p. Lemma 2.3 then yields the result. □

When $m = 2$, Corollary 2.3 implies the following result.

Corollary 2.4. [14, Corollary 3.4] Let q be a power of an odd prime p and let $a, b \in \mathbb{F}_q^*$. Then, the polynomial

$$f(x) = x^{2p} - 2x^{p+1} - ax^p + x^2 + ax - b$$

is irreducible over $\mathbb{F}_q$ if and only if $a^2 + 4b$ is a non-square in $\mathbb{F}_q$ and $\mathrm{Tr}_q(a) \neq 0$.

TABLE 2.1: Irreducible polynomials over $\mathbb{F}_2$ from the product of irreducible binomials over $\mathbb{F}_{2^m}$

m	$g(a)=0$	r	$f(x)$
2	$a^2+a+1=0$	3^k	$x^{2\cdot 3^k}+x^{3^k}+1$
3	$a^3+a+1=0$	7^k	$x^{3\cdot 7^k}+x^{7^k}+1$
3	$a^3+a^2+1=0$	7^k	$x^{3\cdot 7^k}+x^{2\cdot 7^k}+1$
4	$a^4+a+1=0$	$3^k\cdot 5^l$	$x^{4\cdot 3^k\cdot 5^l}+x^{3^k\cdot 5^l}+1$
4	$a^4+a^3+1=0$	$3^k\cdot 5^l$	$x^{4\cdot 3^k 5^l}+x^{3^{k+1}\cdot 5^l}+1$
4	$a^4+a^3+a^2+a+1=0$	5^k	$x^{4\cdot 5^k}+x^{3\cdot 5^k}+x^{2\cdot 5^k}+x^{5^k}+1$
5	$a^5+a^2+1=0$	31^k	$x^{5\cdot 31^k}+x^{2\cdot 31^k}+1$
5	$a^5+a^3+1=0$	31^k	$x^{5\cdot 31^k}+x^{3\cdot 31^k}+1$
5	$a^5+a^3+a^2+a+1=0$	31^k	$x^{5\cdot 31^k}+x^{3\cdot 31^k}+x^{2\cdot 31^k}+x^{31^k}+1$
5	$a^5+a^4+a^2+a+1=0$	31^k	$x^{5\cdot 31^k}+x^{4\cdot 31^k}+x^{2\cdot 31^k}+x^{31^k}+1$
5	$a^5+a^4+a^3+a^2+1=0$	31^k	$x^{5\cdot 31^k}+x^{4\cdot 31^k}+x^{3\cdot 31^k}+x^{2\cdot 31^k}+1$
5	$a^5+a^4+a^3+a+1=0$	31^k	$x^{5\cdot 31^k}+x^{4\cdot 31^k}+x^{3\cdot 31^k}+x^{31^k}+1$

TABLE 2.2: Irreducible polynomials over $\mathbb{F}_3$ from the product of irreducible binomials over $\mathbb{F}_{3^m}$

m	$g(a)=0$	r	$f(x)$
2	$a^2+a+2=0$	2^k	$x^{2^{k+1}}+x^{2^k}+2$
2	$a^2+2a+2=0$	2^k	$x^{2^{k+1}}+2x^{2^k}+2$
3	$a^3+2a+1=0$	13^k	$x^{3\cdot 13^k}+2x^{13^k}+1$
3	$a^3+2a+1=0$	$2\cdot 13^k$	$x^{6\cdot 13^k}+2x^{2\cdot 13^k}+1$
3	$a^3+2a+2=0$	13^k	$x^{3\cdot 13^k}+2x^{13^k}+2$
3	$a^3+a^2+a+2=0$	13^k	$x^{3\cdot 13^k}+x^{2\cdot 13^k}+x^{13^k}+2$
3	$a^3+a^2+2a+1=0$	13^k	$x^{3\cdot 13^k}+x^{2\cdot 13^k}+2x^{13^k}+1$
3	$a^3+a^2+2a+1=0$	$2\cdot 13^k$	$x^{6\cdot 13^k}+x^{4\cdot 13^k}+2x^{2\cdot 13^k}+1$
3	$a^3+2a^2+a+1=0$	13^k	$x^{3\cdot 13^k}+2x^{2\cdot 13^k}+x^{13^k}+1$
3	$a^3+2a^2+a+1=0$	$2\cdot 13^k$	$x^{6\cdot 13^k}+2x^{4\cdot 13^k}+x^{2\cdot 13^k}+1$
3	$a^3+2a^2+2a+2=0$	13^k	$x^{3\cdot 13^k}+2x^{2\cdot 13^k}+2x^{13^k}+2$

Proof. Consider $u(x)=x^2-ax-b\in\mathbb{F}_q[x]$ and let $\alpha\in\mathbb{F}_{q^2}$ be any root of $u(x)$. Then, by Corollary 2.3, we have that $u(x)$ is irreducible over $\mathbb{F}_q$ and $\mathrm{Tr}_{q^2}(\alpha)\neq 0$ if and only if

$$f(x)=(x^p-x-\alpha)(x^p-x-\alpha^q)$$

is irreducible over $\mathbb{F}_q$. Therefore, $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if a^2+4b is a non-square in $\mathbb{F}_q$ and

$$\mathrm{Tr}_{q^2}(\alpha)=\mathrm{Tr}_q\left(\mathrm{Tr}_{q^2|q}(\alpha)\right)=\mathrm{Tr}_q(a)\neq 0.$$

□

Lemma 2.4. [8, Corollary 3.6] For $a, b \in \mathbb{F}_q^*$, the trinomial $x^p - ax - b$ is irreducible over $\mathbb{F}_q$ if and only if $a = A^{p-1}$ for some $A \in \mathbb{F}_q^*$ and $\mathrm{Tr}_q\left(\frac{b}{A^p}\right) \neq 0$.

In particular, if $q = 2^s$ for some positive integer s, then the trinomial $x^2 + ax + b$ is irreducible over $\mathbb{F}_q$ if and only if $\mathrm{Tr}_q\left(\frac{b}{a^2}\right) \neq 0$.

Corollary 2.5. [14, Corollary 3.5] Let $q = 2^s$, where s is a positive integer. Let $a, b \in \mathbb{F}_q^*$. Then, the polynomial $x^4 + (a+1)x^2 + ax + b$ is irreducible over $\mathbb{F}_q$ if and only if $\mathrm{Tr}_q\left(\frac{b}{a^2}\right) \neq 0$ and $\mathrm{Tr}_q(a) \neq 0$.

Proof. Using a similar proof as in Corollary 2.4, Lemma 2.4 then yields the result. □

2.4 Cohen's Theorem Generalization

The following theorem, known as Cohen's theorem, has been used by many authors in order to construct irreducible polynomials over $\mathbb{F}_q$ of higher degree (see, e.g., [1],[23],[27]). The main idea in the mentioned references is to make the polynomial $g(x) - \alpha h(x)$ to be a known irreducible polynomial, say a binomial or a trinomial using existent results.

Theorem 2.3. [15, Lemma 1] Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n. Let $g(x), h(x) \in \mathbb{F}_q[x]$ be relatively prime polynomials with $h(x) \neq 0$. Then, the composition

$$h(x)^n \cdot f\left(\frac{g(x)}{h(x)}\right)$$

is irreducible over $\mathbb{F}_q$ if and only if the polynomial $g(x) - \alpha h(x)$ is irreducible over $\mathbb{F}_{q^n}$ for any root $\alpha \in \mathbb{F}_{q^n}$ of $f(x)$.

Proof. Let $\alpha \in \mathbb{F}_{q^n}$ be a root of $f(x)$, and set $V(x) = g(x) - \alpha h(x) \in \mathbb{F}_{q^n}[x]$. Then, we have

$$f(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}),$$

and

$$\begin{aligned} F(x) = h(x)^n \cdot f\left(\frac{g(x)}{h(x)}\right) &= \prod_{i=0}^{n-1} \left(g(x) - \alpha^{q^i} h(x)\right) \\ &= \prod_{i=0}^{n-1} \Phi^i(V)(x). \end{aligned}$$

Note that $\mathbb{F}_{q^n}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficients of $V(x)$. Then, according to Proposition 2.1, the polynomial $F(x)$ is irreducible over $\mathbb{F}_q$ if and only if the polynomial $V(x)$ is irreducible over $\mathbb{F}_{q^n}$. □

Example 2.4. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree n, and let $\alpha \in \mathbb{F}_{q^n}$ be a root $f(x)$. We will show that the polynomial $f(x^p - x)$ is irreducible over $\mathbb{F}_q$ of degree pn if and only if $\mathrm{Tr}_q(a_{n-1}) \neq 0$. According to Cohen's Theorem, $f(x^p - x)$ is irreducible over $\mathbb{F}_q$ if and only if $x^p - x - \alpha$ is irreducible over $\mathbb{F}_{q^n}$. Then, Lemma 2.3 implies that $x^p - x - \alpha$ is irreducible over $\mathbb{F}_{q^n}$ if and only if $\mathrm{Tr}_{q^n}(\alpha) \neq 0$, or equivalently

$$\mathrm{Tr}_{q^n}(\alpha) = \mathrm{Tr}_q\left(\mathrm{Tr}_{q^n|q}(\alpha)\right) = -\mathrm{Tr}_q(a_{n-1}) \neq 0,$$

since $\mathrm{Tr}_{q^n|q}(\alpha) = -a_{n-1}$.

In the next proposition, we give a generalization of Cohen's Theorem. For this, we need to extend the automorphism Φ given by expression (2.1) to the field of rational functions $\mathbb{F}_{q^m}(x)$ as follows

$$\begin{aligned} \Phi : \mathbb{F}_{q^m}(x) &\to \mathbb{F}_{q^m}(x) \\ \frac{g(x)}{h(x)} &\mapsto \Phi\left(\frac{g}{h}\right)(x) := \frac{\Phi(g)(x)}{\Phi(h)(x)}, \end{aligned}$$

with $h(x) \neq 0$. It is not hard to check that Φ is an automorphism of $\mathbb{F}_{q^m}(x)$.

Proposition 2.2. [14, Proposition 3.2] Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree rm, and let $v(x)$ be an irreducible factor of $f(x)$ over $\mathbb{F}_{q^m}$ of degree r. Let $g(x), h(x) \in \mathbb{F}_q[x]$ be relatively prime polynomials with $h(x) \neq 0$. Then, the composition

$$F(x) = h(x)^{rm} \cdot f\left(\frac{g(x)}{h(x)}\right)$$

is irreducible (resp. primitive) over $\mathbb{F}_q$ if and only if

$$V(x) = h(x)^{r} \cdot v\left(\frac{g(x)}{h(x)}\right)$$

is irreducible (resp. primitive) over $\mathbb{F}_{q^m}$, and $\mathbb{F}_{q^m}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficients of $V(x)$.

Proof. Proposition 2.1 implies that

$$f(x) = \prod_{i=0}^{m-1} \Phi^i(v)(x).$$

Then, we have:

$$\begin{aligned}\prod_{i=0}^{m-1}\Phi^i(V)(x) &= \prod_{i=0}^{m-1}\Phi^i\left(h^r\cdot v\left(\frac{g}{h}\right)\right)(x)\\ &= \prod_{i=0}^{m-1}\Phi^i(h^r)(x)\cdot\Phi^i\left(v\left(\frac{g}{h}\right)\right)(x)\\ &= \prod_{i=0}^{m-1}h(x)^r\cdot\Phi^i(v)\left(\frac{g(x)}{h(x)}\right)\\ &= h(x)^{rm}\cdot f\left(\frac{g(x)}{h(x)}\right)=F(x).\end{aligned}$$

By Proposition 2.1, we have that $F(x)$ is irreducible (resp. primitive) over $\mathbb{F}_q$ if and only if $V(x)$ is irreducible (resp. primitive) over $\mathbb{F}_{q^m}$, and $\mathbb{F}_{q^m}$ is the smallest extension of $\mathbb{F}_q$ containing the coefficients of $V(x)$. □

Remark 2.4. As pointed out in [23], Proposition 2.2 gives an immediate proof for Cohen's theorem by taking $v(x)=x-\alpha$, where $\alpha\in\mathbb{F}_{q^{rm}}$ is a root of $f(x)$.

CHAPTER 3

CONSTRUCTION BY COMPANION MATRIX

As we have seen so far, irreducible polynomials can be constructed using the Frobenius automorphism, or the composition method using Cohen's theorem. In this chapter, we will give a generalization to irreducible polynomials for a construction of primitive polynomials based on the companion matrix established in [13]. The advantage of this construction is that, given an irreducible (resp. primitive) polynomial over $\mathbb{F}_{q^m}$ of degree r, we obtain multiple (resp. all) irreducible polynomials over $\mathbb{F}_q$ of degree rm.

Let $u(x)$ be a primitive polynomial over $\mathbb{F}_q$ of degree m and let β be a root of $u(x)$. Then, we have

$$\mathbb{F}_{q^m} = \left\{0, 1, \beta, \beta^2, \ldots, \beta^{q^m-2}\right\}.$$

Let $\mathbf{C}_u$ be the companion matrix of $u(x)$. Then, we can see the elements of $\mathbb{F}_{q^m}$ as matrices through the field isomorphism (see [13])

$$\begin{aligned} \psi : \mathbb{F}_{q^m} &\to \mathbb{F}_q[\mathbf{C}_u] \\ \beta &\mapsto \mathbf{C}_u. \end{aligned}$$

This isomorphism can be extended to the ring isomorphism

$$\begin{aligned} \Psi : \mathrm{Mat}_{r\times r}(\mathbb{F}_{q^m}) &\to \mathrm{Mat}_{r\times r}(\mathbb{F}_q[\mathbf{C}_u]) \\ (a_{i,j}) &\mapsto \left(\psi(a_{i,j})\right). \end{aligned}$$

3.1 Main Construction

The next theorem, which is the main result in [13], gives a construction of a primitive polynomial over $\mathbb{F}_q$ from a given one over $\mathbb{F}_{q^m}$. The key idea is to transform the companion matrix of the primitive polynomial over $\mathbb{F}_{q^m}$ into a matrix with coefficients in $\mathbb{F}_q$ using the isomorphism Ψ.

Theorem 3.1. [13] Let $\mathbf{C}_v$ be the companion matrix of a primitive polynomial $V(x)$ over $\mathbb{F}_{q^m}$ of degree r. Then, the polynomial

$$\det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v)\right)$$

is primitive over $\mathbb{F}_q$ of degree rm.

Remark 3.1. Theorem 3.1 can also be obtained from the proof of [18, Theorem 6.1].

Now, we will see that this construction remains true for irreducible polynomials, and we show that, in fact, the constructions made in Theorem 3.1 and Proposition 2.1 are the same.

Theorem 3.2. [14, Theorem 4.2] Let $V(x) = \sum_{i=0}^{r} a_i x^i$ be a monic polynomial over $\mathbb{F}_{q^m}$ of degree r, and let $\mathbf{C}_v$ be its companion matrix. Then, the polynomial

$$\det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v)\right)$$

is irreducible over $\mathbb{F}_q$ of degree rm if and only if $V(x)$ is irreducible over $\mathbb{F}_{q^m}$ and $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$, and in this case we have the decomposition

$$\det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v)\right) = \prod_{i=0}^{m-1} \Phi^i(V)(x).$$

Proof. Set $h(x) = \det(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v))$. Note that since $\Psi(\mathbf{C}_v) \in \mathrm{Mat}_{rm\times rm}(\mathbb{F}_q)$, then $h(x) \in \mathbb{F}_q[x]$ is monic of degree rm. Let us write $h(x) = \sum_{i=0}^{rm} h_i x^i \in \mathbb{F}_q[x]$. We have

$$\begin{aligned}\Psi\left(h(\mathbf{C}_v)\right) = \Psi\left(\sum_{i=0}^{rm} h_i \mathbf{C}_v^i\right) &= \sum_{i=0}^{rm} h_i \Psi(\mathbf{C}_v)^i \\ &= h\left(\Psi(\mathbf{C}_v)\right) = \mathbf{O}_{rm}.\end{aligned}$$

As Ψ is a ring isomorphism, then $h(\mathbf{C}_v) = \mathbf{O}_r$. Therefore, $h(x)$ is the minimal polynomial of $\mathbf{C}_v$ over $\mathbb{F}_q$ if and only if $\mathbb{F}_q[\mathbf{C}_v] \cong \mathbb{F}_{q^{rm}}$, if and only if $V(x)$ is irreducible over $\mathbb{F}_{q^m}$ and $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$, and in this case, by Proposition 2.1, we have

$$\det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v)\right) = \prod_{i=0}^{m-1} \Phi^i(V)(x).$$

□

Example 3.1. Taking again $V(x) = x^3 + (2\theta+2)x + \theta + 2 \in \mathbb{F}_{3^2}[x]$ as described in Example 2.1, the polynomial $u(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$ is primitive having θ as a root. Let

$$\mathbf{C}_u = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{F}_3)$$

be the companion matrix of $u(x)$. Then, we can see the elements of $\mathbb{F}_{3^2}$ as matrices through the field isomorphism

$$\begin{aligned}\psi : \mathbb{F}_{3^2} &\to \mathbb{F}_3[\mathbf{C}_u] \\ \theta &\mapsto \mathbf{C}_u,\end{aligned}$$

and we have

$$\mathbb{F}_3[\mathbf{C}_u] = \{\mathbf{O}, \mathbf{I}, 2\mathbf{I}, \mathbf{C}_u, \mathbf{I}+\mathbf{C}_u, 2\mathbf{I}+\mathbf{C}_u, 2\mathbf{C}_u, \mathbf{I}+2\mathbf{C}_u, 2\mathbf{I}+2\mathbf{C}_u\}.$$

The companion matrix of $V(x)$ is

$$\mathbf{C}_v = \begin{pmatrix} 0 & 0 & 2\theta+1 \\ 1 & 0 & \theta+1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{F}_{3^2}).$$

Therefore,

$$\Psi(\mathbf{C}_v) = \begin{pmatrix} \psi(0) & \psi(0) & \psi(2\theta+1) \\ \psi(1) & \psi(0) & \psi(\theta+1) \\ \psi(0) & \psi(1) & \psi(0) \end{pmatrix} = \left(\begin{array}{cc:cc:cc} 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ \hdashline 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ \hdashline 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right) \in \mathrm{Mat}_{6\times 6}(\mathbb{F}_3).$$

Since $V(x) \notin \mathbb{F}_3[x]$, then the polynomial

$$\det\left(x\mathbf{I}_6 - \Psi(\mathbf{C}_v)\right) = \begin{vmatrix} x & 0 & 0 & 0 & 2 & 1 \\ 0 & x & 0 & 0 & 1 & 0 \\ 2 & 0 & x & 0 & 2 & 2 \\ 0 & 2 & 0 & x & 2 & 1 \\ 0 & 0 & 2 & 0 & x & 0 \\ 0 & 0 & 0 & 2 & 0 & x \end{vmatrix} = x^6 + 2x^3 + x^2 + x + 2$$

is irreducible over $\mathbb{F}_3$ of degree 6, and we have

$$\begin{aligned} \prod_{i=0}^{1} \Phi^i(V)(x) = \Phi^0(V)(x) \cdot \Phi(V)(x) &= V(x) \cdot \Phi(V)(x) \\ &= \left(x^3 + (2\theta+2)x + \theta + 2\right)\left(x^3 + (\theta+1)x + 2\theta\right) \\ &= x^6 + 2x^3 + x^2 + x + 2 \\ &= \det(x\mathbf{I}_6 - \Psi(\mathbf{C}_v)). \end{aligned}$$

In order to reduce the complexity of the computation of the determinant considered in the previous theorem, we give the following corollary.

Corollary 3.1. [14, Corollary 4.1] Let $a_0, a_1, \ldots, a_r \in \mathbb{F}_{q^m}$ such that $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$. Then, the polynomial $\sum_{i=0}^{r} a_i x^i$ is monic irreducible over $\mathbb{F}_{q^m}$ of degree r if and only if the polynomial

$$\det\left(\sum_{i=0}^{r} \psi(a_i) x^i\right)$$

is monic irreducible over $\mathbb{F}_q$ of degree rm.

Proof. This follows from Theorem 3.2 and the fact that (see the proof of Corollary 3.2 in [13])

$$\det\left(\sum_{i=0}^{r} \psi(a_i) x^i\right) = \det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{M})\right),$$

where $\mathbf{M}$ is the companion matrix of the polynomial $\sum_{i=0}^{r} a_i x^i$. □

Example 3.2. We take again the polynomial $V(x)$ and the isomorphism ψ given in Example 3.1. Then, we have

$$\begin{aligned}\det\left(\psi(\theta+2)+\psi(2\theta+2)x+\psi(0)x^2+\psi(1)x^3\right) &= \det\left(\begin{pmatrix}2&1\\1&0\end{pmatrix}+\begin{pmatrix}2&2\\2&1\end{pmatrix}x+\begin{pmatrix}1&0\\0&1\end{pmatrix}x^3\right)\\ &= \begin{vmatrix}2+2x+x^3 & 1+2x\\ 1+2x & x+x^3\end{vmatrix}\\ &= 2+x+x^2+2x^3+x^6.\end{aligned}$$

3.2 Generating Multiple Irreducible Poylnomials

As we have mentioned before, the constructions made in Proposition 2.1 and Theorem 3.2 are the same. However, This last construction has the advantage of producing multiple irreducible poylnomials from a given irreducible polynomial as we will see.

Definition 3.1. For a positive integer e such that $\gcd(e,q)=1$, the least positive integer m for which e divides q^m-1 is called the multiplicative order of q modulo e, and denoted by $m=\mathrm{ord}_e(q)$.

Let e be a divisor of $q^{rm}-1$ such that $rm=\mathrm{ord}_e(q)$, we define

$$D_e=\left\{\frac{se}{e'}(\mathrm{mod}\ e) : e' \textit{ divides } e; rm=\mathrm{ord}_{e'}(q); \gcd(s,e')=1\right\}.$$

When the class of an integer k modulo e is in D_e, we simply write $k\in D_e$. Note that D_e is not empty, since for $s=1$ and $e=e'$ we have $1\in D_e$.

Example 3.3. For $(q,r,m)=(2,2,3)$, we have :

$$\begin{aligned}D_9 &= \{1,2,4,5,7,8\},\\ D_{21} &= \{1,2,4,5,8,10,11,13,16,17,19,20\},\\ D_{63} &= \{1,2,3,4,5,6,7,8,10,11,12,13,14,15,16,17,19,20,22,23,24,25,26,28,29,30,31,32,33,\\ &\quad 34,35,37,38,39,40,41,43,44,46,47,48,49,50,51,52,53,55,56,57,58,59,60,61,62\}.\end{aligned}$$

In the following corollary, we show how to generate multiple irreducible polynomials over $\mathbb{F}_q$ of degree rm from an irreducible polynomial over $\mathbb{F}_{q^m}$ of degree r, using its companion matrix.

Corollary 3.2. [14, Corollary 4.2] Let $V(x)=\sum_{i=0}^{r} a_i x^i \in \mathbb{F}_{q^m}[x]$ be a monic irreducible polynomial of degree r with $\mathbb{F}_q(a_0,a_1,\ldots,a_r)=\mathbb{F}_{q^m}$. Let $\mathbf{C}_v$ be the companion matrix of $V(x)$ and $e=\mathrm{ord}(\mathbf{C}_v)$, the order of $\mathbf{C}_v$ in $\mathrm{GL}_r(\mathbb{F}_{q^m})$. Let $k\in\mathbb{N}$. Then, the polynomial

$$\det\left(x\mathbf{I}_{rm}-\Psi(\mathbf{C}_v^k)\right)$$

is irreducible over $\mathbb{F}_q$ of degree rm if and only if $k \in D_e$. Moreover, if $k = \frac{se}{e'} \in D_e$, then

$$\operatorname{ord}\left(\det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v^k)\right)\right) = e'.$$

Proof. As in the proof of Theorem 3.2, we have that $\det(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v^k))$ is irreducible over $\mathbb{F}_q$ if and only if $\mathbb{F}_q[\mathbf{C}_v^k] \cong \mathbb{F}_{q^{rm}}$, if and only if $k = \frac{se}{e'} \in D_e$, where $e' = \operatorname{ord}(\mathbf{C}_v^k)$. □

Example 3.4. Set $(q, m, r) = (2, 3, 3)$ and let $a \in \mathbb{F}_{2^3}$ be a primitive element such that $a^3 + a + 1 = 0$. Consider the irreducible polynomial $V(x) = x^3 + ax + 1 \in \mathbb{F}_{2^3}[x]$ and its companion matrix

$$\mathbf{C}_v = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & a \\ 0 & 1 & 0 \end{pmatrix}.$$

Then, we obtain all the irreducible polynomials over $\mathbb{F}_2$ of degree 9 and order 73, which we list in Table 3.1.

TABLE 3.1:
All irreducible polynomials over $\mathbb{F}_2$ of degree 9 and order 73.

k	$\det(x\mathbf{I}_9 - \Psi(\mathbf{C}_v^k))$
1	$x^9 + x + 1$
3	$x^9 + x^4 + x^2 + x + 1$
5	$x^9 + x^6 + x^3 + x + 1$
9	$x^9 + x^6 + x^5 + x^2 + 1$
11	$x^9 + x^7 + x^4 + x^3 + 1$
13	$x^9 + x^8 + 1$
17	$x^9 + x^8 + x^6 + x^3 + 1$
25	$x^9 + x^8 + x^7 + x^5 + 1$

The next corollary shows that, if a primitive polynomial over $\mathbb{F}_{q^m}$ of degree r is given, then we obtain all irreducible polynomials over $\mathbb{F}_q$ of degree rm.

Corollary 3.3. [14, Corollary 4.3] Let $\mathbf{C}_v$ be the companion matrix of a primitive polynomial $V(x)$ over $\mathbb{F}_{q^m}$ of degree r. Then, the set of all monic irreducible polynomials over $\mathbb{F}_q$ of degree rm is given by

$$\left\{\det(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v^k)) : k \in D_{q^{rm}-1}\right\}.$$

Moreover, the set of all primitive polynomials over $\mathbb{F}_q$ of degree rm is given by

$$\left\{\det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v^k)\right) : 1 \le k \le q^{rm} - 1; \gcd(k, q^{rm} - 1) = 1\right\}.$$

Proof. Since $\operatorname{ord}(\mathbf{C}_v) = q^{rm} - 1$, then for any monic irreducible polynomial $P(x)$ over $\mathbb{F}_q$ of degree rm, we can view $\mathbf{C}_v^k$ as its root for some $1 \le k \le q^{rm} - 1$. In this case we have

$\mathbb{F}_q[\mathbf{C}_v^k] \cong \mathbb{F}_{q^{rm}}$, which is equivalent to $k \in D_{q^{rm}-1}$. Therefore, $P(x) = \det(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v^k))$. Moreover, it is clear that $P(x)$ is primitive if and only if $\mathrm{ord}(\mathbf{C}_v^k) = q^{rm} - 1$, if and only if $\gcd(k, q^{rm} - 1) = 1$. □

Example 3.5. Consider the primitive polynomial $V(x) = x^3 + x + a \in \mathbb{F}_{2^3}[x]$, where $a^3 + a + 1 = 0$ as in Example 3.4. The companion matrix of $V(x)$ is given by

$$\mathbf{C}_v = \begin{pmatrix} 0 & 0 & a \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then, using the matrix $\mathbf{C}_v$ and Corollary 3.3, we obtain all irreducible polynomials over $\mathbb{F}_2$ of degree 9 which we list in Table 3.2.

Remark 3.2. Corollary 3.3 implies that the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree rm depends only on the set $D_{q^{rm}-1}$.

TABLE 3.2: All irreducible polynomials over $\mathbb{F}_2$ of degree 9 and order e.

k	$\det(x\mathbf{I}_9 - \Psi(\mathbf{C}_v^k))$	e	k	$\det(x\mathbf{I}_9 - \Psi(\mathbf{C}_v^k))$	e
1	$x^9+x^7+x^5+x+1$	511	61	$x^9+x^8+x^6+x^4+x^3+x+1$	511
3	$x^9+x^6+x^5+x^4+x^2+x+1$	511	63	x^9+x^8+1	73
5	$x^9+x^6+x^4+x^3+1$	511	75	$x^9+x^6+x^5+x^4+x^3+x^2+1$	511
7	x^9+x+1	73	77	$x^9+x^6+x^5+x^2+1$	73
9	$x^9+x^8+x^7+x^6+x^3+x^2+1$	511	79	$x^9+x^8+x^7+x^6+x^3+x+1$	511
11	$x^9+x^8+x^6+x^5+x^4+x^3+x^2+x+1$	511	83	$x^9+x^8+x^7+x^2+1$	511
13	$x^9+x^7+x^5+x^4+x^3+x^2+1$	511	85	$x^9+x^8+x^7+x^6+x^4+x^2+1$	511
15	$x^9+x^8+x^4+x+1$	511	87	$x^9+x^8+x^4+x^3+x^2+x+1$	511
17	$x^9+x^6+x^4+x^3+x^2+x+1$	511	91	$x^9+x^7+x^4+x^3+1$	73
19	$x^9+x^7+x^6+x^4+1$	511	93	$x^9+x^8+x^7+x^6+x^2+x+1$	511
21	$x^9+x^6+x^3+x+1$	73	95	$x^9+x^7+x^6+x^5+x^4+x^2+1$	511
23	$x^9+x^8+x^6+x^5+x^3+x+1$	511	103	$x^9+x^8+x^6+x^5+x^4+x+1$	511
25	$x^9+x^8+x^6+x^5+1$	511	107	$x^9+x^7+x^2+x+1$	511
27	$x^9+x^8+x^6+x^3+x^2+x+1$	511	109	$x^9+x^7+x^6+x^5+x^4+x^3+1$	511
29	$x^9+x^6+x^5+x^3+x^2+x+1$	511	111	$x^9+x^4+x^3+x+1$	511
31	$x^9+x^8+x^5+x+1$	511	117	x^9+x^5+1	511
35	$x^9+x^4+x^2+x+1$	73	119	$x^9+x^8+x^7+x^5+1$	73
37	$x^9+x^5+x^4+x+1$	511	123	$x^9+x^5+x^3+x^2+1$	511
39	$x^9+x^7+x^5+x^4+x^2+x+1$	511	125	$x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+1$	511
41	$x^9+x^7+x^5+x^2+1$	511	127	$x^9+x^8+x^7+x^5+x^4+x^3+1$	511
43	x^9+x^4+1	511	171	$x^9+x^7+x^5+x^3+x^2+x+1$	511
45	$x^9+x^8+x^7+x^3+x^2+x+1$	511	175	$x^9+x^8+x^6+x^3+1$	73
47	$x^9+x^8+x^7+x^6+x^4+x^3+1$	511	183	$x^9+x^7+x^4+x^2+1$	511
51	$x^9+x^8+x^5+x^4+x^3+x+1$	511	187	$x^9+x^8+x^5+x^4+1$	511
53	$x^9+x^8+x^7+x^6+x^5+x+1$	511	191	$x^9+x^6+x^5+x^3+1$	511
55	$x^9+x^7+x^6+x^4+x^3+x+1$	511	223	$x^9+x^7+x^6+x^3+x^2+x+1$	511
57	$x^9+x^8+x^6+x^5+x^3+x^2+1$	511	239	$x^9+x^8+x^7+x^6+x^5+x^3+1$	511
59	$x^9+x^8+x^7+x^5+x^4+x^2+1$	511	255	$x^9+x^8+x^4+x^2+1$	511

CHAPTER 4

APPLICATIONS TO BCH CODES

Cyclic codes are first studied by Prange [33] in 1957. Since then, the study of these codes is experiencing enormous progress. The class of cyclic codes contains the most efficient codes, such as Hamming codes, Reed-Solomon codes, etc. A special class among cyclic codes are Bose-Chaudhury-Hocquenghem (BCH) codes. These codes were discovered by R. Bose and D.K. Ray-Chaudhuri [9] in 1960, and independently by A. Hocquenghem [21] in 1959. They are of great practical importance for error correction, particularly if the expected number of errors is small compared with the length of the code (see, e.g., [22], [26]). This chapter, as a consequence of our previous results, is devoted to applications to such codes. First, we give a characterization of the generator polynomial of a BCH code. Then, we show how two BCH codes over $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$, respectively, and their generator polynomials are related.

Definition 4.1. Let q be a power of a prime. Let n be an integer such that $\gcd(n, q) = 1$ and set $m = \mathrm{ord}_n(q)$. Let $\alpha \in \mathbb{F}_{q^m}$ be an element of order n, and let δ be an integer such that $2 \leq \delta \leq n$. A narrow-sense BCH code over $\mathbb{F}_q$ of length n and designed distance δ is a cyclic code, with generator polynomial

$$g(x) = \mathrm{lcm}\left\{\mathrm{Min}(\alpha^i, \mathbb{F}_q)(x) : 1 \leq i \leq \delta - 1\right\}.$$

When $n = q^m - 1$, this code is called primitive BCH code and is denoted by $C_{(q,m,\delta)}$.

For practical purposes, we would like to construct a cyclic code with high minimum distance, since the higher the minimum distance, the more errors the code can detect and correct. For that, BCH codes have the following important property.

Theorem 4.1. [22, Theorem 5.1.1](BCH Bound) Let C be a BCH code with a designed distance δ. Then $d \geq \delta$, where d is the minimum distance of C.

This theorem along with Proposition 1.11 assure that the higher the designed distance of C, the more errors the code can detect and correct.

4.1 A Characterization Of The Generator Polynomial Of a BCH Code

As we have seen with the definition of a BCH code C, we need the generator polynomial $g(x)$ in order to describe the code, since the codewords of C are just multiples of $g(x)$ modulo

$x^n - 1$. Recall that for a divisor e of $q^{rm} - 1$ such that $rm = \mathrm{ord}_e(q)$, we defined

$$D_e = \left\{ \frac{se}{e'} (\mathrm{mod}\ e) : e' \textit{ divides } e; rm = \mathrm{ord}_{e'}(q); \gcd(s, e') = 1 \right\}.$$

When the class of an integer k modulo e is in D_e, we simply write $k \in D_e$. Note that D_e is not empty, since for $s = 1$ and $e = e'$ we have $1 \in D_e$.

In the following proposition, we give a characterization of the polynomial $g(x)$.

Proposition 4.1. [14, Proposition 5.1] Let $V(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{F}_{q^m}[x]$ be an irreducible polynomial of degree r with $\mathbb{F}_q(a_0, a_1, \ldots, a_r) = \mathbb{F}_{q^m}$. Let $\mathbf{C}_v$ be the companion matrix of $V(x)$. Let $\alpha \in \mathbb{F}_{q^{rm}}$ be a root of $V(x)$, $n = \mathrm{ord}(\alpha)$ and let δ be an integer with $2 \leq \delta \leq n$. Let C be a narrow-sense BCH code over $\mathbb{F}_q$ of length n and designed distance δ, with generator polynomial

$$g(x) = \mathrm{lcm}\left\{ \mathrm{Min}(\alpha^i, \mathbb{F}_q)(x) : 1 \leq i \leq \delta - 1 \right\}.$$

Set

$$B = \left\{ \det\left(x\mathbf{I}_{rm} - \Psi(\mathbf{C}_v^k) \right) : 1 \leq k \leq \delta - 1; k \in D_n \right\}.$$

Then, the polynomial

$$H(x) = \prod_{f(x) \in B} f(x)$$

divides $g(x)$ in $\mathbb{F}_q[x]$, and it is the product of all irreducible factors of $g(x)$ in $\mathbb{F}_q[x]$ of degree rm. Furthermore, $H(x) = g(x)$ if and only if $1, 2, \ldots, \delta - 1 \in D_n$.

Proof. Since D_n is not empty, then so is B. Using Corollary 3.2, we have that B is the set of all monic irreducible polynomials over $\mathbb{F}_q$ of degree rm of the form $\mathrm{Min}(\alpha^k, \mathbb{F}_q)(x)$ with $1 \leq k \leq \delta - 1$.
Now, $H(x) = g(x)$ if and only if $\mathrm{Min}(\alpha^i, \mathbb{F}_q)(x) \in B$ for all $1 \leq i \leq \delta - 1$, if and only if $1, 2, \ldots, \delta - 1 \in D_n$. □

Example 4.1. Consider the irreducible polynomial

$$V(x) = x^5 + (\theta + 1)x^3 + (\theta + 1)x^2 + x + 1 \in \mathbb{F}_{2^2}[x],$$

where $\theta \in \mathbb{F}_{2^2}$ is the primitive element verifying $\theta^2 + \theta + 1 = 0$. The companion matrix of $V(x)$ is

$$\mathbf{C}_v = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & \theta + 1 \\ 0 & 0 & 1 & 0 & \theta + 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let α be a root of $V(x)$. We have $n = \mathrm{ord}(\alpha) = 341$. Let C be the narrow-sense BCH code over $\mathbb{F}_2$ of length 341 and designed distance $\delta = 11$, with generator polynomial

$$g(x) = \mathrm{lcm}\left\{\mathrm{Min}(\alpha^i, \mathbb{F}_2)(x) : 1 \leq i \leq 10\right\}.$$

Then,

$$H(x) = x^{50} + x^{46} + x^{44} + x^{43} + x^{41} + x^{39} + x^{38} + x^{37} + x^{35} + x^{34} + x^{31} + x^{30} + x^{27} + x^{25} + x^{24} + x^{22} + x^{19} + x^{18} + x^{17} + x^{13} + x^8 + x + 1.$$

Moreover, we have $1, 2, \ldots, 10 \in D_{341}$. Hence $H(x) = g(x)$.

4.2 A Link Between Two BCH Codes And Their Generator Polynomials

A very useful method of constructing codes over $\mathbb{F}_q$ is to restrict codes which are defined over an extension field $\mathbb{F}_{q^m}$. This means that, given a code $C \subseteq \mathbb{F}_{q^m}^n$, one considers the subfield subcode $C|\mathbb{F}_q = C \cap \mathbb{F}_q^n$. Many well-known codes can be defined in this way, for instance BCH codes. In this section, we will see how two BCH codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively, are related.

We consider a primitive polynomial $V(x) \in \mathbb{F}_{q^m}[x]$ of degree r, and we set $f(x) = \prod_{i=0}^{m-1} \Phi(V)$. Let $\alpha, \beta \in \mathbb{F}_{q^{rm}}$ be a root of $V(x)$ and $f(x)$, respectively. Let δ be an integer such that $2 \leq \delta \leq q^{rm} - 1$. Denote by $C = C_{(q^m,r,\delta)}$ and $\widetilde{C} = C_{(q,rm,\delta)}$ the primitive BCH codes with generator polynomials

$$g(x) = \mathrm{lcm}\left\{\mathrm{Min}(\alpha^i, \mathbb{F}_{q^m})(x) : 1 \leq i \leq \delta - 1\right\},$$

and

$$\tilde{g}(x) = \mathrm{lcm}\left\{\mathrm{Min}(\beta^i, \mathbb{F}_q)(x) : 1 \leq i \leq \delta - 1\right\},$$

respectively.

Note that since α and β are roots of $f(x)$, there exists an integer $0 \leq k < rm$ such that $\beta = \alpha^{q^k}$. Therefore, we have $\mathrm{Min}(\beta^i, \mathbb{F}_q)(x) = \mathrm{Min}(\alpha^i, \mathbb{F}_q)(x)$ and

$$\tilde{g}(x) = \mathrm{lcm}\left\{\mathrm{Min}(\alpha^i, \mathbb{F}_q)(x) : 1 \leq i \leq \delta - 1\right\}.$$

Now, we will show how C and $\widetilde{C}$ are related. For this, we need the following two results.

Theorem 4.2. [38, Theorem 9.1.2] For a linear code C over $\mathbb{F}_{q^m}$ of length n, we have

$$\mathrm{Tr}_{q^m|q}(C^\perp) = (C|\mathbb{F}_q)^\perp,$$

where $C^\perp$ is the orthogonal code of C.

Lemma 4.1. [38, Lemma 9.1.3] Let C be a linear code over $\mathbb{F}_{q^m}$ of length n. Then

$$\dim(C) \leq \dim(\mathrm{Tr}_{q^m|q}(C)) \leq m \dim(C).$$

Proposition 4.2. [14, Proposition 5.2] With the notation above, we have:

(i) $\widetilde{C} = C|\mathbb{F}_q$,

(ii) $\mathrm{Tr}_{q^m|q}(C^\perp) = \widetilde{C}^\perp$,

(iii) $\dim(C^\perp) \leq \dim(\widetilde{C}^\perp) \leq m.\dim(C^\perp)$.

Proof. (i) The polynomial $\mathrm{Min}(\alpha^i, \mathbb{F}_{q^m})(x)$ divides $\mathrm{Min}(\alpha^i, \mathbb{F}_q)(x)$ in $\mathbb{F}_{q^m}[x]$. Therefore, $g(x)$ divides $\tilde{g}(x)$ in $\mathbb{F}_{q^m}[x]$ and $\widetilde{C} \subset C|\mathbb{F}_q$. Now, let $c(x) \in C|\mathbb{F}_q$. For any root λ of $\tilde{g}(x)$, there exist some integers i and j such that $1 \leq i \leq \delta - 1$, $0 \leq j < rm$ and $\lambda = (\alpha^i)^{q^j}$. Then, since $c(x) \in C$ we have

$$c(\lambda) = c\left((\alpha^i)^{q^j}\right) = c(\alpha^i)^{q^j} = 0.$$

Hence, $\tilde{g}(x)$ divides $c(x)$ in $\mathbb{F}_q[x]$ and $c(x) \in \widetilde{C}$.
(ii) By replacing $C|\mathbb{F}_q$ by $\tilde{C}$ in Theorem 4.2 and using Part (i), we get $\mathrm{Tr}_{q^m|q}(C^\perp) = \widetilde{C}^\perp$.
(iii) Here we replace C by $C^\perp$ in Lemma 4.1. Part (ii) then yields the result. □

The next proposition is useful to find the polynomial $\tilde{g}(x)$ if $g(x)$ is given.

Proposition 4.3. [14, Proposition 5.3] Let $m \geq 2$ and $c = \max\{d : d \text{ is a proper divisor of } m\}$. Set for all $s \in \{1, 2, \ldots, \delta - 1\}$, $V_s(x) = \mathrm{Min}(\alpha^s, \mathbb{F}_{q^m})(x)$ and $f_s(x) = \mathrm{Min}(\alpha^s, \mathbb{F}_q)(x)$. The following statements are satisfied:

(i) If $\delta \leq \frac{q^{rm}-1}{q^{rc}-1}$, then

$$f_s(x) = \prod_{i=0}^{m-1} \Phi^i(V_s)(x).$$

(ii) We have that $\delta \leq q$ if and only if

$$\tilde{g}(x) = \prod_{i=0}^{m-1} \Phi^i(g)(x).$$

(iii) We have also $\delta \leq q$ if and only if $\dim(\widetilde{C}) = m \dim(C) - n(m-1)$.

Proof. (i) If $\delta \leq \frac{q^{rm}-1}{q^{rc}-1}$, then for any proper divisor d of m, $V_s(x) \notin \mathbb{F}_{q^d}[x]$. Indeed, if there exists such d with $V_s(x) \in \mathbb{F}_{q^d}[x]$, then $q^{rm} - 1$ divides $(q^{d \deg(V_s(x))} - 1)s$, which implies

$$\frac{q^{rm} - 1}{q^{d \deg(V_s(x))} - 1} \leq s,$$

a contradiction, since

$$s < \delta \leq \frac{q^{rm}-1}{q^{rc}-1} \leq \frac{q^{rm}-1}{q^{d\deg(V_s(x))}-1}.$$

Then, Proposition 2.1 implies the result.
(ii) If $\delta \leq q$, then for all integers i and j with $1 \leq i < j \leq \delta - 1$, we have $V_i(x) \neq V_j(x)$ and $f_i(x) \neq f_j(x)$. Indeed, suppose, on the contrary, that there exist such integers i and j for which $V_i(x) = V_j(x)$ or $f_i(x) = f_j(x)$. Then, $\alpha^i = \alpha^{jq^{mk}}$ for some $k \in \{0, 1, \ldots, r-1\}$ or $\alpha^i = \alpha^{jq^l}$ for some $l \in \{0, 1, \ldots, rm-1\}$, which implies that $q^{rm}-1$ divides $jq^{km} - i$ or that $q^{rm}-1$ divides $jq^l - i$. Thus, $q^m \leq j$ or $q \leq j$, a contradiction. Therefore, we have

$$g(x) = \prod_{i=1}^{\delta-1} V_i(x)$$

and

$$\tilde{g}(x) = \prod_{i=1}^{\delta-1} f_i(x).$$

Since $\delta \leq q < \frac{q^{rm}-1}{q^{rc}-1}$, then, Part (i) implies that

$$\tilde{g}(x) = \prod_{i=1}^{\delta-1} f_i(x) = \prod_{i=1}^{\delta-1}\prod_{j=0}^{m-1} \Phi^j(V_i)(x) = \prod_{j=0}^{m-1} \Phi^j\left(\prod_{i=1}^{\delta-1} V_i\right)(x) = \prod_{j=0}^{m-1} \Phi^j(g)(x).$$

Conversely, suppose that $\tilde{g}(x) = \prod_{i=0}^{m-1} \Phi^i(g)(x)$ and $\delta > q$. Notice that $V_q(x) = \Phi(V_1)(x)$. Hence, $V_1(x) \neq V_q(x)$ and $V_1(x)V_q(x)$ divides $g(x)$ in $\mathbb{F}_{q^m}[x]$. Then, the polynomial

$$f_1(x)f_q(x) = f_1(x)^2$$

divides $\tilde{g}(x)$ in $\mathbb{F}_q[x]$, a contradiction, and Part (ii) holds.
(iii) Suppose that

$$g(x) = \prod_{i\in J} V_i(x) \quad \text{and} \quad \tilde{g}(x) = \prod_{i\in I} f_i(x)$$

for some $I, J \subset \{1, 2, \ldots, \delta - 1\}$. Then, for all $i = 1, 2, \ldots, \delta - 1$, there exists $j \in J$ such that $V_i(x) = V_j(x)$, which implies that $f_i(x) = f_j(x)$. Hence, $\tilde{g}(x)$ divides $\prod_{k\in J} f_k(x)$ in $\mathbb{F}_q[x]$. Since $f_k(x)$ divides $\prod_{i=0}^{m-1} \Phi^i(V_k)(x)$ in $\mathbb{F}_q[x]$, then $\tilde{g}(x)$ divides $\prod_{i=0}^{m-1} \Phi^i(g)(x)$ in $\mathbb{F}_q[x]$. Thus, there exists a monic polynomial $h(x) \in \mathbb{F}_q[x]$ such that

$$h(x) \cdot \tilde{g}(x) = \prod_{i=0}^{m-1} \Phi^i(g)(x).$$

Part (ii) implies that $\delta \leq q$ if and only if $\deg(h(x)) = 0$ if and only if $\deg(\tilde{g}(x)) = m\deg(g(x))$, or equivalently $\dim(\widetilde{C}) = m\dim(C) - n(m-1)$. □

Example 4.2. Set $(q, m, r) = (11, 2, 2)$ and $\delta = 8$. Let $\mathbb{F}_{11^2} = \mathbb{F}_{11}(\theta)$, where $\theta^2 + 7\theta + 2 = 0$. Let $\alpha \in \mathbb{F}_{11^4}$ a primitive element verifying $\alpha^4 + 8\alpha^2 + 10\alpha + 2 = 0$. Then, we have the following

table, where $f_s(x) = \mathrm{Min}(\alpha^s, \mathbb{F}_{11})(x)$ and $V_s(x) = \mathrm{Min}(\alpha^s, \mathbb{F}_{11^2})(x)$:

s	$f_s(x)$	$V_s(x)$
1	$x^4 + 8x^2 + 10x + 2$	$x^2 + (3\theta + 5)x + \theta$
2	$x^4 + 5x^3 + 2x^2 + 9x + 4$	$x^2 + (2\theta + 4)x + 4\theta + 9$
3	$x^4 + 8x^3 + 5x^2 + 3x + 8$	$x^2 + (3\theta + 9)x + 3\theta + 3$
4	$x^4 + x^3 + 10x^2 + x + 5$	$x^2 + (9\theta + 10)x + 4\theta + 5$
5	$x^4 + 7x^3 + 5x + 10$	$x^2 + (5\theta + 10)x + 10\theta + 3$
6	$x^4 + x^3 + 4x^2 + 5x + 9$	$x^2 + (4\theta + 9)x + 10\theta + 2$
7	$x^4 + 6x^3 + 6x^2 + 7$	$x^2 + 7\theta x + 9\theta + 2$

Since $c = 1$ and $\delta \leq \dfrac{11^4 - 1}{11^2 - 1}$, then for all $s \in \{1, 2, \ldots, 7\}$, $f_s(x) = V_s(x) \cdot \Phi(V_s)(x)$. We have also:

$$g(x) = x^{14} + 3x^{13} + (\theta + 9)x^{12} + (4\theta + 8)x^{11} + (10\theta + 6)x^{10} + (7\theta + 6)x^8 + (4\theta + 2)x^7 + (7\theta + 10)x^6 + (10\theta + 3)x^5 + (7\theta + 7)x^4 + (4\theta + 2)x^3 + (5\theta + 5)x^2 + 4\theta x + 5\theta + 9,$$

$$\Phi(g)(x) = x^{14} + 3x^{13} + (10\theta + 2)x^{12} + (7\theta + 2)x^{11} + (\theta + 2)x^{10} + (4\theta + 1)x^8 + (7\theta + 7)x^7 + (4\theta + 5)x^6 + (\theta + 10)x^5 + (4\theta + 2)x^4 + (7\theta + 7)x^3 + (6\theta + 3)x^2 + (7\theta + 5)x + 6\theta + 7,$$

$$\tilde{g}(x) = x^{28} + 6x^{27} + 9x^{26} + 10x^{25} + 3x^{24} + 8x^{23} + 4x^{22} + 9x^{21} + 6x^{20} + 9x^{19} + 2x^{18} + 5x^{16} + 7x^{15} + 8x^{14} + 7x^{13} + 7x^{12} + 4x^{11} + 6x^{10} + 8x^9 + 3x^8 + 6x^7 + 9x^6 + 7x^5 + 5x^4 + 9x^3 + 7x^2 + 4x + 3.$$

Since $\delta \leq 11$, then $\tilde{g}(x) = g(x) \cdot \Phi(g)(x)$. Finally, the two codes C and $\tilde{C}$ generated by $g(x)$ and $\tilde{g}(x)$, respectively, have dimensions $\dim \widetilde{C} = 14640 - 28 = 14612$ and $\dim C = 14640 - 14 = 14626$, which satisfy $2\dim(C) - \dim(\widetilde{C}) = 14640$.

CONCLUSION

In this work, we have seen some interesting constructions of irreducible polynomials. We have presented the construction through the Frobenius automorphism. We have also present ed a construction using the companion matrix of an irreducible polynomial. We have shown how to obtain multiple and even all irreducible polynomials over $\mathbb{F}_q$ of degree rm. As an application, a characterization of the generator polynomial of a BCH code over $\mathbb{F}_q$ has been given. Then, we have seen how two BCH codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively, and their generator polynomials are related.

We plan to continue our investigation of BCH codes, that is, how to determine the parameters (dimension, minimum distance and Bose distance) of certain classes of BCH codes using the results in Chapter 4?

As we have mentioned before, Cohen's Theorem has been used by many authors to construct irreducible polynomials of increasing degree from known ones. Therefore, we would like to investigate the possibility of doing the same thing using our generalization of Cohen's Theorem.

Another question arises, if both constructions, given by Proposition 2.1 and Theorem 3.2, are the same, which is more efficient in computational terms? In other words, what is the time complexity of each construction?

We are also interested in applications to linear recurring sequences over finite fields. A work in this direction is in progress.

BIBLIOGRAPHY

[1] S.E. Abrahamyan, M. Alizadeh, M.K. Kyureghyan, Recursive constructions of irreducible polynomials over finite fields, Finite Fields Appl. 18 (2012) 738–745. doi : 10.1016/j.ffa.2012.03.003.

[2] S. Agou, Factorisation sur un corps fini $\mathbb{F}_{p^n}$ des polynomes composés $f(X^s)$ lorsque $f(X)$ est un polynome irréductibile de $\mathbb{F}_{p^n}[X]$, L'Enseignement Math., IIe Ser. 22 (1976) 305–312.

[3] S. Agou, Critères d'irréductibilité des polynômes composés à coefficients dans un corps fini, Acta Arithmetica 30 (1976) 213–223.

[4] S. Agou, Irréductibilité des polynomes $f(X^{p^r} - aX)$ sur un corps fini $\mathbb{F}_{p^s}$, J. Reine Angew. Math. 292 (1977) 191–195.

[5] S. Agou, Irréductibilité des polynomes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$, J. Number Theory 10 (1978) 64–69.

[6] S. Agou, Irréductibilité des polynomes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$, J. Number Theory 11 (1979) 20.

[7] M. Alizadeh, On the irreducibility of some composite polynomials, J. Math. Ext. 6 (2012) 65–73.

[8] I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian, Applications of finite fields, Springer US, 1993.

[9] R.C. Bose, and D.K. Ray-Chaudhuri, On a class of error correcting binary group codes, Inf. Control. 3 (1960) 68–79. doi : 10.1109/TIT.1965.1053825.

[10] R.P. Brent, P. Zimmermann, The great trinomial hunt. Notices of the AMS 58 (2010).

[11] M.C.R. Butler, The irreducible factors of $f(x^m)$ over a finite field, J. London Math. Soc., 2nd Ser. 30 (1955) 480–482.

[12] S.D. Cardell, J.J. Climent, V. Requena, A construction of MDS array codes, WIT Trans Inf Commun Technol. 45 (2013) 47–58. doi : 10.2495/DATA130051.

[13] S.D. Cardell, J.J. Climent, A construction of primitive polynomials over finite fields, Linear and Multilinear Algebra 65 (2017) 2424–2431. doi : 10.1080/03081087.2016.1275507.

[14] A. Cherchem, S. Bouguebrine, H. Boughambouz, On the construction of irreducible and primitive polynomials from $\mathbb{F}_{q^m}[x]$ to $\mathbb{F}_q[x]$, Finite Fields Appl. 78 (2022) 101971. doi: 10.1016/j.ffa.2021.101971.

[15] S.D. Cohen, On irreducible polynomials of certain types in finite fields, Proc. Cambridge Philos. Soc. 66 (1969) 335–344. doi : 10.1017/S0305004100045023.

[16] S.D. Cohen, The irreducibility of compositions of linear polynomials over a finite field, Compos. Math. 47 (1982) 149–152.

[17] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, Recurrence Sequences, AMS Surveys and Monographs, Vol. 104 (AMS, 2003).

[18] S.R. Ghorpade, S.U. Hasan, M. Kumari, Primitive Polynomials, Singer Cycles, and Word-oriented Linear Feedback Shift Registers, Des. Codes Cryptogr. 58 (2011) 123–134. doi : 10.1007/s10623-010-9387-7.

[19] S.W. Golomb, Shift Register Sequences, Aegean Park Press, Laguna Hills, California, 1982.

[20] J.W.P. Hirschfeld, G. Korchmaros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.

[21] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres 2 (1959) 147–156.

[22] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge Univ. Press, Cambridge, U.K., 2003.

[23] M.K. Kyuregyan, G.M. Kyureghyan, Irreducible compositions of polynomials over finite fields, Des. Codes. Cryptogr. 61 (2011) 301–314. doi : 10.1007/s10623-010-9478-5.

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

[25] A. F. Long, Jr., Factorization of irreducible polynomials over a finite field with the substitution $x^{p^r} - x$ for x, Duke Math. J 40 (1973) 63–76.

[26] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, 10th Impression, North-Holland, Amsterdam, 1998.

[27] S. Mehrabi, M.K. Kyuregyan, Irreducible compositions of polynomials over finite fields of even characteristic, Appl. Algebra Eng. Commun. Comput. 23 (2012) 207–220. doi : 10.1007/s00200-012-0175-7.

[28] G.L. Mullen, D. Panario, Handbook of Finite Fields, Taylor & Francis, Boca Raton, 2013.

[29] R.C. Mullin, J.L. Yucas, G.L. Mullen, A generalized counting and factoring method for polynomials over finite fields, J. Comb. Math. Comb. Comput. 72 (2010) 121–143.

[30] O. Ore, Contributions to the theory of finite fields, Trans. Amer. Math. Soc. 36 (1934) 243–274.

[31] A. Pellet, Sur les fonctions irréducibles suivant un module premier, C.R. Acad. Sci. Paris 93 (1881) 1065–1066.

[32] E. Petterson, Uber die Irreduzibilitat ganzzahliger Polynome nach einem Primzahlmodul, J. Reine Angew. Math. 175 (1936) 209–220.

[33] E. Prange, Cyclic error-correcting codes in two symbols, Air force Cambridge research center, 1957.

[34] J. A. Serret, Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modularie irréductible, Mém. Acad. Sci., Inst. de France 1 (1866) 617–688.

[35] J.A. Serret, Cours d'Algèbre Supérieure. Tome I, Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Editions Jacques Gabay, Sceaux, 1992, Reprint of the fourth (1877) edition.

[36] C.E. Shannon, A mathematical theory of communication, Bell System Tech. J. 27 (1948) 379–423.

[37] I.E. Shparlinski, Finite Fields: Theory and Computation: The meeting point of number theory, computer science, coding theory and cryptography. Kluwer, 1999.

[38] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd edition, Graduate Texts in Mathematics, vol. 254, Springer, Berlin, 2009.