FREE STORAGE BASIS CONVERSION OVER EXTENSION FIELD

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

NDANGANG YAMPA HAROLD

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

DECEMBER, 2014

Approval of the thesis:

FREE STORAGE BASIS CONVERSION OVER EXTENSION FIELD

submitted by **NDANGANG YAMPA HAROLD** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. BÜLENT KARASÖZEN
Director, Graduate School of **Applied Mathematics** _____

Prof. Dr. FERRUH ÖZBUDAK
Head of Department, **Cryptography** _____

Prof. Dr. ERSAN AKYILDIZ
Supervisor, **Cryptography, METU** _____

Examining Committee Members:

Prof. Dr. ERSAN AKYILDIZ
Cryptography Program, METU _____

Prof. Dr. FERRUH ÖZBUDAK
Cryptography Program, METU _____

Assoc. Prof. Dr. ZÜLFÜKAR SAYGI
Mathematics Department, TOBB ETU _____

Assoc. Prof. Dr. ÖMER KÜÇÜKSAKALLI
Mathematics Department, METU _____

Assist. Prof. Dr. MURAT CENK
Cryptography Program, METU _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: NDANGANG YAMPA HAROLD

Signature :

ABSTRACT

FREE STORAGE BASIS CONVERSION OVER EXTENSION FIELD

HAROLD, NDANGANG YAMPA
M.S., Department of Cryptography
Supervisor : Prof. Dr. ERSAN AKYILDIZ

December, 2014, 48 pages

The representation of elements over finite fields play a great impact on the performance of finite field arithmetic. So if efficient representation of finite field elements exists and conversion between these representations is known, then it becomes easy to perform computation in a more efficient way. In this thesis, we shall provide a free storage basis conversion in the extension field $\mathbb{F}_{q^p}$ of $\mathbb{F}_q$ between Normal basis and Polynomial basis and vice versa. The particularity of this thesis is that, our transition matrix is of a special form and requires no memory to store its entries. Also the inverse of the transition matrix is obtained just by permuting the row entries of the transition matrix. Therefore the complexity of the algorithm for obtaining both the transition matrix and its inverse is the same.

Keywords : Finite fields, normal basis, polynomial basis

ÖZ

CİSİM GENİŞLEMESİ ÜZERİNDE SERBEST DEPOLAMA BAZ DÖNÜŞÜMÜ

HAROLD, NDANGANG YAMPA
Yüksek Lisans, Kriptografi Programı
Tez Yöneticisi : Prof. Dr. ERSAN AKYILDIZ

December, 2014, 48 sayfa

Sonlu cisim elamanların gösterimlermin sonlu cisim aritmetiğinin performansı üzerinde çok önemli bir etkisi vardır. Eğer sonlu cisim elamanlarının iyi bir gösterimi varsa ve gösterimler arası dönüşümler biliniyorsa, cisim üzerindeki aritmetik hesaplamalar daha hızlı ve verimli yapılabilir. Bu tezde,$\mathbb{F}_q$ uzerindeki $\mathbb{F}_{q^p}$ cisim genişlemesi üzerinde, Normal baz ve Polinom baz arasında iki taraflı serbest depolama baz dönüşümü çalışılmıştır. Bu dönüşümün özelliği, geçiş matrisinin özel bir formda olması ve girdilerinin depolanması için hafızaya ihtiyaç duyulmamasıdır. Ayrıca geçiş matrisinin tersi tam olarak satırlarının permütasyonu alınarak elde edilir. Bu sebeple geçiş matrisini elde etme de kullanılan algoritmanın karmaşıklığı ile bu matrisin tersini elde etmede kullanılan algoritmanın karmaşıklığı aynıdır.

Anahtar Kelimeler : Sonlu Cisimler, Normal Baz, Polinom Bazı

To My Family

ACKNOWLEDGMENTS

I am grateful to "Yurtdışı Türkler ve Akraba Topluluklar Başkanlığı" for the scholarship I was offered. I also express my sincere gratitude to my thesis supervisor Prof. Dr. ERSAN AKYILDIZ for introducing me to this topic. Despite the fact that he is busy, he always assisted me and gave me his advices, guidances and even encouragement.

I also thank AHMET SINAK, for his guidances, help and encouragement and helping me to correct my typing errors.
In addition, I also thank Dr. MURAT CENK, for his advices especially when I encountered difficulties. Last but not the least, I thank all my professors and friends in the Institute of Applied Mathematics during this Program who have always shown me their love and sometimes I felt as if I was in my home town.

Finally, I owe thanks to my family in Cameroon, despite the distance, they have continuously supported me throughout my education.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

$\mathbb{F}_q$	Finite fields of q elements.
$Aut_{F_q}(\mathbb{F}_{q^n})$	Group automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$
$\mathrm{Tr}_{F/K}(\alpha)$	The trace of an element α with respect to the extension F/K

CHAPTER 1

INTRODUCTION

1.1 Introduction

Let $\mathbb{F}_{q^n}$ be an extension of finite field $\mathbb{F}_q$ of degree n. Then for any ordered basis $\beta = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, one has a unique representation of each element $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ in the form $\alpha = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ where $\alpha = \sum_{i=1}^{n} c_i\alpha_i \in \mathbb{F}_{q^n}$. Let ρ be another element of $\mathbb{F}_{q^n}$ with $\rho = \sum_{i=1}^{n} d_i\alpha_i$. Then $\rho = (d_1, \ldots, d_n)$ where $d_i \in \mathbb{F}_q$ for $i \in \{1, 2, \ldots, n\}$. This representation being an F_q- linear isomorphism gives us the sum $\alpha + \rho \in \mathbb{F}_{q^n}$ in terms of the n components of α and ρ and the scalar multiplication $c \cdot \alpha \in \mathbb{F}_{q^n}$ with $c \in \mathbb{F}_q$ in terms of components of α. So in the implementation point of view, sum and scalar multiplication of elements in $\mathbb{F}_{q^n}/\mathbb{F}_q$ have the same complexity for any choice of an ordered basis. But when it comes to multiplication $\alpha\rho$ and the inverse $\alpha^{-1} \in \mathbb{F}_{q^n}$, one wonders how to choose the ordered basis $\beta = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $\mathbb{F}_{q^n}/\mathbb{F}_q$ so that multiplication $\alpha\rho = (c_1, \ldots, c_n)(d_1, \ldots, d_n)$ and inverse $\alpha^{-1} = (t_1, \ldots, t_n)$ of α can be computed efficiently. For this purpose, there has been some studies in the literature and these studies brought the concept of normal bases, optimal normal bases. So far no body knows how to choose an ordered basis β in $\mathbb{F}_{q^n}/\mathbb{F}_q$ so that multiplication $\alpha\rho$ and the inverse α^{-1} is more efficient than any other choice. In any case, there is an obvious natural ordered basis $\beta = \{\alpha_1, \ldots, \alpha_n\} = \{1, x, \ldots, x^{n-1}\}$ of $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/_{(p(x))}$ where $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is the irreducible polynomial representation (field polynomial) of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, called the polynomial basis. In this representation, the multiplication of $\alpha\rho \in \mathbb{F}_{q^n}$ is performed in two steps: polynomial multiplication over $\mathbb{F}_q$ and modular reduction by $p(x)$. As the complexity of the field multiplication depends on the number of non-zero terms in the reduction polynomial, it is desirable to use reduction polynomial with fewer number of terms. And the inverse α^{-1} of $\alpha = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ can be obtained by using the extended euclidean algorithm. The problem in the implementation of arithmetic operation of $\mathbb{F}_{q^n}$ is to find a good ordered basis β such that the algorithms for performing $\alpha\rho$ and α^{-1} are efficient. So far one still doesn't know a generic choice for this problem. In literature, in order to improve the efficiency of arithmetic operations over finite fields, one usually perform the conversion between polynomial basis representation to another representation of field element and vice versa. This is what we are going to do in this thesis for the field $\mathbb{F}_{q^p}$ where $q = p^n$ and p an odd prime.

1.2 Motivation and Outline of the Thesis

Given two bases $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_m\}$, the traditional method for converting from one basis to another is to form an $m \times m$ transition matrix T such that $A = T * B$ and $B = T^{-1} * A$. This method requires $O(m^2)$ field operations and also required $O(m^2)$ storage requirement for coefficients. Burton and Kaliski in [2] proposed an efficient finite field basis conversion in $\mathbb{F}_{q^m}$ using an import and export algorithm which requires $O(m \log q)$ field operations and require storage for $O(m)$ coefficients.

Our Motivation started in [16] in which the author provided a basis conversion over $\mathbb{F}_{p^p}$. In this thesis, we constructed the finite field $\mathbb{F}_{q^p}$ by using the irreducible polynomial $f(x) = x^p - x + 1 \in \mathbb{F}_p[x]$ over $\mathbb{F}_q$ where $q = p^n, \gcd(p, n) = 1$ and p is an odd prime. Clearly $\mathbb{F}_{q^p} \cong \mathbb{F}_q[x]/_{(f(x))}$ has the polynomial basis $\{1, \alpha, \ldots, \alpha^{p-1}\}$. We realised that the construction of the extension field $\mathbb{F}_{q^p}$ with the irreducible polynomial f over $\mathbb{F}_q$ does not have a normal basis. In order to construct the normal basis of $\mathbb{F}_{q^p}$, we have seen that the reciprocal $g(x) = x^p - x^{p-1} + 1 \in \mathbb{F}_p[x]$ of f which is also irreducible over $\mathbb{F}_q$ is normal polynomial in $\mathbb{F}_{q^p}$. Therefore, we constructed the normal basis $\{\beta, \beta^q, \ldots, \beta^{p-1}\}$ of $\mathbb{F}_q(\beta) \cong \mathbb{F}_q[x]/_{(g(x))}$. We wrote each of the β^{q^i} as a linear combination of the α^i for $i \in \{0, 1, \ldots, p-1\}$ and we form the transition matrix M of polynomial basis to normal basis. This matrix is of special form and also the inverse of this matrix is obtained just by permutation of the row entries of M. Therefore the complexity of finding M and its inverse M^{-1} are equal. The time complexity of our method is $O(np^3)$ and no extra memory requirement is needed apart from the memory of the input. The rest of this thesis is organized as follows:

- The second chapter of this thesis deals with basic definition in finite fields, construction of extension fields, nature of roots of irreducible polynomials over extensions and we provide an algorithm to factorise square free polynomial into irreducible polynomials.
- In next chapter the aim is to develop condition under which extensions fields have normal basis and then apply those conditions on irreducible polynomials to check whether they are normal or not.
- In the fourth chapter, we analysed the roots of trinomial $f(x) = x^p - x + 1 \in \mathbb{F}_p[x]$ and whether the roots of its reciprocal polynomial $g(x) = x^p - x^{p-1} + 1 \in \mathbb{F}_p[x]$ form a normal basis or not, we use those roots to construct the transition matrix from polynomial basis to normal basis and vice versa. Furthermore, we construct Algorithm 1 and 2 with their complexities. Finally we shall provide our future interest of research on this topic.

CHAPTER 2

Preliminary

In this chapter, we give the fundamental definitions and structures related to our work. For further explanations, applications and previous work, see [1, 9, 5, 3] and references there in.
Finite fields is a branch of mathematics discovered by Evariste Galois [9] and it serves as the building blocks for cryptography and coding theory. In this section we shall give a brief summary about finite fields, irreducible polynomials and construction of extension fields.

Definition 2.1. [9]. A ring R is a set with two binary operations denoted + and $\cdot$ called addition and multiplication satisfying

1. R is an abelian group under $+$
2. $\cdot$ is associative. That is for any $a, b, c \in R$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. $\cdot$ is distributive with respect to $+$ i.e for $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

If R has an identity element with respect to multiplication, we denote it as 1_R and the identity element of R with respect to addition is denoted as 0_R.

R is said to be commutative if the operation $\cdot$ of R is commutative, i.e for any $x, y \in R$ $x \cdot y = y \cdot x$

Example 2.1. The set of integers form a commutative ring.

Definition 2.2. [9] A field F is a commutative ring with $1_R \neq 0$ such that every non-zero elements of R has multiplicative inverse.

A subset K of F is called a subfield of F, if K forms a field under the same operations as in F.

Example 2.2. The set of rational numbers $\mathbb{Q}$ is a field.

Let p be a prime, the residue class ring $\mathbb{Z}/_{p\mathbb{Z}}$ is a field having the representation set $\{0, 1, \ldots, p-1\}$ and this is denoted as $\mathbb{F}_p$.

Remark 2.1. A field with finite number of elements is called a Galois field (GF). The number of elements (order) of a finite field is always a prime or a power of a prime.

Notation: The Galois field $GF(p)$ is denoted as $\mathbb{F}_p$.

Example 2.3. The field GF$(3) = \{0, 1, 2\}$ is a finite field in which addition and multiplication of two elements in GF(3) is taken modulo 3 and the elements in $\{1, 2\}$ have multiplicative inverses $\{1, 2\}$ respectively.

Definition 2.3. [9] The characteristics of a field F is the smallest positive integer $n \in \mathbb{N}$ such that $nr = 0$ for all $r \in$ F.

Example 2.4. The characteristics of the field $\mathbb{F}_3$ is three .

Remark 2.2. The characteristics of any finite field is always a prime number.

Theorem 2.1. *[9](Freshmann Dream) Let R be a commutative ring with prime characteristic p. Then $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ and $(a-b)^{p^n} = a^{p^n} - b^{p^n}$ for $a, b \in R$ and $n \in \mathbb{N}$.*

In the next section, we will briefly describe irreducible polynomials over finite fields.

2.1 Irreducible Polynomials over a Finite Field

Irreducible polynomials are important for constructions of Extension fields which are usually used for implementation cryptographic algorithms. In this section we will give basic properties concerning irreducible polynomials and after completing structure of finite fields, we will be ready to give a formula for the number of irreducible polynomials over finite fields and later at the end of this chapter, we will show that for any prime p and any integer n, there always exists an irreducible polynomial of degree n over the finite field $\mathbb{F}_p$. Let $\mathbb{F}_p[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \mid a_i \in \mathbb{F}_p, 0 \leq i \leq n\}$ be the ring of polynomials of degree less than or equal to n.

Definition 2.4. [9] A polynomial $f \in \mathbb{F}_p[x]$ is said to be irreducible in $\mathbb{F}_p[x]$ if

1. deg $f \geq 1$
2. if $f = hg$ for some $h, g \in \mathbb{F}_p[x]$ then either g or h are constant polynomials.

We note that the condition for a polynomial to be irreducible depends on the field.

Example 2.5. The polynomial $x^2 - 2$ is reducible over $\mathbb{R}$ since $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \notin \mathbb{Q}$.

Example 2.6. The polynomial $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$ but reducible over $\mathbb{F}_3$ since 1 is the root of $x^2 + x + 1$ which belongs in $\mathbb{F}_3$.

Let $\mathrm{F}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \mid a_i \in \mathrm{F}, 0 \leq i \leq n\}$ be a ring of polynomials over F. Let $< f(x) >$ be an ideal generated by $f \in \mathrm{F}[x]$. Let $L = \mathrm{F}[x]/(f) = \{r+(f) \mid r \in \mathrm{F}[x], \deg r < \deg f\}$. The following theorem will help us to construct Extension field, and the proof is given in [9].

Theorem 2.2. *[9] Let F be a field and with $1 \leq deg f \leq n$ then $F[x]/(f)$ is a field if and only if f is irreducible over F.*

2.2 Field Extensions

Definition 2.5. [9] Let K be a subfield of F then F is called an extension of K and we denote it as F/K.

Example 2.7. The field of complex number $\mathbb{C}$ is an extension field of real number $\mathbb{R}$.

Remark 2.3. The Galois field $\mathbb{F}_p = GF(p)$ contains no proper subfield so it cannot be an extension of any field.

Let K be a subfield of F and S be subset of F, the smallest field containing K and S is called the extension of K by adjoining the elements of S. We denote it as $\mathrm{K}(S)$. Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ for $\alpha_i \in F$. Then we write $\mathrm{K}(S) = \mathrm{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. If $S = \{\alpha\}$, we say that $\mathrm{K}(\alpha)$ is the simple extension of K and α is called the defining element of F/K.

Definition 2.6. [9] Let K be a subfield of F. An element $\alpha \in$ F is said to be algebraic over K if $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some $a_{n-1}, \ldots, a_0 \in$ K.

Example 2.8. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a field extension and $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since $\sqrt{2}$ is the root of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$.

The following propositions will be helpful for the construction of finite fields of prime power and its proofs can be found in [9].

Proposition 2.3. *[9] Let F/K be a field extension and α be algebraic over K, then there exist a unique irreducible monic polynomial $g \in K[x]$ such that $g(\alpha) = 0$. The polynomial g is denoted as $g = Irr(\alpha, K)$. This polynomial is called the minimal polynomial of α.*

Proposition 2.4. *[9] Let K be a field and let $f \in K[x]$ be a monic irreducible polynomial over K, then there exists a simple algebraic extension $K(\alpha)$ where α is the root of f. In other words, K has a simple algebraic extension in which f has a root.*

Proposition 2.5. *[9] Let F/K be extension of K and $\alpha \in F$ be algebraic over K with $g = Irr(\alpha, K)$ and n=deg g. Then*

- *$K(\alpha) \cong K[x]/(g)$ and $K(\alpha) = K[\alpha] = \{f(\alpha) \mid f \in K[x]\}$.*
- *$[K(\alpha) : K] = n$ and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of $K(\alpha)$ over K.*

- *Every $\beta \in K(\alpha)$ is algebraic over K, namely $K(\alpha)$ is an algebraic extension of K.*

Example 2.9. $\mathbb{F}_3[x]$ is a ring of polynomials whose coefficients belong in $\mathbb{F}_3$. Let α be a root of an irreducible polynomial of degree 2. We determine the simple extension field $\mathbb{F}_3(\alpha)$ as follows:
We chose the polynomial $f(x) = x^2 + 1$ which is irreducible over $\mathbb{F}_3$. By Theorem 2.5, $\mathbb{F}_3[x]/(f)$ is a field. By proposition 2.4, there exists a simple extension $\mathbb{F}_3(\alpha)$ such that α is the root of the polynomial i.e $f(\alpha) = 0$. By Proposition 2.5, L= $\mathbb{F}_3[x]/(f)$ is isomorphic to $\mathbb{F}_3(\alpha)$ and $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 2$ also $\{1, \alpha\}$ is a basis of L. So L =$\{a + b\alpha \mid a, b \in \mathbb{F}_3\} = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$.

2.3 Structure of Finite Fields

In this section, we shall describe the construction of finite fields of order p^n and also show that for every prime p, there exists an irreducible polynomial f of degree n such that $f(x) \in \mathbb{F}_p[x]$. Let p be the characteristic of the field $\mathbb{F}_q$ where q is a power of p. Consider the polynomial $x^q - x \in \mathbb{F}_p[x]$, then the roots of this polynomial are all distinct, the smallest field containing all the roots of the above polynomial is called the splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p[x]$. In fact this splitting field is isomorphic to any field of q elements. Now we state the following theorem and the proof can be obtained in [9].

Theorem 2.6. *[9] For any prime p and for any integer n, there is a finite field with p^n elements denoted $\mathbb{F}_{p^n}$. This field is isomorphic to the splitting field of the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$.*

In order to construct a field of order p^n, it suffices to choose an irreducible polynomial f of degree n over $\mathbb{F}_p$ and construct the field L = $\mathbb{F}_p[x]/(f) = \mathbb{F}(\alpha)$ where α is the root of f in $\mathbb{F}_p[x]/(f)$. We shall prove later that for any p and n, there exists an irreducible polynomial of degree n over $\mathbb{F}_p$.

Example 2.10. Let n=2 and p=2, we construct a finite field $\mathbb{F}_{2^2}$ as follow:
The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$. Let α be the root of the polynomial in the extension. Then L = $\mathbb{F}_2[x]/(f)$ =$\mathbb{F}_2(\alpha)$ and $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2$ also $\{1, \alpha\}$ is a basis of $\mathbb{F}_2(\alpha)$. So L=$\{a + b\alpha \mid a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, \alpha + 1\}$.

Proposition 2.7. *[9] The splitting field of any two irreducible polynomials of the same degree over the same prime field are isomorphic.*

Next we present a theorem for the characterization of subfields of the finite field $\mathbb{F}_q$, where $q = p^n$ for any positive integer n and prime p.

Theorem 2.8. *[9](Subfield Criterion) Let $q = p^n$. Let $\mathbb{F}_q$ be a field of q elements. Then any Subfield of $\mathbb{F}_q$ has order p^r where r is positive divisor of n. Conversely for any positive divisor r of n, there exists one subfield of $\mathbb{F}_q$ with p^r elements.*

Proof. By Theorem 2.6, we are sure for any prime number p and any positive integer r there exists a finite field of order p^r. Suppose K is a subfield of $\mathbb{F}_q$ and the order of K is p^r. We need to show that $r|n$. Since the order of K is p^r, K is regarded as a vector space over the prime field $\mathbb{F}_p$. So the dimension of the vector space K denoted **dim**K = $[\mathrm{K} : \mathbb{F}_p]$ =r. Also $\mathbb{F}_q$ is regarded as a vector space over K and let t be the degree of the extension of $\mathbb{F}_q$. That is t =$[\mathbb{F}_q : K]$. Then we have $n = [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : K][K : \mathbb{F}_p]$. Then we have $n = rt$.
Conversely suppose $r|n$, we need to show that $\mathbb{F}_{p^r}$ is subfield of $\mathbb{F}_{p^n}$. In other words we need to show that $x^{p^r} - x \mid x^{p^n} - x$. To do this, we first note that $p^r - 1 \mid p^n - 1$. This is due to the fact $r|n$.
Now we show that $x^{p^r-1} - 1 \mid x^{p^n-1} - 1$. The proof follow immediately from the statement above. So any root of the polynomial $x^{p^r} - x$ is also a root of the polynomial $x^{p^n} - x$. Hence $\mathbb{F}_q$ contains the splitting field of the polynomial $x^{p^r} - x \in \mathbb{F}_p[x]$. Now we show the uniqueness of the existence of the subfield K. Suppose $\mathbb{F}_q$ has another subfield $\bar{K}$ with p^r elements and K $\neq \bar{K}$. Then $|K \cup \bar{K}| > p^r$. But each element in $K \cup \bar{K}$ is a root of $x^{p^r} - x$. So we get a contradiction. □

Example 2.11. Let $\mathbb{F}_{p^{25}}$ be an extension field of $\mathbb{F}_{p^5}$. Then the subfields of $\mathbb{F}_{p^{25}}$ are in bijection to the positive divisor of 25. So positive divisors of 25 are $\{1, 5, 25\}$ and the subfields of $\mathbb{F}_{p^{25}}$ are respectively $\mathbb{F}_p$, $\mathbb{F}_{p^5}$, $\mathbb{F}_{p^{25}}$.

The aim in the following part is to show that for any prime p and any natural number n there exist an irreducible polynomial in $\mathbb{F}_p$ of degree n. We first need some foundations.

Theorem 2.9. *[5] Let F be a field and G be a finite subgroup of the multiplicative group F^*. Then G is a cyclic group.*

The proof of this theorem is given [5].

Corollary 2.10. *[5] Let $q = p^n$ and $\mathbb{F}_q$ be a field. Then $\mathbb{F}_q^*$ is cyclic.*

The proof is immediate from the Theorem 2.9 above since $\mathbb{F}_q^*$ is a multiplicative subgroup of itself.

Definition 2.7. [9] Any generator $g \in \mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q^*$.

Therefore $\mathbb{F}_q^*$ = $< g >$ =$\{g, g^2, \ldots, g^{q-1} = 1\}$. The number of primitive elements of $\mathbb{F}_q^*$ is $\phi(q-1)$ where $\phi(q-1)$ =$|$ $\{k \in \mathbb{N} \mid k < q-1$ and $\gcd(k, q-1) = 1\}$ $|$

Example 2.12. In Example 2.10, the finite field with 4 elements was L=$\{0, 1, \alpha, \alpha+1\}$ where α is the root of the irreducible polynomial $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. The number of primitive elements of L is $\phi(3)$=2. Since 1 is not a primitive element, then automatically the primitive elements of L are $\{\alpha, \alpha + 1\}$.

$$\alpha^1 = \alpha$$
$$\alpha^2 = \alpha + 1$$
$$\alpha^3 = \alpha^2 + \alpha = 1$$

Hence α is a generator of L. We proceed the same with $\alpha + 1$.

Corollary 2.11. *[9] Let $\mathbb{F}_{q^t}$ be an extension $\mathbb{F}_q$. Then $\mathbb{F}_{q^t}$ is a simple extension of $\mathbb{F}_q$, in fact for any primitive element u of $\mathbb{F}_{q^t}$ we have $\mathbb{F}_{q^t} = \mathbb{F}_q(u)$.*

Proof. $\mathbb{F}_{q^t} =< u > \cup\{0\} = \{u, u^2, u^3, \ldots, u^{q^t-1} = 1\} \cup \{0\}$. Since $\mathbb{F}_{q^t}$ is an extension of $\mathbb{F}_q$, then clearly $\mathbb{F}_{q^t} =< u > \cup\{0\} \supseteq \mathbb{F}_q(u) = \mathbb{F}_{q^t}^* \cup \{0\}$. Since u is a primitive element of $\mathbb{F}_{q^t}$. Hence $\mathbb{F}_{q^t} = \mathbb{F}_q(u)$. □

Now we are ready to prove the existence of irreducible polynomial for every prime p and every positive integer n.

Corollary 2.12. *[9] For every finite field $\mathbb{F}_q$ and every positive integer $n \geq 1$, there exists an irreducible polynomial of degree n over $\mathbb{F}_q$.*

Proof. Let $\bar{q} = q^n$. Then $\mathbb{F}_{\bar{q}}$ is a simple extension of $\mathbb{F}_q$. That is $\mathbb{F}_{\bar{q}} = \mathbb{F}_q(u)$ for any primitive element u. Therefore we have $n = [\mathbb{F}_{\bar{q}} : \mathbb{F}_q] = [\mathbb{F}_q(u) : \mathbb{F}_q]$. But $n = [\mathbb{F}_q(u) : \mathbb{F}_q] = deg(Irr(u, \mathbb{F}_q))$. Therefore we obtain an irreducible polynomial of degree n over $\mathbb{F}_q$. □

Before given a formula to calculate the number of irreducible polynomial of degree n over the prime field $\mathbb{F}_p[x]$, we shall give properties of the roots of irreducible polynomial of degree n.

2.4 Roots of irreducible polynomials over $\mathbb{F}_q$.

In this section we shall give the nature of roots of irreducible polynomial of degree n in finite field $\mathbb{F}_q$. Let $\mathbb{F}_q$ be a finite field and p be a characteristics of the finite field $\mathbb{F}_q$.

Lemma 2.13. *[9] Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial and α be a root of f in some extension K of $\mathbb{F}_q$. Then for a polynomial $h \in \mathbb{F}_q[x]$, we have $h(\alpha) = 0$ if and only if $f \mid h$ in $\mathbb{F}_q[x]$.*

Proof. Let $g(x) = Irr(\alpha, \mathbb{F}_q)$ and $f(x) = c^{-1}g(x)$ for $c \in \mathbb{F}_q$.
Clearly $h(\alpha) = 0 \iff g(x) \mid h(x)$. Hence we have $c^{-1}g(x) \mid h(x) \iff f(x) \mid h(x)$. □

Given an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree m. The following theorem gives us the nature of the roots of f in the extension $\mathbb{F}_{q^m}$.

Theorem 2.14. *[9] Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m. Then f has a root $\alpha \in \mathbb{F}_{q^m}$. Moreover all the roots of f are simple and they are $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$.*

Proof. Let α be the root of the polynomial f with degree m in some splitting field $\mathbb{F}_q(\alpha)$. Since f is irreducible and $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Then $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. So $\alpha \in \mathbb{F}_{q^m}$.
Now we show that $\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are also the roots $f(x)$.

Let $f(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0$ with $a_i \in \mathbb{F}_q$. We know that $f(\alpha) = 0$ since α is the root of f.
First we show that $(f(\alpha))^{q^i} = f(\alpha^{q^i})$ for $0 \leq i \leq m-1$

$$\begin{aligned}
(f(\alpha))^{q^i} &= (a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_0)^{q^i} \text{ for } 0 \leq i \leq m-1 \\
&= (a_{m-1}\alpha^{m-1})^{q^i} + (a_{m-2}\alpha^{m-2})^{q^i} + \cdots + (a_0)^{q^i} \\
&= (a_{m-1})^{q^i}(\alpha^{q^i})^{m-1} + (a_{m-2})^{q^i}(\alpha^{q^i})^{m-2} + \cdots + {a_0}^{q^i} \\
&= a_{m-1}(\alpha^{q^i})^{m-1} + a_{m-2}(\alpha^{q^i})^{m-2} + \cdots + a_0 \\
&= f(\alpha^{q^i})
\end{aligned}$$

But since $f(\alpha)$=0, we have $f(\alpha^{q^i}) = 0$ for $0 \leq i \leq m-1$. Hence all the roots of f are α^{q^i} for $0 \leq i \leq m-1$. Note that $\alpha^{q^m} = \alpha$ since $\alpha \in \mathbb{F}_{q^m}$. Now we need to show that all the roots of f are distinct. Suppose

$$\begin{aligned}
\alpha^{q^i} &= \alpha^{q^j} \text{for } 0 \leq i < j \leq m-1 \\
\alpha^{q^{m-j+i}} &= \alpha
\end{aligned}$$

Hence α satisfies the polynomial $h(x) = x^{q^{m-j+i}} - x$. And by Lemma 2.13, we have $f \mid h$. But this is a contradiction since the degree of h is less than f. □

Corollary 2.15. *[9] If $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of $\deg m$ then the splitting field of f over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^m}$=$\mathbb{F}_q(\alpha)$ where α is any root of f in $\mathbb{F}_{q^m}$. All the roots of f are $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$.*

Proof. For the proof just apply the above theorem. □

Definition 2.8. [9] Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$. Then the conjugates of α with respect to $\mathbb{F}_q$ are $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$.

Proposition 2.16. *[9] The conjugates of $\alpha \in \mathbb{F}_q$ with respect to any subfield K has the same order in the multiplicative group $\mathbb{F}_q^*$.*

Proof. Let c be a primitive element in $\mathbb{F}_q$. Then $\mathbb{F}_q^* = \{c, c^2, c^3, \ldots, c^{q-1} = 1\}$. Let $\alpha = c^k$. Let the order of α be denoted as ord(α). Then

$$\begin{aligned}
\text{ord}(\alpha) &= \text{ord}(c^k) \\
&= \frac{\text{ord}(c)}{\gcd(k, \text{ord}(c))}
\end{aligned}$$

So the conjugates of α with respect to the subfield K $\subseteq \mathbb{F}_q$ with $K = \mathbb{F}_{p^s}$ is given by : $\alpha, \alpha^{p^s}, \alpha^{p^{2s}}, \ldots, \alpha^{p^{s(t-1)}}$ that is $c^k, c^{pks}, c^{pk2s}, \ldots, c^{ps(t-1)}$ with $t = [\mathbb{F}_q : \mathbb{F}_{p^s}]$.
For $0 \leq j \leq t$ we have

$$\begin{aligned}
\text{ord}(\alpha^{p^{js}}) &= \text{ord}(c^{k^{pjs}}) \\
&= \frac{\text{ord}(c)}{\gcd(kp^{js}, \text{ord(c)})} \\
&= \frac{q-1}{\gcd(kp^{js}, q-1)}
\end{aligned}$$

$q-1 = p^{st}-1$ is relatively prime with p^{js}. So the $\gcd(kp^{js}, q-1) = \gcd(k, q-1)$ So ord$(\alpha^{p^{js}}) =$ ord(α). So all the conjugates of α have the same order. □

Corollary 2.17. *[9] If α is a primitive element of $\mathbb{F}_q$ then all the conjugates of α are primitive elements over any sub field K of $\mathbb{F}_q$.*

Proof. The proof is deduced from Proposition 2.16. □

Example 2.13. Consider the irreducible polynomial $g(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$. By Theorem 2.14, the polynomial g has a root $\alpha \in \mathbb{F}_{3^2}$.

We check whether α is a generator of $\mathbb{F}_9^*$.

$$\begin{aligned}\alpha^2 &= 2\alpha + 1\\ \alpha^4 &= (2\alpha+1)(2\alpha+1) = 2\\ \alpha^8 &= (2)(2) = 4 = 1\end{aligned}$$

So α is a primitive element $\mathbb{F}_9^*$. Therefore

$$\begin{aligned}\mathbb{F}_9^* &= \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8\}\\ &= \{\alpha, 2\alpha+1, 2\alpha+2, 2, 2\alpha, \alpha+2, 1\}\end{aligned}$$

By Corollary 2.15, the roots of f are α and $\alpha^3 = 2\alpha + 2$. These roots have the same order and are primitive elements of $\mathbb{F}_9^*$. In the following section we shall discuss $\mathbb{F}_q$-Automorphisms and further use it to define the Trace of a root of an irreducible polynomial.

2.5 $\mathbb{F}_q$-automorphisms of $\mathbb{F}_{q^n}$

Definition 2.9. [9] A map $\sigma : \mathbb{F}_{q^n} \mapsto \mathbb{F}_{q^n}$ is called an $\mathbb{F}_q$ automorphism if:

- $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ for all $\alpha, \beta \in \mathbb{F}_{q^n}$
- $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$
- σ is bijective
- $\sigma(c) = c$ for all $c \in \mathbb{F}_q$

Proposition 2.18. *[9] The map $\phi : \mathbb{F}_{q^n} \mapsto \mathbb{F}_{q^n}$ such that $\alpha \mapsto \alpha^q$ is an $\mathbb{F}_q$ automorphism.*

Proof. Let the prime p be the characteristics of the field $\mathbb{F}_q$ and $\alpha, \beta \in \mathbb{F}_{q^n}$.

$$\begin{aligned}\phi(\alpha+\beta) &= (\alpha+\beta)^q\\ &= \alpha^q + \beta^q \text{ by Theorem } 2.1\\ &= \phi(\alpha) + \phi(\beta)\end{aligned}$$

Now we prove the second statement

$$\phi(\alpha\beta) = (\alpha\beta)^q = \alpha^q\alpha^q = \phi(\alpha)^q\phi(\alpha)^q$$

We now prove the third statement and we first prove injectivity. Suppose $\alpha, \beta \in \mathbb{F}_{q^n}$

$$\begin{aligned} \phi(\alpha) &= \phi(\beta) \\ \alpha^q &= \beta^q \\ (\alpha-\beta)^q &= 0 \text{ by Theorem 2.1} \\ \alpha - \beta &= 0 \\ \alpha &= \beta \end{aligned}$$

We now prove Surjectivity. Since $\phi : \mathbb{F}_{q^n} \mapsto \mathbb{F}_{q^n}$ is injective and $\mid \mathbb{F}_{q^n} \mid = q^n$ is finite, we conclude that ϕ is surjective. □

Definition 2.10. [9] The $\mathbb{F}_q$ automorphism $\phi : \mathbb{F}_{q^n} \mapsto \mathbb{F}_{q^n}$ such that $\alpha \mapsto \alpha^q$ is called a Frobenius Map.

Now we state a theorem about the group automorphism and the proofs can be found in [5].

Theorem 2.19. *[9] The distinct $\mathbb{F}_q$- automorphisms of $\mathbb{F}_{q^n}$ are the maps $\sigma^0, \sigma^1, \sigma^2, \ldots, \sigma^{n-1}$*

$$\begin{aligned} \sigma^i : &\mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \\ &\alpha \longmapsto \sigma^i(\alpha) = \alpha^{q^i} \end{aligned}$$

where Moreover $\sigma^i = \phi^i = \phi \circ \phi \circ \cdots \circ \phi$ for $0 \leq i \leq n-1$. This set of distinct automorphisms form a group under composition of mapping. This group is cyclic group of order n generated by the Frobenius map σ.

Notation : We denote the group of automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ as $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.
Now we give the definition of the trace of an element in $\mathbb{F}_{q^n}$. And also state some properties without giving any proof.

Definition 2.11. [9] The trace of an element α with respect to the extension F/K denoted $\text{Tr}_{\text{F/K}}(\alpha)$, is given by $\text{Tr}_{\text{F/K}}(\alpha) = \sum_{\sigma \in \text{AutF}/K} \sigma(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$.
If $K = \mathbb{F}_p$, then $\text{Tr}_{\text{F/K}}(\alpha) = \text{Tr}_F(\alpha)$. And we called $\text{Tr}_F(\alpha)$ the absolute trace.

Remark 2.4. Notice the trace of α is just the sum of conjugates of α with respect F/K.

Properties of Trace: Let $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^n}$ then $\text{Tr}_{\text{F/K}}$: $F \mapsto K$ satisfies

- $\text{Tr}_{\text{F/K}}(\alpha + \beta) = \text{Tr}_{\text{F/K}}(\alpha) + \text{Tr}_{\text{F/K}}(\beta)$
- $\text{Tr}_{\text{F/K}}(c\alpha) = c\text{Tr}_{\text{F/K}}(\alpha)$ for $c \in K$ and $\alpha \in \mathbb{F}_{q^n}$
- $\text{Tr}_{\text{F/K}}$ is surjective if the $\gcd(n, q) = 1$
- $\text{Tr}_{\text{F/K}}(c) = nc$ for $c \in K$, $n = [F : K]$

- $\text{Tr}_{F/K}(\alpha^{q^i}) = \text{Tr}_{F/K}(\alpha)$ for all i such that $0 \leq i \leq n-1$

The proof of the above properties are obvious and can be obtained in [9].

Example 2.14. Let $\alpha \in \mathbb{F}_{2^3}$ be a root of the polynomial $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Determine the trace of α.
The polynomial $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ is irreducible over $\mathbb{F}_2$. Then $\mathbb{F}_2[x]/(f(x))$ is a field. By Proposition 2.3, $\mathbb{F}_{2^3}$ is isomorphic to $\mathbb{F}_2(\alpha)$ and $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of $\mathbb{F}_2(\alpha)$. So

$$\mathbb{F}_{2^3} = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_2\} = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$$

By Theorem 2.14, the roots of f in $\mathbb{F}_2(\alpha)$ are $\alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha + 1$.

$$\text{Tr}_F(\alpha) = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + \alpha^2 + \alpha + 1 = 1$$

The conjugates of α have the same trace value.

2.6 Counting Irreducible Polynomials of degree n over finite field by the Inclusion and exclusion Principle

Gauss gave a formula to count the number of irreducible polynomials over finite fields. And he used the notion of Moebius inversion function in order to proof his formula. In this thesis we shall use the Inclusion and Exclusion Principle to count the number of irreducible polynomials over finite fields and then confirm our result with Gauss Formula. This method is solely based on finite fields. Before we begin, we state inclusion -exclusion principle without proving it.

Theorem 2.20. $(Inclusion-ExclusionPrinciple)$ *[18] Let* $\mid A \mid$ *denote the cardinal number of a set* A *then it follows that*

$$\mid A \cup B \mid = \mid A \mid + \mid B \mid - \mid A \cap B \mid .$$

The more general formula can be generalized in the following way:
Let $\{A_i\}$ *for* $0 \leq i \leq p$ *be a collection of subsets of a set* S *then*
$\mid A_1 \cup A_2 \cup \cdots \cup A_p \mid$
$= \sum_{1 \leq i \leq p} \mid A_i \mid - \sum_{1 \leq i_1 < i_2 \leq p} \mid A_{i_1} \cap A_{i_2} \mid + \sum_{1 \leq i_1 < i_2 < i_3 \leq p} \mid A_{i_1} \cap A_{i_2} \cap A_{i_3} \mid$
$- \cdots + (-1)^{p-1} \mid A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap \cdots \cap A_{i_p} \mid .$

Example 2.15. Let $S = \{1, 2, \ldots, 10\}$, $A_1 = \{2, 3, 7, 9, 10\}$, $A_2 = \{1, 2, 3, 9\}$, $A_3 = \{2, 4, 9, 10\}$. We have the following:
$A_1 \cap A_2 = \{2, 3, 9\}$, $A_1 \cap A_3 = \{2, 3, 10\}$, $A_2 \cap A_3 = \{2, 9\}$ $A_1 \cap A_2 \cap A_3 = \{2, 9\}$
$\mid A_1 \cup A_2 \cup A_3 \mid = (5 + 4 + 4) - (3 + 3 + 2) + 2 = 7$

Theorem 2.21. *[5] The number* $N_q(n)$ *of monic irreducible polynomials of degree* n *in* $\mathbb{F}_q[x]$ *is given by:*

$$N_q(n) = 1/n \sum_{d/n} \mu(n/d) q^d = 1/n \sum_{d/n} \mu(d) q^{\frac{n}{d}}$$

where

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ (-1)^k \text{ if } n \text{ is the product of } k \text{ distinct primes} \\ 0 \text{ if } n \text{ is divisible by the square of a prime} \end{cases}$$

As mentioned above we shall prove this theorem using Inclusion and exclusion principle. Before the proof, we will give some remarks of finite fields which are going to be useful to state the formula of the number of irreducible polynomial of degree n over $\mathbb{F}_q$.

Remark 2.5.

- For any prime p and any positive integer n, there exists a finite field of order $q = p^n$ and this field is unique up to isomorphism. And we denote that field as $\mathbb{F}_q$.
- The splitting field of any irreducible polynomial of degree n over $\mathbb{F}_q[x]$ is $\mathbb{F}_{q^n}$.
- Any irreducible polynomial of degree n over $\mathbb{F}_q$ have n distinct roots in $\mathbb{F}_{q^n}$.
- Any two irreducible polynomials of degree n over $\mathbb{F}_q$ cannot have a common root in $\mathbb{F}_{q^n}$.
- All the sub fields of $\mathbb{F}_{q^n}$ are in bijection with the divisors of n.

Proof. We now prove Theorem 2.21. For $n = 1$, the number of monic irreducible polynomial over $\mathbb{F}_q$ is q since all the polynomials of the form $x - a_i$ for $a_i \in \mathbb{F}_q$ are irreducible. This is also confirmed by the Gauss formula when we substitute $n = 1$ in the formula $N_q(n) = 1/n \sum d/n\mu(n/d)q^d = 1/n \sum d/n\mu(d)q^{n/d}$.
Now we assume that $n > 1$.
Let R_n denote the collection of the roots of all irreducible polynomials of degree n over $\mathbb{F}_q$. And let T_n denote the collection of all irreducible polynomials of degree n over $\mathbb{F}_q$. Then by Remarks 2.5 above the collection of all the roots is given by:

$$R_n = nT_n$$

So now we calculate R_n explicitly:

$$R_n = \begin{cases} \{\alpha \in \mathbb{F}_{q^n} \mid f(\alpha) = 0\} \\ \{\alpha \in \mathbb{F}_{q^n} \mid [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n\} \\ \{\alpha \in \mathbb{F}_{q^n} \mid \alpha \text{ is not contained in any proper subfield of } \mathbb{F}_{q^n}\} \\ \{\alpha \in \mathbb{F}_{q^n} \mid \alpha \text{ is not contained in any maximal subfield of } \mathbb{F}_{q^n}\} \end{cases}$$

Let $n = u^a v^b w^c \cdots d^s$ be a prime factorization of n with r distinct prime factors. Then the maximal subfields of $\mathbb{F}_q$ are of the form
$F_u = \mathbb{F}_{q/u}, F_v = \mathbb{F}_{q/v}, F_w = \mathbb{F}_{q/w}, \ldots, F_d = \mathbb{F}_{q/d}$ by Remark 2.5 above.
By the fourth interpretation given above

$$\mid R_n \mid = \mid (F_u \cup F_v \cup F_w \cdots \cup F_d)^c \mid$$

where the complement is taken over $\mathbb{F}_{q^n}$. By 5 of Remark 2.5, we have $F_u \cap F_v = \mathbb{F}_{q^{n/uv}}$, $F_u \cap F_w = \mathbb{F}_{q^{n/uw}}$, $F_u \cap F_v \cap F_w = \mathbb{F}_{q^{n/uvw}} \cdots F_u \cap F_v \cdots \cap F_d = \mathbb{F}_{q^{n/uv\ldots d}}$. We now calculate the cardinality of $\mid R_n \mid$ by applying the inclusion and exclusion principle:

$$\begin{aligned} \mid R_n \mid \; &= q^n - q^{n/u} - q^{n/v} - q^{n/w} + \cdots - q^{n/uv} - q^{n/uw} \\ &\quad -q^{n/wv} - \cdots + q^{n/uvw} + q^{n/uvd} + q^{n/udw} + \cdots + (-1)^r q^{n/uvw\cdots r} \end{aligned} \tag{2.1}$$

So we obtain T_n by dividing by R_n by n. □

We proved the theorem by using finite fields instead of using Moebius inversion formula used in number theory.

Example 2.16. Find the number of all irreducible polynomials of degree 12 over $\mathbb{F}_7$:
$n = 2^2 \cdot 3$, $F_2 = \mathbb{F}_{12/2}$ $F_3 = \mathbb{F}_{12/3}$, $F_2 \cap F_3$=$\mathbb{F}_{12/6}$
So

$$\mid R_{12} \mid = 7^{12} - 7^6 - 7^4 + 7^2.$$

Hence the number of monic irreducible polynomials of degree 12 is given by:

$$P_{12} = 1/12(7^{12} - 7^6 - 7^4 + 7^2)$$

In the previous section, we saw that given a prime p and a positive integer n, there always exists an irreducible polynomial of $\deg n$ over the finite field $\mathbb{F}_p$. So far, we have not seen a deterministics algorithm to construct such irreducible polynomials but there exists algorithms to factorise square free polynomials into irreducible polynomials. One of this algorithm that we shall discuss is the Berlekamp Algorithm. So one can choose a square free polynomial and then use Berlekamp Algorithm to get irreducible polynomials. But this is first of all a Probabilistic Algorithm since in priority, one does not know which degree he will get.

2.7 Berlekamp Algorithm

Given a square free monic polynomial $b(x)$ of $\deg n$, we will determine its complete factorization. For what follows, let $q = p^n$ where p is a prime number and $\mathbb{F}_q$= $GF(q)$ is a finite field consisting of q elements. $V = \mathbb{F}_q[x]/(b(x)) = \{r(x) + (b(x)) \mid \deg r(x) < \deg b(x)\}$ be a ring of residue classes of polynomials. We shall identify an element $r(x) + (b(x))$ of V as $r(x) \mod b(x)$.
Let $W = \{v(x) \in V \mid (v(x))^q = v(x) \mod b(x)\}$.

Theorem 2.22. *[3] The subset W of V is a subspace.*

Proof. W is non-empty set since every element in $\mathbb{F}_q$ belongs in W. Let $t(x), h(x) \in W$.

- $(h(x) + t(x))^q = (h(x))^q + (t(x))^q = h(x) + t(x) \mod b(x)$. Hence $h(x) + t(x) \in W$.

- Let $d \in \mathbb{F}_q$ $(dh(x))^q = d^q(h(x))^q = dh(x) \mod b(x)$. Hence $dh(x) \in W$

Thus W is a subspace of V. □

Theorem 2.23. *[3] If $b(x)$ is irreducible then the dimension of subspace W is one.*

Proof. $b(x)$ is irreducible polynomial implies $V = \mathbb{F}_q[x]/(b(x))$ is a field. The polynomial $p(t) = t^q - t$ has at most q roots. By Fermat Little Theorem, $r^q = r$ for all $r \in \mathbb{F}_q$ so each of the q elements of $\mathbb{F}_q$ satisfy $r^q - r = 0$. Hence all the q roots of the polynomial $p(t)$ are constant in $\mathbb{F}_q$. That is consists of constant polynomial and can be identified with $\mathbb{F}_q$ which is generated by a single element $\{1\}$. So W is a subspace of dimension one in V. □

The following theorem tells us the number of irreducible factors of the polynomial $b(x)$.

Theorem 2.24. *[3] Let $b(x)$ be a square free polynomial. Then dimension of the subspace W is equal to the number of irreducible factors of $b(x)$.*

Proof. Let $b(x) = b_1(x)b_2(x)\cdots b_k(x)$ be the unique monic irreducible factorization of $b(x)$. For each i from 1 to k, let $V_i = \mathbb{F}_q[x]/(b_i(x))$. By the Chinese Remainder Theorem, $\mathbb{F}_q[x]/b(x) \cong \mathbb{F}_q[x]/b_1(x) \times \mathbb{F}_q[x]/b_2(x) \times \cdots \times \mathbb{F}_q[x]/b_k(x)$ through the ring isomorphism

$$\begin{aligned} \phi : & V \to V_1 \times V_2 \times \cdots \times V_k \\ v(x) \mod b(x) & \longmapsto (v(x) \mod b_1(x), v(x) \mod b_2(x), \ldots, v(x) \mod b_k(x)). \end{aligned}$$

The restrictions of ϕ on W induces a map

$$\phi_W : W \mapsto W_1 \times W_2 \times W_3 \times \cdots \times W_k$$

where $W_i = \{s \in V_i \mid s^q = s \mod b_i(x)\}$ for $i = 0, 1, \ldots, k$. In order to prove that the dimension of W is k, it suffices to show that ϕ_W is an isomorphism.

First we show that ϕ_W is surjective. Let $(c_1, c_2, c_3, \ldots, c_k) \in (W_1 \times W_2 \times W_3 \times \cdots \times W_k)$. Since ϕ is surjective, there exists an element $h(x) \in V$ such that $\phi(h(x)) = (c_1, c_2, c_3, \ldots, c_k)$.
Then we have $\phi(v(x)^q)) = (c_1^q, c_2^q, c_3^q, \ldots, c_k^q) = (c_1, c_2, \ldots, c_k) = \phi(h(x))$. But since ϕ is an isomorphism, it follows that $v(x) \in W$. Then injectivity of ϕ_W follows directly from the fact that ϕ has the same property. So the dimension W equals the number of irreducible polynomial of $b(x)$. Assuming we know the number of elements of W. We now show how to find the irreducible factors of $b(x)$.

Theorem 2.25. *[3] Let $b(x)$ be a monic square free polynomial in $\mathbb{F}_q[x]$ and let $v(x)$ be a non-constant polynomial in W. Then*

$$b(x) = \prod_{s \in \mathbb{F}_q} \gcd(v(x) - s, b(x)).$$

Proof. We first show that $b(x) \mid \prod_{s\in\mathbb{F}_q} gcd(b(x), v(x) - s)$ for $x \in \mathbb{F}_q[x]$,

$$x^q - x = \prod_{s\in\mathbb{F}_q} (x - s). \tag{2.2}$$

From above,

$$v(x)^q - v(x) = \prod_{s\in\mathbb{F}_q} (v(x) - s)$$

$v(x) \in W$ implies that $b(x) \mid v(x)^q - v(x) = \prod_{s\in\mathbb{F}_q}(v(x) - s)$. This implies, $b_i(x) \mid \prod_{s\in\mathbb{F}_q}(v(x) - s)$ for all $i = 1, \ldots, k$. Since $\gcd(b_i(x), b_j(x)) = 1$ for $i \neq j$ and for any two distinct elements $s, t \in \mathbb{F}_q$ $\gcd(v(x) - s, v(x) - t) = 1$, we get $b_i(x) \mid v(x) - s_i$ for exactly one i. Therefore, $b_i(x) \mid \gcd(b(x), v(x) - s_i)$ implies that $b(x) \mid \prod_{s\in\mathbb{F}_q} gcd(b(x), v(x)-s)$. Now we show that $\prod_{s\in\mathbb{F}_q} gcd(b(x), v(x)-s) \mid b(x)$. Clearly, $\gcd(b(x), v(x) - s) \mid b(x)$ for all s and since $v(x) - s$ are relatively prime for distinct s, we have $\prod_{s\in\mathbb{F}_q} gcd(b(x), v(x) - s) \mid b(x)$. Hence we have

$$b(x) = \prod_{s\in\mathbb{F}_q} \gcd(v(x) - s, b(x)).$$

□

Now we present a method how to determine the elements of W. Let $\{1, x, \ldots, x^{n-1}\}$ be a basis of V. Let $v(x) \in \mathbb{F}_q[x]$. Then

$$\begin{aligned}(v(x))^q &= (x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0)^q \\ &= x^{(n-1)q} + (a_{n-2})^q x^{(n-2)q} + \cdots + a_0^q \\ &= v(x^q) \text{ since each } a_i \in \mathbb{F}_q.\end{aligned}$$

Therefore

$$\begin{aligned}W &= \{v(x) \in \mathbb{F}_q[x] \mid (v(x))^q = v(x) \mod b(x)\}. \\ &= \{v(x) \in \mathbb{F}_q[x] \mid v(x^q) = v(x) \mod b(x)\}.\end{aligned}$$

Since $\{1, x, \ldots, x^{n-1}\}$ is a basis of V and W is a subspace of V. Then for $0 \leq j \leq n - 1$,

$$x^{qj} = q_{0,j} + q_{1,j}x + \cdots + q_{n-1,j}x^{n-1} \mod b(x).$$

Let coefficient matrix of this system of equation be an $n\times n$ matrix $M = (q_{i,j})_{(0\leq i,j\leq n-1)}$.

Theorem 2.26. *[3] Given W and M as defined previously, then*

$$W = \{v = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_{q^n} \mid (M - I)v = 0\}$$

Proof. $v(x^q) = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} q_{i,j}x^j$ where $(q_{i,j})$ is the $n \times n$ coefficient matrix of the system of equations

$$x^{qj} = q_{0,j} + q_{1,j}x + \cdots + q_{n-1,j}x^{n-1} \mod b(x).$$

For any $v(x) \in W$

$$\begin{aligned} 0 = v(x^q) - v(x) &\iff \sum_{j=0}^{n-1} a_j (\sum_{i=0}^{n-1} q_{j,i} x^i) - \sum_{j=0}^{n-1} a_j x^j \\ &\iff \sum_{i=0}^{n-1} (\sum_{i=0}^{n-1} a_j q_{j,i} - a_j) x^i \mod b(x) \\ &\iff \sum_{j=0}^{n-1} a_j q_{j,i} - a_j = 0 \text{ for all } i = 0, 1, \ldots, n-1. \end{aligned}$$

This is equivalent to $M.(v_0, \ldots, v_{n-1}) - (v_0, \ldots, v_{n-1}) = (0, \ldots, 0)$. Therefore, we have $(M - I).v = (0, \ldots, 0)$. So $v(x) \in W \iff (M - I).v = (0, \ldots, 0)$. In order to find the basis of W, it suffices to find a null space of the matrix $M - I$. □

Now we describe a method how to compute M. Computing M requires that we express x^{qi} as linear combination of $\{1, x, \ldots, x^{n-1}\}$ for $i = 0, \ldots, n-1$. This can be done using iterative procedure that generates $x^{t+1} \mod b(x)$ given that $x^t \mod b(x)$ has been determined. Assume that $b(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + x^n$.

$$\begin{aligned} x^t &= b_{t,0} + b_{t,1} x + b_{t,2} x^2 + \cdots + b_{t,n-2} x^{n-2} + b_{t,n-1} x^{n-1} \mod b(x) \\ x^{t+1} &= b_{t,0} x + b_{t,1} x^2 + b_{t,2} x^3 + \cdots + b_{t,n-1} x^{n-1} + b_{t,n-1} x^n \mod b(x) \\ &= b_{t,0} x + b_{t,1} x^2 + b_{t,2} x^3 + \cdots + b_{t,n-2} x^{n-1} + \\ & b_{t,n-1}(-a_0 - a_1 x - a_2 x^2 - \cdots - a_{n-1} x^{n-1}) \\ &= b_{t,n-1} a_0 + x(b_{t,0} - a_1 b_{t,n-1}) + x^2 (b_{t,1} - b_{t,n-1} a_2) + \cdots + \\ & ((b_{t,n-1} - b_{t,n-1} a_{n-1})) x^{n-1} \\ &= d_{t+1,0} + d_{t+1,1} x + \cdots + d_{t+1,n-1} x^{n-1} \end{aligned}$$

where $d_{t+1,0} = -b_{t,n-1}$ and $d_{t+1,i} = b_{t,i-1} - b_{t,n-1} a_i$. So the entries of the matrix M is obtained by storing a vector d of elements from $\mathbb{F}_q$:

$$d \leftarrow (d_0, d_1, \ldots, d_{n-1})$$

d is initialised as

$$d \leftarrow (1, \ldots, 0)$$

and is updated by

$$d \leftarrow (-b_{n-1}.a_0, b_0 - b_{n-1}.a_1, \ldots, b_{n-2} - b_{n-1}.a_{n-1})$$

After the $(iq)^{th}$ iteration, the entries of the vector are copied into the i^{th} column of the M-matrix. So computing the M matrix requires qn multiplications for each column since there are n columns. So the number of operations to generate the entire matrix is $O(qn^2)$ operations in $\mathbb{F}_q$. After obtaining the matrix M, by the method described above, we find the null space of the matrix $M - I$ which corresponds to the basis of W. Then we apply Theorem 2.25. This process is applied repeatedly until the number of factors equal to the dimension of W.

Theorem 2.27. *[3] The cost of the Berlekamp algorithm for computing factors of a monic square polynomial $b(x)$ of $\deg n$ which has k distinct irreducible polynomials over $\mathbb{F}_q$ is $O(k \cdot q \cdot n^2 + n^3)$ operations in $\mathbb{F}_q$.*

Proof. Each k factors require q gcd calculations. Each cost approximately n^2 operations. In order to find the null space of $M - I$, we perform the Gaussian elimination method which cost $O(n^3)$ operations in $\mathbb{F}_q$. Therefore the total cost of the algorithm is $O(k \cdot q \cdot n^2 + n^3)$ operations in $\mathbb{F}_q$. □

Example 2.17. Let $f(x) = x^4 + x^2 + x + 1 \in \mathbb{F}_2[x]$. We use Berlekamp Algorithm to factor the above polynomial.
The derivative of f is relative prime to f therefore, f has no repeated roots. Now we compute the power $x^{2i} \mod f(x)$ for $0 \leq i \leq 3$. This yields

$$\begin{aligned} x^0 &= 1 \mod f(x) \\ x^2 &= x^2 \mod f(x) \\ x^4 &= 1 + x + x^2 \mod f(x) \\ x^6 &= 1 + x + x^3 \mod f(x) \end{aligned}$$

So the 4×4 Matrix is given by :

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

and the matrix $M - I$ is :

$$M - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

The basis for the null space of the matrix $M - I$ are $\{1, 0, 0, 0\}$ and $\{0, 0, 1, 1\}$ and the polynomial of each are $t_1(x) = 1$ and $t_2(x) = x^2 + x^3$ respectively. Since the dimension of the null space is 2, we are sure that the number of irreducible factors of f is 2. Applying Theorem 2.25, we calculate

$$\gcd(f(x), t_2(x) - 0) = x + 1, \ \gcd(f(x), t_2(x) - 1) = x^3 + x^2 + 1$$

So our desired factorization is $f(x) = (x + 1)(x^3 + x^2 + 1)$.

□

In the following section, we will give a brief introduction about modules and Group Algebras, this will help us to proof the Normal basis theorem and the condition for a linearly independent set to form a normal basis in the next chapter.

2.8 Brief Introduction to Modules

Definition 2.12. Let R be a commutative ring. A (left) R-Module is an additive abelian group M equipped with a map $R \times M \mapsto M$ $(r, m) \mapsto rm$ satisfying

- $(r_1 + r_2)m_1 = r_1m_1 + r_2m_1$
- $r(m_1 + m_2) = rm_1 + rm_2$
- $r_1(r_2m) = (r_1r_2)m$
- $1m = m$

for all $r_1, r_2 \in R$ and $m_1, m_2 \in M$.

A left-Module M is said to be unitary if $1_R \cdot u = u$ for every $u \in M$. A right R-module has the similar definition as above but the difference is that the elements of R are on the right side to that of the elements of M. If R is commutative then the left-module and the right Module coincide.
Properties of Modules
Let M be an R-Module and $x \in M$, $r \in R$, we distinguish between 0_M and 0_R.

- $r0_M = 0_M$
- $0_Rx = 0_M$
- $(-r)x = r(-x) = -(rx)$

Example 2.18. Let $R = \mathbb{F}$ be a field. Then all the vector spaces over $\mathbb{F}$ are $\mathbb{F}$-modules.

Example 2.19. Let $R = \mathbb{F}[x]$ where $\mathbb{F}$ a field. If V is an $\mathbb{F}$ vector space and $T : V \mapsto V$ a linear map(vector space endomorphism) then V may be regarded as $F[X]$-module via

$$f(X) \cdot v = f(T)(v)$$

for $v \in V$. Different maps T yield different $F[X]$-module.

2.8.1 Module Homomorphism

Definition 2.13. A module homomorphism is a map $f : M \mapsto N$ between two modules over a ring R with the following properties:

- $f(x + y) = f(x) + f(y)$ for all $x, y \in M$.
- $f(rx) = rf(x)$ for all $r \in R$ and $x \in M$.

2.8.2 Group Algebra

Let K be a field and G be a group. The group algebra $K[G]$ with operation $\cdot$ is the set of all linear combination of finitely many elements of G with coefficients in K. That is all the elements of the form

$$a_1 g_1 + a_2 g_2 + \cdots + a_n g_n$$

where $a_i \in K$ and $g_i \in G$ for all $i = 1, \ldots, n$. The element in $K[G]$ is of the form $\sum_{g \in G} a_g g$ where it is assumed that $a_g = 0$ for all but finitely many elements of g.
$K[G]$ is an algebra over K with respect to the addition and multiplication defined as follows:

- $\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$.
- product by a scalar is given by: $a(\sum_{g \in G} a_g g) = \sum_{g \in G} (a a_g) g$.
- Multiplication of two elements: $(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{x \in G} (c_x \cdot x)$ where $x = gh$ and $c_x = \sum_{g \in G} a_g b_{g^{-1}x}$. It follows that the identity element 1 of G is the unit of $K[G]$ and $K[G]$ is commutative if and only if G is an abelian group.

CHAPTER 3

Basics of Normal Basis

For many years, Normal basis has been used to represent elements of finite fields and this is mostly advantageous in the hardware implementation of arithmetic operations such as Squaring and Exponentiation which are done at most at no cost over field of characteristics 2. Hensel (1888) in [12] deeply studied normal basis over finite fields and proved that they always exists. Eisentein (1850) in [8] has already noted that the normal basis already exist. Hensel and Ore (1934) derive a formula to count the number of such basis. Perlis [15] proved that if degree n of irreducible polynomial is a prime power, then the polynomial is normal if and only if its trace is non-zero. In [6], if $n = 2^r p^k$ is degree of irreducible polynomial and 2 is a primitive root $\mod p^k$, then the irreducible polynomial over $\mathbb{F}_p$ is normal if and only if its trace is non-zero.
Let p be a prime, $q = p^r$ for some positive integer r and $\mathbb{F}_q$ denotes a field with q elements. The characteristics of the field $\mathbb{F}_q$ is p. And $\mathbb{F}_{q^n}$ is an n dimensional vector space over $\mathbb{F}_q$.
The trace function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for $\alpha \in \mathbb{F}_{q^n}$ is given by:

$$\mathrm{Tr}_{F_{q^n}/q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}$$

It is a linear functional and the trace of an element over its prime field is called the absolute Trace. Let $\alpha \in \mathbb{F}_{q^n}$. If the set $N = \{\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots, \alpha^{q^{n-1}}\}$ is linearly independent, then we call N a normal basis of $\mathbb{F}_{q^n}$ and the element α is called a Normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. A polynomial f of degree n is a Normal polynomial if it irreducible polynomial over $\mathbb{F}_q$ and the roots of f are all the elements of N. Hence a normal polynomial is another way of describing normal basis.

In this chapter our main aim is to find the conditions for which an element $\alpha \in \mathbb{F}_{q^n}$ is a normal element and later look for conditions such that an irreducible polynomial over $\mathbb{F}_q$ is a normal polynomial. We will begin by reviewing some concepts of linear algebra.

Let V be an n dimensional vector space over a field K and $T : V \mapsto V$ be a linear operator on V. The characteristics polynomial of T is

$$\triangle_T = det(xI - T)$$

which is a monic polynomial and $\deg \triangle_T = n = dim_K V$. Let f be a polynomial such that $f(T) = 0$, then we say that f is annihilated by T.
Let K be a field. Consider the set

$$J_T = \{g \in K[x] \mid g(T) = 0\}$$

J_T is non-empty, by Cayley Hamitonian Theorem, $\triangle_T(T) = 0$, so $\triangle_T \in J_T$. Clearly the set J_T is an ideal of $K[x]$ and the set J_T is a principal ideal. So there is exists a monic polynomial of smallest degree which generates J_T and we write

$$J_T =< \gamma_T >$$

γ_T is called the minimal polynomial of T that is monic polynomial of smallest degree over K such that $\gamma_T(T) = 0$. For any polynomial $g(x) \in K[x]$, $g(T)$ is a linear transformation on V. The null space of $g(T)$ consists of all vectors $\alpha \in V$ such that $g(T)\alpha = 0$. The monic polynomial $g(x) \in K[x]$ of smallest degree such that $g(T)\alpha = 0$ is called the T-order of α or the minimal polynomial of α and this polynomial is denoted as $ord_{\alpha,T}(x)$. Also $ord_{\alpha,T}(x) \mid h(x)$ for any polynomial $h(x) \in K[x]$ such that $h(T)\alpha = 0$.

Definition 3.1. [9] An element α is called a cyclic vector for the linear operator T on V if the set $\{\alpha, T(\alpha), T^2(\alpha), T^3(\alpha), \ldots, T^{k-1}(\alpha)\}$ spans V for $k = \mathbf{dim}_K V$.

The following lemma will help us to characterize cyclic vectors over V, It's proof is given in [10].

Lemma 3.1. *[10] Let T be a linear operator on a finite dimensional vector space V. Then V has a cyclic vector if and only the characteristics and the minimal polynomial of the linear map T defined on V are equal.*

Lemma 3.2. *[9] Let G be group and K be a field and let $T_1, T_2, \ldots, T_n : G \mapsto K^*$ be distinct homomorphism of groups of G and $K^* = K\{0\}$. Then $T_1, T_2, \ldots, T_n$ are linearly independent over K in the sense that if $(a_1, a_2, \ldots, a_m) \neq (0, 0, \ldots, 0)$. Then $a_1T_1(g) + a_2T_2(g) + \cdots + a_nT_n(g) \neq 0$ for some $g \in G$.*

Let $V = \mathbb{F}_{q^n}$ be a vector space over $K = \mathbb{F}_q$ and consider the Frobenius Map

$$\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$$
$$\alpha \longmapsto \alpha^q$$

Since for all $\alpha, \beta \in \mathbb{F}_{q^n}$ $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(c\alpha) = c\sigma(\alpha)$, then σ is consider as a linear operator. The distinct automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are $G = \{\sigma^0, \sigma^1, \sigma^2, \ldots, \sigma^{n-1}\}$ which form a group under composition of mapping and the order of σ is n.

Lemma 3.3. *[13] Let V be an n- dimensional extension of the field and σ be the Frobenius map. Then the minimal and characteristics equation of σ are equal both to $x^n - 1$.*

Proof. The distinct automorphisms $\sigma^0, \sigma^1, \sigma^2, \ldots, \sigma^{n-1}$ of V over K form a group and the $ord(\sigma) = n$ since $\sigma^n = I$. The characteristics polynomial $\triangle_\sigma = det(xI - \sigma) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{K}[x]$.
$x^n - 1$ is annihilated by σ because $\sigma^n - I = 0$. Therefore, the minimal polynomial $\gamma_\sigma \mid \triangle_\sigma$. So $\deg \gamma_\sigma \leq n$. In fact, $\deg \gamma_\sigma = n$. Suppose on the contrary that $\deg \gamma_\sigma < n$ then σ satisfies the relation $a_{n-1}\sigma^{n-1} + a_{n-2}\sigma^{n-2} + \cdots + a_1\sigma + a_0 = 0$ for some $a_0, a_1, \ldots, a_{n-1} \in K$. But this will contradicts Lemma 3.1 because $I, \sigma, \ldots, \sigma^{n-1}$ are n distinct homomorphism which are linearly independent in sense of Lemma 3.1. Therefore, $\deg \gamma_\sigma = n$. $\gamma_\sigma \mid x^n - 1$ with $\deg \gamma_\sigma = n$ implies that $\gamma_\sigma = x^n - 1$. On the other hand, $\gamma_\sigma \mid \triangle_\sigma$ and $\triangle_\sigma$ is monic polynomial of degree $n = dim_K V$. Therefore $x^n - 1 \mid \triangle_\sigma$ implies $\triangle_\sigma = \gamma_\sigma = x^n - 1$. □

Theorem 3.4. *[7] Let E be a finite extension field over K with dimension n. And assume that the Galois group G of E over K denoted as $Gal(E/K)$ is cyclic of order n. Then there exists an element $\alpha \in E$ which generate a normal basis over K.*

Before given the proof, we remark that the additive group $(E, +)$ of E can be viewed as a module over the group algebra $K[G]$, where the scalar multiplication is defined by

$$\sum_{y \in G} a_y y \cdot \alpha := \sum_{y \in G} a_y y(\alpha)$$

Proof. Let σ be a generator of G. Let $G = \{id, \sigma, \ldots, \sigma^{n-1}\}$ where $n := |G|$ is the degree of E over K. Then for every $g \in K[G]$, there exists a unique polynomial $c = \sum_{i=0}^{n-1} c_i x^i \in K[x]$ of deg at most $n - 1$ with $\alpha \in E$ such that

$$g \cdot \alpha = c(\sigma)(\alpha)$$

where

$$c(\sigma)(\alpha) := \sum_{i=0}^{n-1} c_i \sigma^i(\alpha)$$

Since $\sigma^n(\alpha) = id$ is the identity element on E for all $\alpha \in E$. Therefore

$$(x^n - 1)\sigma(\alpha) = \sigma^n(\alpha) - id(\alpha) = \alpha - \alpha = 0$$

for all $\alpha \in E$. Therefore $x^n - 1$ is the $\sigma-$order of α since $\{\sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ is linearly independent. Moreover since the dimension of E over K is equal to the degree of $x^n - 1$, then this polynomial is also the characteristics polynomial of α with respect to σ. Now from Lemma 3.1 since the minimal polynomial and the characteristics polynomial of α with respect σ equal $x^n - 1$, therefore there exists an $\alpha \in E$ such that the set $M = \{\sigma^i(\alpha)\}$ span E for $i \in \mathbb{N}$. For $k \in \mathbb{N}$, $\sigma^k(\alpha) = \sigma^{n+k}(\alpha)$ since $ord(\sigma) = n$. Therefore, $M = \{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ span E. Therefore $M = \{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ is a basis of E since the dimension of E is n. □

Remark 3.1. If E is an n-dimensional cyclic Galois extension over K and σ is a generator of G. Then $\alpha \in E$ is normal over K if and only if the minimal polynomial of α with respect to σ (this is the monic polynomial of least degree such that $f(\sigma)(\alpha) = 0$) is equal to $x^n - 1$, where $n = |G|$.

Let $E = \mathbb{F}_{q^n}$ and $K = \mathbb{F}_q$ and σ be the Frobenius map defined on E. If an element $\alpha \in E$ is normal then $\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ is linearly independent and minimal polynomial of α with respect to σ is $x^n - 1$. So there is no polynomial of smaller degree less than n that annihilates σ. That is α is the cyclic vector of σ on E. So an element $\alpha \in E$ is cyclic if and only if the minimal polynomial of α with respect to σ over K is $x^n - 1$. Let p be the characteristic of K and $n = mp^e$ with $\gcd(p, m) = 1$. Let $p^e = t$. Suppose $x^n - 1$ has the factorization in K

$$x^n - 1 = (\mu_1(x)\mu_2(x) \cdots \mu_r(x))^t \tag{3.1}$$

where μ_i are distinct irreducible factors of $x^n - 1$. Suppose also that μ_i has degree d_i for $i = 1, 2, \ldots r$. Let

$$\bar{\mu_i}(x) = \frac{x^n - 1}{\mu_i(x)} \tag{3.2}$$

for $i = 0, 1, \ldots, r$. Then we have a following characterization of Normal elements in $\mathbb{F}_{q^n}$.

Theorem 3.5. *[17] An element $\alpha \in \mathbb{F}_{q^n}$ is normal if and only if $\bar{\mu_i}(\sigma)\alpha \neq 0$ for $i = 0, 1, \ldots, r$ where σ is the Frobenius map and $\bar{\mu_i}$ is defined in equation 3.2.*

Proof. Suppose α is a normal element in $\mathbb{F}_{q^n}$ then $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This implies that the minimal polynomial of α with respect to σ is equal to $x^n - 1$. Therefore for $i = 0, 1, \ldots, r \bar{\mu_i}(\sigma)\alpha \neq 0$. The converse of the proof is given in [17]. □

3.1 Characterization of Normal Polynomials

In the previous section we saw that irreducible polynomial over $\mathbb{F}_q$ whose roots are linearly independent is called a Normal Polynomial. In this section we will give conditions such that irreducible polynomials over $\mathbb{F}_q$ are normal.
Let f be an irreducible polynomial over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ be the root of f. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is called the polynomial basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The direct way to check whether α^{q^i} for $i = 0, 1, \ldots, n-1$ is a normal element is to write

$$\alpha^{q^i} = \sum_{j=0}^{n-1} b_{i,j}\alpha^j$$

where $b_{i,j} \in \mathbb{F}_q$ and α^j for $0 \leq j \leq n-1$ is the polynomial basis. If the $n \times n$ matrix $(b_{ij})_{0 \leq i,j \leq n-1}$ is non-singular then the set $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ is linearly independent therefore f is a normal polynomial. This method is not efficient since it requires a lot of computation especially if n is too large. The natural question to ask, is there a simple criteria to identify Normal polynomials. The answer is yes in certain cases. We first give the following definition before reformulating Theorem 3.5.

Definition 3.2. [9] Let $K = \mathbb{F}_q$. The polynomial $L_f(x) = \sum_{i=0}^{n} c_i x^{q^i} \in K[x]$ corresponding with the polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$ is called the linearized $q-$associate

of $f(x)$. Conversely, $f(x) = \sum_{i=0}^{n} c_i x^i$ is called convectional $q-$associate of the $q-$polynomial $\sum_{i=0}^{n} c_i x^{q^i}$ in $K[x]$.

Theorem 3.6. *[19] Let f be an irreducible polynomial of degree n over $\mathbb{F}_q$ and let α be a root of f. Let*

$$x^n - 1 = (\mu_1(x)\mu_2(x)\cdots\mu_r(x))^t$$

where μ_i are distinct irreducible factors of $x^n - 1$ and $t \in \mathbb{N}$. Suppose also that μ_i has degree d_i for $i = 1, 2, \ldots, r$. Then the polynomial f is normal if and only if

$$L_{\bar{\mu_i}}(\alpha) \neq 0$$

where $\bar{\mu_i}(x) = \frac{x^n-1}{\mu_i(x)}$ for each $i = 0, 1, \ldots, r$ and $L_{\bar{\mu_i}}(x)$ is the linearised $q-$ associate of $\bar{\mu_i}(x)$.

The proof of the above theorem is just a reformulation the proof of Theorem 3.5 since $L_{\bar{\mu_i}}(\alpha) = \bar{\mu_i}(\sigma)\alpha$ where α is a root of f. The following concepts in [9] will be freely used in our next examples.

Definition 3.3. [9] Let $n \geq 1$ be an integer and K be a field with characteristics p. Suppose $\gcd(p, n) = 1$ and ξ be a primitive n^{th} root of unity over K. The polynomial $Q_n(x) = \prod_{k:\gcd(k,n)=1}^{n}(x - \xi^k)$ is called the n cyclotomic polynomial over K.

Theorem 3.7. *[9] Let K be a field with characteristics p and n is an integer not divisible by p. Then*

- $x^n - 1 = \prod_{d|n} Q_d(x)$
- *If $K = \mathbb{F}_q$ with (n,q)=1 and $d = Ord(q) \mod n$ then $Q_n(x)$ factors into $\frac{\phi(n)}{d}$ irreducible distinct polynomial of the same degree d over K where ϕ is the Euler function.*

The proof of the following Theorem is given in [9]

Example 3.1. Let $f(x) = 1 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ be a monic irreducible polynomial of degree $n = p^e$ over $\mathbb{F}_q$ and α is a root of f. We wish to determine under which conditions f is a normal polynomial.
$x^n - 1 = (x - 1)^{p^e}$. Hence $\mu(x) = 1 + x + x^2 + \cdots + x^{n-1}$ and $L_\mu(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}$ = $\mathbf{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = -a_{n-1}$. Therefore our polynomial is Normal if and only if $\mathbf{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$. This is a known result in [15].

Example 3.2. Let $f(x) = 1 + x + \cdots + a_{n-1}x^{n-1} + x^n$ be a monic irreducible polynomial over $\mathbb{F}_p$ of degree n where n is a prime and p is a primitive element $\mod n$. We determine conditions under which f is normal.
$\mu_1(x) = x - 1$ and $\mu_2 = 1 + x + x^2 + \cdots + x^{n-1}$. Let α be a root of f. The necessary and sufficient conditions for f to be normal is that

- $L_{\mu_1}(\alpha) = \mathbf{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} \neq 0$

- $L_{\mu_2}(\alpha) = \alpha^p - \alpha \neq 0$

The second condition is obvious since the roots of f must be distinct.

In the following example, we determine conditions under which irreducible polynomials over $\mathbb{F}_2$ of degree 23 are normal polynomial.

Example 3.3. Let $p = 2$. Find the conditions under which the irreducible polynomial of degree 23 over $\mathbb{F}_2$ form a normal basis. Since 2 is a primitive element $\mod 23$, we have the following factorisation

$$x^{23} - 1 = (x+1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$

$$\begin{aligned}
\bar{\mu_1}(x) &= x^{22} + x^{21} + \cdots + x + 1 \\
\bar{\mu_2}(x) &= x^{12} + x^{10} + x^7 + x^4 + x^3 + x^2 + x + 1 \\
\bar{\mu_3}(x) &= x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^2 + 1
\end{aligned}$$

So the linearized polynomial of each of the above polynomials is given by:

$$\begin{aligned}
L_{\bar{\mu_1}}(x) &= x^{2^{22}} + x^{2^{21}} + \cdots + x \\
L_{\bar{\mu_2}}(x) &= x^{2^{12}} + x^{2^{10}} + x^{2^7} + x^{2^4} + x^{2^3} + x^{2^2} + x^2 + x \\
L_{\bar{\mu_3}}(x) &= x^{2^{12}} + x^{2^{11}} + x^{2^{10}} + x^{2^9} + x^{2^8} + x^{2^5} + x^{2^2} + x
\end{aligned}$$

Let $\alpha \in \mathbb{F}_{2^{23}}$ of a irreducible polynomial of degree 23 over $\mathbb{F}_2$, the conjugates of α form a normal basis if and only if

$$\mathrm{Tr}_{\mathbb{F}_{2^{23}}/\mathbb{F}_2}(\alpha) \neq 0 \tag{3.3}$$

$$\alpha^{2^{12}} + \alpha^{2^{10}} + \alpha^{2^7} + \alpha^{2^4} + \alpha^{2^3} + \alpha^{2^2} + \alpha^2 + \alpha \neq 0, \tag{3.4}$$

$$\alpha^{2^{12}} + \alpha^{2^{11}} + \alpha^{2^{10}} + \alpha^{2^9} + \alpha^{2^8} + \alpha^{2^5} + \alpha^{2^2} + \alpha \neq 0 \tag{3.5}$$

So we just need to express each $\alpha^{2^{12}}, \alpha^{2^{11}}, \alpha^{2^{10}}, \alpha^{2^9}, \alpha^{2^8}, \alpha^{2^7}$ as a linear combination of $\{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{21}\}$. Therefore an irreducible polynomial of degree 23 over $\mathbb{F}_2$ is normal polynomial if a root α of f satisfy the above conditions in 3.3, 3.4and 3.5.

Example 3.4. Let $f(x) = x^2 + a_1 x + a_2$ be an irreducible polynomial over $\mathbb{F}_q$. Then f is normal if and only if $a_1 \neq 0$.

Corollary 3.8. *[17] Let $n = p^e r$ where r is a prime different from p and q is a primitive element $\mod r$. Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be an irreducible polynomial over $\mathbb{F}_q$ and α be a root of f. Let $u = \sum_{i=0}^{p^e-1} \alpha^{q^{ir}}$. Then f is normal if and only if $a_1 \neq 0$ and $u \notin \mathbb{F}_q$.*

Proof. $x^n - 1 = x^{rp^e} - 1 = (x^r - 1)^{p^e} = (x-1)^{p^e}(x^{r-1} + x^{r-2} + \cdots + 1)^{p^e}$ since q is a primitive element $\mod r$, the polynomial$(x^{r-1} + x^{r-2} + \cdots + 1)^{p^e}$ is irreducible over $\mathbb{F}_q$. Hence

$$\mu_1(x) = \frac{x^n - 1}{x - 1} = \sum_{i=1}^{n-1} x^i$$

and

$$\mu_2(x) = \frac{x^n - 1}{x^{r-1} + x^{r-2} + \cdots + 1} = (x-1)\frac{x^n - 1}{x^r - 1}$$

$$= (x-1)\sum_{i=0}^{p^e-1} x^{ir} = \sum_{i=0}^{p^e-1} x^{ir+1} - \sum_{i=0}^{p^e-1} x^{ir}$$

It follows

$$L_\mu(\alpha) = \sum_{i=0}^{p^e-1} \alpha^{q^{ir+1}} - \sum_{i=0}^{p^e-1} \alpha^{q^{ir}} = (\sum_{i=0}^{p^e-1} \alpha^{q^{ir}})^q - \sum_{i=0}^{p^e-1} \alpha^{q^{ir}}$$

So f is normal if and only if $a_1 \neq 0$ and $(\sum_{i=0}^{p^e-1} \alpha^{q^{ir}})^q \neq \sum_{i=0}^{p^e-1} \alpha^{q^{ir}}$ $i.e$ $u^q \neq u$. □

The following example will be the motivation for our next chapter .

Example 3.5. Consider the trinomial $x^p - a_1 x^{p-1} + a \in \mathbb{F}_p[x]$ where p is an odd prime. This polynomial is irreducible over $\mathbb{F}_q$ where $\gcd(p, n) = 1$ and $q = p^n$. Determine the conditions under which this polynomial is normal.
Let α be a root of f. Then $x^p - 1 = (x-1)^p$. Hence $\bar{\mu}(x) = 1 + x + x^2 + \cdots + x^{n-1}$. $L_{\bar{\mu}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}$ = $\mathbf{Tr}_{\mathbb{F}_{q^p}/\mathbb{F}_p}(\alpha) = -a_1$. Therefore our polynomial is Normal if and only if $\mathbf{Tr}_{\mathbb{F}_{q^p}/\mathbb{F}_q}(\alpha) = -a_1 \neq 0$

Therefore from the example above, we can conclude that the irreducible polynomial $f(x) = x^p - x + a$ over $\mathbb{F}_q$ is not normal where $\gcd(p, n) = 1$ but its reciprocal $f^*(x) = x^p - x^{p-1} + a$ is normal. In the next chapter we shall discuss how to provide free storage basis conversion from the roots of the polynomial $f^*(x) = x^p - x^{p-1} + 1$ to the polynomial basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ and vice versa. We summarized this Chapter by giving the steps to determine if a polynomial is normal over an extension field.

3.2 Steps To Determine if an irreducible polynomial is normal over the subfield $K = \mathbb{F}_q$ of $F = \mathbb{F}_{q^n}$.

Let $\alpha \in F$ be a root of an irreducible polynomial f of degree n over K.

1. $\mathbf{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$, otherwise f is not normal over K.

2. If n=p^k, $f(x)$ must be a normal polynomial over K. [15].
3. if n= $2^r p^k$ and 2 is a primitive root modulo p^k, f must be a normal polynomial over K [6].
4. Factorize $x^n - 1 = \prod_{i=1}^{r} (\mu_i(x))^t$. Let $\mu_1(x) = x - 1$ and find $\bar{\mu}_i(x) = \frac{x^n-1}{\mu_i(x)}$ for $i \in \{2, \ldots, r\}$.
5. Compute the $q-$ associate $L_{\bar{\mu}_i}(x)$ for $i \in \{2, \ldots, r\}$.
6. If $L_{\bar{\mu}_i}(x)$ is not divided by $f(x)$ for $i \in \{2, \ldots, r\}$, then f is a normal polynomial otherwise f is not normal over K.

CHAPTER 4

Free Storage Basis Conversion over Extension Fields

In [16], the author represented the field element of the extension field $\mathbb{F}_{p^p}$ by using the irreducible polynomial $f(x) = x^p - x - 1 \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. Furthermore, he found a way of constructing efficiently Normal basis of the field $\mathbb{F}_{p^p}$. Together with the polynomial basis of $\mathbb{F}_{p^p}$, he provided a free storage basis conversion over $\mathbb{F}_{p^p}$. In this chapter, we shall provide a free storage basis conversion over $\mathbb{F}_{q^p}$ where $q = p^n$, $\gcd(p, n) = 1$ and p is an odd prime using the irreducible polynomial $f(x) = x^p - x - 1 \in \mathbb{F}_p[x]$ over $\mathbb{F}_q$.
Trinomials over finite fields $K = \mathbb{F}_q[x]$ are polynomials of the form $x^n + ax^k + b$ where $(n \geq k \geq 0)$ and $ab \neq 0$. Irreducible trinomial has a structure that makes it a pleasant choice for representing extension field. The reduction operation can be faster if an irreducible trinomial is used, therefore choosing an irreducible trinomial can lead to a faster arithmetic operation implementation of the field [11]. In this chapter, we shall use the irreducible trinomials $f(x) = x^p - x + 1 \in \mathbb{F}_p[x]$ over $\mathbb{F}_q$ where $q = p^n$ as field polynomial to construct the polynomial basis of $\mathbb{F}_{q^p}$ and later form the normal basis of field $\mathbb{F}_{q^p}$ by using the reciprocal of the polynomial f. We shall provide a free storage basis conversion between the two basis.

Definition 4.1. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + 1$ be a monic irreducible polynomial of $\deg n$ over $\mathbb{F}_p$. The reciprocal of f denoted as f^* is defined by

$$\begin{aligned} f^*(x) &= x^n f(1/x) \\ &= x^n + \cdots + a_{n-1}x + 1 \end{aligned}$$

We state without proofs the following two lemmas.

Lemma 4.1. *[9] The reciprocal of a monic irreducible polynomial over finite field K is also irreducible polynomial over K.*

Theorem 4.2. *[9] Let $q = p^n$, the polynomial $f(x) = x^p - x + 1 \in \mathbb{F}_p[x]$ is irreducible over $\mathbb{F}_{p^n}$ with $\gcd(p, n) = 1$.*

Let $f(x) = x^p - x + 1 \in \mathbb{F}_p[x]$ then $\mathbb{F}_q[x]/_{<f(x)>}$ is a field and is consider as a vector space over $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_{q^p}$ be a root of f. Therefore $\mathbb{F}_q[x]/_{<f(x)>} \cong \mathbb{F}_q(\alpha)$ and $\{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p-1}\}$ is a basis of $\mathbb{F}_q(\alpha)$. From [15], the irreducible polynomial

$f(x) = x^p - x + 1$ over $\mathbb{F}_q$ is not normal. But the reciprocal polynomial $f^*(x) = x^p - x^{p-1} + 1 \in \mathbb{F}_p[x]$ is normal in $\mathbb{F}_{q^p}$.
Let $\beta \in \mathbb{F}_{q^p}$ be a root of f^*, then all the distinct roots of f^* are $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{p-1}}$ and the set $\{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{p-1}}\}$ form a normal basis of the vector space $\mathbb{F}_q(\beta)$. Our aim is to provide a free storage conversion from the polynomial basis to the normal basis of the vector space $\mathbb{F}_q(\beta)$. To do this, we shall express each β^{q^i} for $1 \leq i \leq p-1$ as a linear combination of α^i, $0 \leq i \leq p-1$ and therefore form the transition matrix for the conversion of the polynomial basis to the normal basis.
The Frobenius map σ of $\mathbb{F}_{q^p}$ over $\mathbb{F}_q$ is defined as:

$$\begin{aligned} \sigma : \mathbb{F}_{q^p} &\to \mathbb{F}_{q^p} \\ \beta &\longmapsto \beta^q \end{aligned}$$

α is a root of f implies that $\alpha^p = \alpha - 1$. We have the following by using the Freshman Dream:

$$\begin{aligned} \alpha^{p^2} &= (\alpha - 1)^p = \alpha^p - 1^p = \alpha - 2 \\ \alpha^{p^3} &= (\alpha - 2)^p = \alpha^p - 2^p = \alpha - 3 \end{aligned}$$

So by induction, we have

$$\alpha^{p^n} = (\alpha - n + 1)^p = \alpha^p - n^p + 1^p = \alpha - n$$

Clearly $\beta = \alpha^{-1} = 1 - \alpha^{p-1}$.

$$\begin{aligned} \beta^q &= (1 - \alpha^{p-1})^q = 1 - \alpha^{q(p-1)} = 1 - (\alpha - n)^{(p-1)} \\ \beta^{q^2} &= 1 - (\alpha - n)^{(p-1)^q} = 1 - (\alpha - n)^{q(p-1)} \\ &= 1 - (\alpha^q - n^q)^{p-1} = 1 - (\alpha - 2n)^{p-1} \\ \beta^{q^3} &= 1 - (\alpha - 2n)^{(p-1)^q} = 1 - (\alpha^q - (2n)^q)^{p-1} = 1 - (\alpha - 3n)^{p-1} \end{aligned}$$

In same way up to k=p-1, we have

$$\beta^{q^{p-1}} = 1 - ((\alpha - (p-2)n)^q)^{p-1} = 1 - (\alpha - n(p-1))^{p-1}$$

Now we want to find $(\alpha - nk)^{p-1}$ for $0 \leq k \leq p-1$. By binomial expansion formula

$$\begin{aligned} (\alpha - nk)^{p-1} &= \sum_{j=0}^{p-1} \binom{p-1}{j} \alpha^{p-1-j}(-nk)^j \\ &= \sum_{j=0}^{p-1} \binom{p-1}{j} \alpha^{p-1-j}(k)^j(-n)^j \end{aligned}$$

From Number theory, $\binom{p-1}{j}$ is a an integer, so it must be an element of the prime field.

Lemma 4.3. *Let p prime number and j be positive integer less than p. Then $\binom{p-1}{j} = (-1)^j \mod p$.*

Proof. $\binom{p-1}{j} = \frac{(p-1)!}{j!(p-1-j)!}$. By Wilson's Theorem, $(p-1)! \equiv -1 \mod p$. If we show that $j!(p-1-j)! \equiv (-1)^{1-j} \mod p$ then we are done. Consider the following statement:
Let $S_j : j!(p-1-j)! \equiv (-1)^{1-j} \mod p$. We shall prove by induction that the statement S_j is true. For $j = 0$, Left Hand Side (LHS) of S_j is given by $(p-1)!$ and Right Hand Side (RHS) is given by $(-1) \mod p$. So we conclude by Wilson's Theorem that LHS equals the RHS. Assume that the statement is true for $j \in \mathbb{N}$, we now prove that is true for $j+1$:

$$\begin{aligned}(j+1)!(p-1-(j+1))! &= (j+1)!(p-1-j-1)! \\ &= (j+1)\frac{j!(p-1-j)!}{p-1-j} \\ &\equiv \frac{j+1}{p-1-j}(-1)^{1-j} \mod p \text{ By the induction Hypothesis.}\end{aligned}$$

We have

$$\begin{aligned}(j+1)!(p-1-(j+1))!(p-1-j) &\equiv (j+1)(-1)^{1-j} \mod p \\ -(j+1)!(p-1-(j+1))!(j+1) &\equiv (j+1)(-1)^{1-j} \mod p\end{aligned}$$

Therefore we obtain,

$$(j+1)!(p-1-(j+1))! \equiv (-1)^j \mod p$$

by the induction principle, our statement S_k is true for any $k \in \mathbb{N}$ □

$$\begin{aligned}(\alpha - nk)^{p-1} &= \sum_{j=0}^{p-1} \binom{p-1}{j} \alpha^{p-1-j}(-nk)^j \\ &= \sum_{j=0}^{p-1} (-1)^j \alpha^{p-j-1}(-n)^j k^j \\ &= \sum_{j=0}^{p-1} \alpha^{p-j-1} k^j n^j\end{aligned}$$

Therefore,

$$\beta^{q^k} = 1 - \sum_{j=0}^{p-1} \alpha^{p-j-1} k^j n^j \text{ for } 0 \leq k \leq p-1$$

For k=1, we have

$$\beta^q = -\alpha^{p-1} - n\alpha^{p-2} - n^2\alpha^{p-3} - \cdots - n^{p-2}\alpha$$

For k=2, we have

$$\beta^{q^2} = -\alpha^{p-1} - (2)(n)\alpha^{p-2} - (2^2)(n^2)\alpha^{p-3} - \cdots - (n^{p-2})(2^{p-2})\alpha$$

In the same way up to for $k = p - 1$ we have

$$\beta^{q^{p-1}} = -\alpha^{p-1} - n(p-1)\alpha^{p-2} - n^2(p-1)^2\alpha^{p-3} - \cdots - n^{p-2}(p-1)^{p-2}\alpha.$$

So in matrix representation we have,

$$\begin{pmatrix} \beta \\ \beta^q \\ \beta^{q^2} \\ \vdots \\ \beta^{q^{p-2}} \\ \beta^{q^{p-1}} \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & 1 \\ -(n)^0 & -(n)^1 & -(n)^2 & \dots & -(n)^{p-2} & 0 \\ -(2n)^0 & -(2n)^1 & -(2n)^2 & \dots & -(2n)^{p-2} & 0 \\ \vdots & & & & & \\ -(n(p-2))^0 & -(n(p-2))^1 & -(n(p-2))^2 & \dots & -(n(p-2))^{p-2} & 0 \\ -(n(p-1))^0 & -(n(p-1))^1 & -(n(p-1))^2 & \dots & -(n(p-1))^{p-2} & 0 \end{pmatrix} \begin{pmatrix} \alpha^{p-1} \\ \alpha^{p-2} \\ \alpha^{p-3} \\ \vdots \\ \alpha \\ 1 \end{pmatrix}$$

Or equivalently $\bar{\beta} = M\bar{\alpha}$ where the transition matrix $M \in \mathbb{F}_p^{p\times p}$ and we donot extra memory to store M and the complexity to obtain the coefficients of M is $O(p^2 \log^3 p)$.

Theorem 4.4. *The matrix*

$$M = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & 1 \\ -1 & -(n)^1 & -(n)^2 & \dots & -(n)^{p-2} & 0 \\ -1 & -(2n)^1 & -(2n)^2 & \dots & -(2n)^{p-2} & 0 \\ \vdots & & & & & \\ -1 & -(n(p-2))^1 & -(n(p-2))^2 & \dots & -(n(p-2))^{p-2} & 0 \\ -1 & -(n(p-1))^1 & -(n(p-1))^2 & \dots & -(n(p-1))^{p-2} & 0 \end{pmatrix}$$

is the transition matrix from the polynomial basis $\{1, \alpha, \alpha^2, \dots, \alpha^{p-1}\}$ *to the normal basis* $\{\beta, \beta^q, \beta^{q^2}, \dots, \beta^{q^{p-1}}\}$ *of the vector space* $\mathbb{F}_{q^p}$ *over* $\mathbb{F}_q$ *where* α *is the root* $f(x) = x^p - x + 1$ *and* $\beta = \alpha^{-1}$.

Lemma 4.5. *Let* $k \in \mathbb{F}_p^*$. *Then*

$$\sum_{m=0}^{p-2} k^m \mod p \equiv \begin{cases} -1 & \mod p \text{ if } k = 1 \\ 0 & \mod p \text{ otherwise} \end{cases}$$

Proof. If $k = 1$, then $\sum_{m=0}^{p-2} 1^m \mod p = p - 1 \mod p = -1$.
Suppose $k \neq 1$

$$\begin{aligned} \sum_{m=0}^{p-2} k^m \mod p &= 1 + k^2 + k^3 + k^4 + \cdots + k^{p-2} \\ &= \frac{1(k^{p-1} - 1)}{k - 1} \mod p \\ &= 0 \text{ since } k \in \mathbb{F}_{p^*} \end{aligned}$$

This sum is a Geometric progression with common ratio k. □

Theorem 4.6. *Let*

$$M = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & 1 \\ -1 & -(n)^1 & -(n)^2 & \dots & -(n)^{p-2} & 0 \\ -1 & -(2n)^1 & -(2n)^2 & \dots & -(2n)^{p-2} & 0 \\ \vdots & & & & & \\ -1 & -(n(p-2))^1 & -(n(p-2))^2 & \dots & -(n(p-2))^{p-2} & 0 \\ -1 & -(n(p-1))^1 & -(n(p-1))^2 & \dots & -(n(p-1))^{p-2} & 0 \end{pmatrix}$$

The inverse of M can be computed by simple transpose of the permuted rows of the matrix M.

Proof. The $p \times p$ matrix M contains a $(p-1) \times (p-1)$ a sub matrix

$$Q = \begin{pmatrix} -1 & -(n)^1 & -(n)^2 & \dots & -(n)^{p-2} \\ -1 & -(2n)^1 & -(2n)^2 & \dots & -(2n)^{p-2} \\ \vdots & & & & \\ -1 & -(n(p-2))^1 & -(n(p-2))^2 & \dots & -(n(p-2))^{p-2} \\ -1 & -(n(p-1))^1 & -(n(p-1))^2 & \dots & -(n(p-1))^{p-2} \end{pmatrix}$$

The matrix Q is called a Vandermonde matrix and is well known to be invertible. The corresponding Row entries $R_{i \mod p}$ of the matrix Q is just the power from i to $p-2$ of the field element ni for $0 \leq i, j \leq p-2$. The scalar multiplication of two rows can be obtained as follows:
$-R_{i \mod p} = (ni)^0, (ni)^1, (ni)^2, \dots, (ni)^{p-2}$
$-R_{j \mod p} = (nj)^0, (nj)^1, (nj)^2, \dots, (nj)^{p-2}$

$$\begin{aligned} R_{i \mod p} * R_{j \mod p} &= (ni * nj)^0 + (ni * nj)^1 + \dots + (ni * nj)^{p-2} \\ &= \begin{cases} -1 & \mod p \text{ if } ni * nj = 1 \mod p \\ 0 & \mod p \text{ otherwise due to Lemma 4.5} \end{cases} \\ &= \begin{cases} -1 & \mod p \text{ if } i * j = n^{-2} \mod p \\ 0 & \mod p \text{ otherwise due to Lemma 4.5} \end{cases} \end{aligned}$$

The above property allows to find the Inverse matrix Q^{-1} just by performing permutation on the rows on Q such that column(i) of Q^{-1} = -(Row(j) of $Q)^T$ where $i * j = n^{-2} \mod p$. Therefore we can write

$$C_{i \mod p} = -(R_{j \mod p})^T$$

where $j = i^{-1} * n^{-2}$ where C_i stands for the for the i^{th} column of the matrix Q^{-1}.

Now we present the steps for inversion of the Matrix M.
The inverse of the transition matrix M can be computed in 3 steps.

- Column 1 of M^{-1} is the p^{th} column of M upside down.

- Last Row of the Matrix M^{-1} is all 1
- The inverse of $(p-1) \times (p-1)$ matrix is equal to Q^{-1} as describe above.

□

Also transition matrix $M^{-1} \in \mathbb{F}_p^{p \times p}$ and we donot extra memory to store its coefficients and the time complexity to obtain its coefficients is $O(p^2 log^3 p)$ since M^{-1} is obtained just permutation of the row entries of M.

The following example illustrate how to find the inverse of the transition matrix M.

Example 4.1. Let q= 5^2. The transition matrix from the polynomial basis $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ to the normal Basis $\{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \beta^{q^4}\}$ of the vector space $\mathbb{F}_{q^5}$ over $\mathbb{F}_q$ where α is the root of the polynomial $x^5 - x + 1 \in \mathbb{F}_p[x]$ and $\beta = \alpha^{-1}$ is given by:

$$M = \begin{pmatrix} -1 & 0 & 0 & 0 & 1 \\ -1 & -2 & -4 & -3 & 0 \\ -1 & -4 & -1 & -4 & 0 \\ -1 & -1 & -1 & -1 & 0 \\ -1 & -3 & -4 & -2 & 0 \end{pmatrix}$$

Our $p-1 \times p-1$ matrix Q is given as follows:

$$Q = \begin{pmatrix} -1 & -2 & -4 & -3 \\ -1 & -4 & -1 & -4 \\ -1 & -1 & -1 & -1 \\ -1 & -3 & -4 & -2 \end{pmatrix}$$

Let C_i be the column of $Q^{-1}$and R_j be the Row of Q. Then using the relation $i * j = 2^{-2} = 4 \mod 5$

$$\begin{aligned} C_4 &= -R_1^T \text{ when j=1, i =4} \\ C_2 &= -R_2^T \\ C_3 &= -R_3^T \\ C_1 &= -R_4^T \end{aligned}$$

we obtain the matrix Q^{-1} as follows:

$$Q^{-1} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 1 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

The matrix M^{-1} is given by

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 3 & 4 & 1 & 2 \\ 0 & 4 & 1 & 1 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

and

$$M * M^{-1} \mod 5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

4.1 Avoiding the inverse in calculation of M^{-1}

Given the transition matrix M from polynomial to normal basis, in order to construct the M^{-1} we first found the inverse of the $p-1 \times p-1$ matrix Q using the relation $C_{i \mod p} = -(R_{j \mod p})^T$ where $j = i^{-1} * n^{-2} \mod p$ and C_i represents i^{th} entry of the column of M^{-1} and R_j represents the j^{th} row of M. The complexity of finding the inverse of each i^{th} entry is $O(\log^3 p)$ which is expensive. Due to the construction of M, we observe that the inversion of M is avoided by performing permutation as described below.
Each entry of the row matrix of M is nothing of the powers of the prime field element and j^{th} row entry of the submatrix Q is given by:

$$R_j = ((jn)^0, (jn)^1, (jn)^2, \ldots, (jn)^{p-2})$$

Using the relation $C_i = R_{j \mod p}$ where $j = i^{-1} * n^{-2} \mod p$, C_i column of Q^{-1} is computed as follow:

$$\begin{aligned} C_i &= ((n * i^{-1} * n^{-2})^0, (n * i^{-1} * n^{-2})^1, (n * i^{-1} * n^{-2})^2, \ldots, (n * i^{-1} * n^{-2})^{p-2}) \\ &= ((n^{-1} * i^{-1})^0, (n^{-1} * i^{-1})^1, (n^{-1} * i^{-1})^2, \ldots, (n^{-1} * i^{-1})^{p-2}) \end{aligned}$$

Since all the computations are done $\mod p$, we have the following:
$1 = (n^{-1}i^{-1})^{p-1} = (n^{-1}i^{-1})^{p-2} * (n^{-1}i^{-1})^1$ implies $(in) = (n^{-1}i^{-1})^{p-2}$. In the same way, we have

$$\begin{aligned} (in)^2 &= (n^{-1}i^{-1})^{p-3} \\ (in)^3 &= (n^{-1}i^{-1})^{p-4} \\ (ni)^4 &= (n^{-1}i^{-1})^{p-5} \\ &\vdots \\ (in)^{p-3} &= (n^{-1}i^{-1})^2 \\ (in)^{p-2} &= (n^{-1}i^{-1})^1 \\ (in)^{p-1} &= (n^{-1}i^{-1})^0 \end{aligned}$$

Therefore

$$C_i = ((in)^{p-1}, (in)^{p-2}, \ldots, (in)^2, (in)^1) \tag{4.1}$$

Example 4.2. Consider Example 4.1, for $j = 1$, first row in Q is $R_1 = -(1, 2, 4, 3)$, the corresponding column for R_1 by using the relation $i = j^{-1}n^{-2}$ is C_4. So applying Equation 4.1, we have $C_4 = (1, 2, 4, 3)$ which is in conformity with Example 4.1.

We easily observe that the entries of the C_i are just equal to that of R_j. This concludes that the construction of the matrix M is the same as the construction of the matrix M^{-1} and both have equal complexity.

4.2 Basis Conversion

4.2.1 Polynomial to Normal Basis Conversion

Normal basis can be computed from polynomial basis using the transition matrix described in 4.4. The matrix for converting from the polynomial basis to Normal basis is given as follow :

$$\begin{pmatrix} \beta \\ \beta^q \\ \beta^{q^2} \\ \vdots \\ \beta^{q^{p-2}} \\ \beta^{q^{p-1}} \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & \ldots & 0 & 1 \\ -(n)^0 & -(n)^1 & -(2)^2 & \ldots & -(n)^{p-2} & 0 \\ -(2n)^0 & -(2n)^1 & -(2n)^2 & \ldots & -(2n)^{p-2} & 0 \\ \vdots & & & & & \\ -(n(p-2))^0 & -(n(p-2))^1 & -(n(p-2))^2 & \ldots & -(n(p-2))^{p-2} & 0 \\ -(n(p-1))^0 & -(n(p-1))^1 & -(n(p-1))^2 & \ldots & -(n(p-1))^{p-2} & 0 \end{pmatrix} \begin{pmatrix} \alpha^{p-1} \\ \alpha^{p-2} \\ \alpha^{p-3} \\ \vdots \\ \alpha \\ 1 \end{pmatrix}$$

Let $q = p^n$. We provide an algorithm for converting polynomial to normal basis.
We shall provide two examples to show how the Algorithm 1 works.

Example 4.3. Let $q = 5^3$ with $n = 3$ and $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ be the polynomial basis of the finite field $\mathbb{F}_q(\alpha)$ where α is the root of the irreducible polynomial $x^5 - x + 1 \in \mathbb{F}_p[x]$. We shall perform Algorithm 1 steps by steps in order to obtain the Normal basis $\{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \beta^{q^4}\}$ where $\beta = \alpha^{-1}$

$q = 5^3, n = 3, z = 2$
$\beta[1] = (\alpha[5] - \alpha[1]) \mod 5$
i=1
$x = 1$, $y_1 = 0$, $y_2 = 0$, $x_1 = 0$, $x_2 = 0$, $x = 1$, $m = 1$
For $j = 1$ and $j = 2$,

y_1	y_2	x	x_1	x_2	m
-α[1]	-α[3]	3	-α[1]	-α[3]	-3
-α[1]-α[2]	-α[3]-3α[4]	$9 = 4 \mod 5$	-α[1]+3α[2]	-α[3]+3α[4]	$9 = 4 \mod 5$

$$\beta[2] = -\alpha[1] - 3\alpha[2] + 4(-\alpha[3] - 3\alpha[4]) = -\alpha[1] - 3\alpha[2] - 4\alpha[3] - 2\alpha[4] \mod 5$$

Algorithm 1 Polynomial Basis to Normal Basis Conversion

Input: $(\bar{\alpha} = \{\alpha^{p-1}, \alpha^{p-2}, \ldots, \alpha, 1\}, n)$
Output: $\bar{\beta} = \{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{p-1}}\}$

1: $z = \frac{p-1}{2}$
2: $\beta[1] = \alpha[p] - \alpha[1] \mod p$
3: **for** i =1 **to** z **do**
4: $x = 1; m = 1;$
5: $y_1 = 0; y_2 = 0; x_1 = 0, x_2 = 0;$
6: **for** j=1 to z **do**
7: $y_1 = (y_1 - x * \alpha[j]) \mod p;$
8: $y_2 = (y_2 - x * \alpha[z + j]) \mod p;$
9: $x = x * (ni) \mod p$
10: $x_1 = (x_1 - m * \alpha[j] \mod p)$
11: $x_2 = (x_2 - m * \alpha[z + j] \mod p)$
12: $m = m * (-ni)$
13: **end for**
14: $\beta[i + 1] = (y_1 + x * y_2) \mod p;$
15: $\beta[p - i + 1] = (x_1 + m * x_2) \mod p;$
16: **end for**
17: Output $= \bar{\beta}$

$$\beta[5] = -\alpha[1] - 3\alpha[2] + 4(-\alpha[3] + 3\alpha[4]) = -\alpha[1] + 3\alpha[2] - 4\alpha[3] + 2\alpha[4] \mod 5$$

i=2
$x = 1$, $y_1 = 0$, $y_2 = 0$, $x_1 = 0$, $x_2 = 0$, $x = 1$, $m = 1$
For $j = 1$ and $j = 2$,

y_1	y_2	x	x_1	x_2	m
-α[1]	-α[3]	$6 = 1 \mod 5$	-α[1]	-α[3]	$-6 = -1 \mod 5$
-α[1]-α[2]	-α[3]-α[4]	1	-α[1]+α[2]	-α[3] +α[4]	1

$$\beta[3] = -\alpha[1] - \alpha[2] - \alpha[3] - \alpha[4]$$
$$\beta[5] = -\alpha[1] + \alpha[2] - \alpha[3] + \alpha[4] \quad (4.2)$$

There fore we obtain :

$$\begin{pmatrix} \beta[1] \\ \beta[2] \\ \beta[3] \\ \beta[4] \\ \beta[5] \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 0 & 1 \\ -1 & -3 & -4 & -2 & 0 \\ -1 & -1 & -1 & -1 & 0 \\ -1 & -4 & -1 & -4 & 0 \\ -1 & -2 & -4 & -3 & 0 \end{pmatrix} \begin{pmatrix} \alpha[1] \\ \alpha[2] \\ \alpha[3] \\ \alpha[4] \\ \alpha[5] \end{pmatrix}$$

This transition matrix of our example corresponds to that of Theorem 4.6 when $n = 3$ and $p = 5$

We provide another example with $p = 7$ and $n = 2$ in order to verify the algorithm.

Example 4.4. Let $q = 7^2$ with $n = 2$ and $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ be the polynomial basis of the finite field $\mathbb{F}_q(\alpha)$ where α is the root of the irreducible polynomial $x^7 - x + 1 \in \mathbb{F}_p[x]$. We shall perform Algorithm 1 steps by steps in order to obtain the Normal basis $\{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \beta^{q^4}, \beta^{q^5}, \beta^{q^6}\}$ where $\beta = \alpha^{-1}$

$q = 7^2$, $n = 2$, $z = 3$
$b[1] = (\alpha[7] - \alpha[1]) \mod 5$
<u>i=1</u>
$x = 1$, $y_1 = 0$, $y_2 = 0$, $x_1 = 0$, $x_2 = 0$, $x = 1$, $m = 1$
For $j = 1$, $j = 2$ and $j = 3$

y_1	y_2	x	x_1	x_2	m
-α[1]	-α[4]	2	-α[1]	-α[4]	-2
-α[1]-2α[2]	-α[4]-2α[5]	4	-α[1]+2α[2]	-α[4]+2α[5]	4
-α[1]-2α[2]-4α[3]	-α[4]-2α[5]-4α[6]	1	-α[1]+2α[2]-4α[3]	-α[4]+2α[5]-4α[6]	-1

$$\beta[2] = -\alpha[1] - 2\alpha[2] - 4\alpha[3] - \alpha[4] - 2\alpha[5] - 4\alpha[6]$$
$$\beta[7] = -\alpha[1] + 2\alpha[2] - 4\alpha[3] + \alpha[4] - 2\alpha[5] + 4\alpha[6]$$

<u>i=2</u>
$x = 1$, $y_1 = 0$, $y_2 = 0$, $x_1 = 0$, $x_2 = 0$, $x = 1$, $m = 1$
For $j = 1$, $j = 2$ and $j = 3$

y_1	y_2	x	x_1	x_2	m
-α[1]	-α[4]	4	-α[1]	- α[4]	-4
-α[1]-4α[2]	-α[4]-4α[5]	2	-α[1]+4α[2]	-α[4]+4α[5]	2
-α[1]-4α[2]-2α[3]	-α[4]-4α[5]-2α[6]	1	-α[1]+4α[2]-2α[3]	-α[4]+4α[5]-2α[6]	-8

$$\beta[3] = -\alpha[1] - 4\alpha[2] - 2\alpha[3] - \alpha[4] - 4\alpha[5] - 2\alpha[6]$$
$$\beta[6] = -\alpha[1] + 4\alpha[2] - 2\alpha[3] + \alpha[4] - 4\alpha[5] + 2\alpha[6]$$

<u>i=3</u>
$x = 1$, $y_1 = 0$, $y_2 = 0$, $x_1 = 0$, $x_2 = 0$, $x = 1$, $m = 1$
For $j = 1$, $j = 2$ and $j = 3$

y_1	y_2	x	x_1	x_2	m
-α[1]	-α[4]	6	-α[1]	-α[4]	-6
-α[1]-6α[2]	-α[4]-6α[5]	1	-α[1] +6α[2]	-α[4]+6α[5]	1
-α[1]-6α[2]-α[3]	-α[4]-6α[5]-α[6]	6	-α[1] +6α[2]-α[3]	-α[4]+6α[5]-α[6]	-6

$$\begin{aligned}\beta[4] &= -\alpha[1] - 6\alpha[2] - \alpha[3] - 6\alpha[4] - 36\alpha[5] - 6\alpha[6] \mod 7 \\ &= -\alpha[1] - 6\alpha[2] - \alpha[3] - 6\alpha[4] - \alpha[5] - 6\alpha[6]\end{aligned}$$

$$\begin{aligned}\beta[5] &= -\alpha[1] + 6\alpha[2] - \alpha[3] + 6\alpha[4] - 36\alpha[5] + 6\alpha[6] \mod 7 \\ &= -\alpha[1] + 6\alpha[2] - \alpha[3] + 6\alpha[4] - \alpha[5] + 6\alpha[6]\end{aligned}$$

There fore we obtain :

$$\begin{pmatrix}\beta[1]\\ \beta[2]\\ \beta[3]\\ \beta[4]\\ \beta[5]\\ \beta[6]\\ \beta[7]\end{pmatrix} = \begin{pmatrix}-1 & 0 & 0 & 0 & 0 & 0 & 1\\ -1 & -2 & -4 & -1 & -2 & -4 & 0\\ -1 & -4 & -2 & -1 & -4 & -2 & 0\\ -1 & -6 & -1 & -6 & -1 & -6 & 0\\ -1 & -1 & -1 & -1 & -1 & -1 & 0\\ -1 & -3 & -2 & -6 & -4 & -5 & 0\\ -1 & -4 & -4 & -6 & -2 & -3 & 0\end{pmatrix} \begin{pmatrix}\alpha[1]\\ \alpha[2]\\ \alpha[3]\\ \alpha[4]\\ \alpha[5]\\ \alpha[6]\\ \alpha[7]\end{pmatrix}$$

This Transition Matrix corresponds to that of Theorem 4.6 when $n = 2$ and $p = 7$.

Now we provide the algorithm to compute the polynomial basis from the Normal Basis.

Algorithm 2 Normal Basis to Polynomial Basis

Input: $(\bar{\beta} = \{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{p-1}}\}, n)$
Output: $\bar{\alpha} = \{\alpha^{p-1}, \alpha^{p-2}, \ldots, \alpha, 1\}$

1: $z = \frac{p-1}{2}$
2: $\alpha[p] = \beta[p]$
3: **for** i =1 **to** z **do**
4: $\quad \alpha[p] = (\alpha[p] + \beta[i] + \beta[p-i]) \mod p$
5: $\quad x = 1, m = 1, y = 0$
6: $\quad$ **for** j=1 **to** p-1 **do**
7: $\quad\quad x = x * (n * i) \mod p$
8: $\quad\quad m = m * n * (-i) \mod p$
9: $\quad\quad y = \alpha[p-j]$
10: $\quad\quad \alpha[p-j] = (y + m * \beta[p-i+1] + x * \beta[i+1]) \mod p$
11: $\quad$ **end for**
12: **end for**
13: Output = $\bar{\alpha}$

Now we provide an example to show how the Algorithm from Normal Basis to Polynomial Basis works.

Example 4.5. Let $q = 5^3$. The set $\{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \beta^{q^4}\}$ is the Normal basis of the finite field $\mathbb{F}_q[x]/ < x^5 - x^4 + 1 >$, where β is the root of $x^5 - x^4 + 1 \in \mathbb{F}_p[x]$. We perform the above Algorithm 2 step by steps in order to obtain $\{\alpha^4, \alpha^3, \alpha^2, \alpha, 1\}$ where $\beta = \alpha^{-1}$
For i = 1 to 2 do : $\alpha[5] = (\alpha[5] + \beta[1] + \beta[4]) \mod p$
$x = 1$, $m = 1$, $y = 0$
$\underline{i = 1}$
For j=1 to 4
<u>i=2</u>
α[5]=α[5] + β[2]+β[3]
$x = 1$, $m = 1$, $y = 0$.

j	x	m	y	$a[p-j]$
j =1	$3 \mod 5$	$-3 \mod 5$	α[4]	α[4]=α[4]-3β[5]+3β[2]
j=2	$4 = 9 \mod 5$	$4 = 9 \mod 5$	α[3]	α[3]=α[3]+4β[5]+4β[2]
j=3	$2 = 12 \mod 5$	$-2 = 12 \mod 5$	α[2]	α[2]=α[2]-2β[5]+2β[2]
j=4	$1 = 6 \mod 5$	$1 = 6 \mod 5$	α[1]	α[1]=α[1]+β[5]+β[2]

j	x	m	y	α[p-j]
j=1	-1	-1	α[4]	α[4]=α[4]-β[4]+β[3]
j=2	1	1	α[3]	α[3]=α[3]+β[4]+β[3]
j=3	1	-1	α[2]	α[2]= α[2]-β[4]+β[3]
j=4	1	1	α[1]	α[1]=α[1] + β[4]+β[3]

Therefore we have the following :

$$\begin{aligned}
\alpha[1] &= \alpha[1] + \beta[4] + \beta[3] \\
&= \alpha[1] + \beta[2] + \beta[3] + \beta[4] + \beta[5] \\
\alpha[2] &= \alpha[2] - \beta[4] + \beta[3] \\
&= \alpha[2] + 2\beta[2] + \beta[3] - \beta[4] - 2\beta[5] \\
\alpha[3] &= \alpha[3] + \beta[4] + \beta[3] \\
&= \alpha[3] + 4\beta[2] + \beta[3] + \beta[4] + 4\beta[5] \\
\alpha[4] &= \alpha[4] - \beta[4] + \beta[3] \\
&= \alpha[4] + 3\beta[2] + \beta[3] - \beta[4] - 3\beta[5] \\
\alpha[5] &= \alpha[5] + \beta[1] + \beta[2] + \beta[3] + \beta[4] \\
&= \beta[1] + \beta[2] + \beta[3] + \beta[4] + \beta[5]
\end{aligned}$$

Setting $\alpha[i] = 0$ for $1 \leq i \leq p-1$, We obtain

$$\begin{pmatrix} \alpha[1] \\ \alpha[2] \\ \alpha[3] \\ \alpha[4] \\ \alpha[5] \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & -1 & -2 \\ 0 & 4 & 1 & 1 & 4 \\ 0 & 3 & 1 & -1 & -3 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \beta[1] \\ \beta[2] \\ \beta[3] \\ \beta[4] \\ \beta[5] \end{pmatrix}$$

The transition Matrix from polynomial to normal basis when $n = 3$ and $p = 5$ is

$$M = \begin{pmatrix} -1 & 0 & 0 & 0 & 1 \\ -1 & -3 & -4 & -2 & 0 \\ -1 & -1 & -1 & -1 & 0 \\ -1 & -4 & -1 & -4 & 0 \\ -1 & -2 & -4 & -3 & 0 \end{pmatrix}$$

We now verify whether transition matrix from normal basis to polynomial basis is the

coefficient matrix produced from our algorithm.

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & -1 & -2 \\ 0 & 4 & 1 & 1 & 4 \\ 0 & 3 & 1 & -1 & -3 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 & 0 & 1 \\ -1 & -3 & -4 & -2 & 0 \\ -1 & -1 & -1 & -1 & 0 \\ -1 & -4 & -1 & -4 & 0 \\ -1 & -2 & -4 & -3 & 0 \end{pmatrix} = \begin{pmatrix} -4 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -34 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We conclude that our algorithm works.

Example 4.6. Let $q = 7^2$. The set $\{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \beta^{q^4}, \beta^{q^5}, \beta^{q^6}\}$ is the Normal basis of the finite field $\mathbb{F}_q[x]/ < x^7 - x^6 + 1 >$, where β is the root of $x^7 - x^6 + 1 \in \mathbb{F}_p[x]$. We perform the above Algorithm 2 step by steps in order to obtain $\{\alpha^6, \alpha^5, \alpha^4, \alpha^3, \alpha^2, \alpha, 1\}$ where $\beta = \alpha^{-1}$
For i = 1 to 3 do : $\alpha[7] = (\alpha[7] + \beta[1] + \beta[6]) \mod 7$
$x = 1, m = 1, y = 0$
$\underline{i = 1}$
For j=1 to 6

j	x	m	y	α[p-j]
$j = 1$	2	-2	$y = \alpha[6]$	$\alpha[6]=\alpha[6]-2\beta[7]+2\beta[2]$
$j = 2$	4	4	$y = \alpha[5]$	$\alpha[5] = \alpha[5] + 4\beta[7] + 4\beta[2]$
$j = 3$	1	-1	$y = \alpha[4]$	$\alpha[4] = \alpha[4] - \beta[7] + \beta[2]$
$j = 4$	2	2	$y = \alpha[3]$	$\alpha[3] = \alpha[3] + 2\beta[7] + 2\beta[2]$
$j = 5$	4	-4	$y = \alpha[2]$	$\alpha[2] = \alpha[2] - 4\beta[7] + 4\beta[2]$
$j = 6$	1	1	$y = \alpha[1]$	$\alpha[1] = \alpha[1] + \beta[7] + \beta[2]$

$\underline{\text{i=2}}$
$\alpha[7] = \alpha[7] + \beta[2] + \beta[5]$
$x = 1, m = 1, y = 0$

j	x	m	y	$\alpha[p-j]$
$j = 1$	4	-4	$\alpha[6]$	$\alpha[6] = \alpha[6] - 4\beta[6] + 4\beta[3]$
$j = 2$	$16 = 2 \mod 7$	2	$\alpha[5]$	$\alpha[5] = \alpha[5] + 2\beta[6] + 2\beta[3]$
$j = 3$	1	-1	$\alpha[4]$	$\alpha[4] = \alpha[4] - \beta[6] + \beta[3]$
$j = 4$	4	4	$\alpha[3]$	$\alpha[3] = \alpha[3] + 4\beta[6] + 4\beta[3]$
$j = 5$	2	-2	$\alpha[2]$	$\alpha[2] =\alpha[2] - 2\beta[6] + 2\beta[3]$
$j = 6$	1	1	$\alpha[1]$	$\alpha[1] =\alpha[1] + \beta[6] + \beta[3]$

$\underline{\text{i=3}}$
$\alpha[7] = \alpha[7] + \beta[3] + \beta[4]$
$x = 1, m = 1, y = 0$

j	x	m	y	$\alpha[p-j]$
$j=1$	6	-6	$\alpha[6]$	$\alpha[6]=\alpha[6]-6\beta[5]+6\beta[4]$
$j=2$	1	1	$\alpha[5]$	$\alpha[5]=\alpha[5]+\beta[5]+\beta[4]$
$j=3$	6	-6	$\alpha[4]$	$\alpha[4]=\alpha[4]-6\beta[5]+6\beta[4]$
$j=4$	1	1	$\alpha[3]$	$\alpha[3]=\alpha[3]+\beta[5]+\beta[4]$
$j=5$	6	-6	$\alpha[2]$	$\alpha[2]=\alpha[2]-6\beta[5]+6\beta[4]$
$j=6$	1	1	$\alpha[1]$	$\alpha[1]=\alpha[1]+\beta[5]+\beta[4]$

Therefore we have the following :

$$
\begin{aligned}
\alpha[1] &= \alpha[1]+\beta[5]+\beta[4] \\
&= \alpha[1]+\beta[6]+\beta[3]+\beta[4]+\beta[5] \\
&= \alpha[1]+\beta[2]+\beta[3]+\beta[4]+\beta[5]+\beta[6]+\beta[7] \\
\alpha[2] &= \alpha[2]-6\beta[5]+6\beta[4] \\
&= \alpha[2]-2\beta[6]+2\beta[3]-6\beta[5]+6\beta[4] \\
&= \alpha[2]-2\beta[6]+2\beta[3]-6\beta[5]+6\beta[4]-4\beta[7]+4\beta[2] \\
\alpha[3] &= \alpha[3]+\beta[5]+\beta[4] \\
&= \alpha[3]+4\beta[6]+4\beta[3]+\beta[4]+\beta[5] \\
&= \alpha[3]+2\beta[2]+4\beta[3]+\beta[4]+\beta[5]+4\beta[6]+2\beta[7] \\
\alpha[4] &= \alpha[4]-6\beta[5]+6\beta[4] \\
&= \alpha[4]-\beta[6]+\beta[3]-6\beta[5]+6\beta[4]-\beta[7]+\beta[2] \\
&= \alpha[4]+\beta[2]+\beta[3]+6\beta[4]-6\beta[5]-\beta[6]-\beta[7] \\
\alpha[5] &= \alpha[5]+\beta[3]+\beta[4] \\
&= \alpha[5]+\beta[3]+\beta[4]+2\beta[6]+2\beta[3] \\
&= \alpha[5]+4\beta[2]+2\beta[3]+\beta[4]+\alpha[5]+2\beta[6]+4\beta[7] \\
\alpha[6] &= \alpha[7]-6\beta[5]+6\beta[4] \\
&= \alpha[7]-4\beta[6]+4\beta[3]-6\beta[5]+6\beta[4] \\
&= \alpha[7]+2\beta[2]+4\beta[3]+6\beta[4]-6\beta[5]-4\beta[6]-2\beta[7] \\
\alpha[7] &= \alpha[7]+\beta[3]+\beta[4] \\
&= \alpha[7]\beta[2]+\beta[3]+\beta[4]+\beta[5] \\
&= \beta[1]+\beta[3]+\beta[4]+\beta[5]+\beta[6]+\beta[7]
\end{aligned}
$$

Setting $\alpha[i]=0$ for $1 \le i \le p-1$, we obtain

$$
\begin{pmatrix} \alpha[1] \\ \alpha[2] \\ \alpha[3] \\ \alpha[4] \\ \alpha[5] \\ \alpha[6] \\ \alpha[7] \end{pmatrix}
=
\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 4 & 2 & 6 & -6 & -2 & -4 \\
0 & 2 & 4 & 1 & 1 & 4 & 2 \\
0 & 1 & 1 & 6 & -6 & -1 & -1 \\
0 & 4 & 2 & 1 & 1 & 2 & 4 \\
0 & 2 & 4 & 6 & -6 & -4 & -2 \\
1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
\begin{pmatrix} \beta[1] \\ \beta[2] \\ \beta[3] \\ \beta[4] \\ \beta[5] \\ \beta[6] \\ \beta[7] \end{pmatrix}
$$

The transition matrix from polynomial to normal basis when $n = 2$ and $p = 7$ is

$$M = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & -2 & -4 & -1 & -2 & -4 & 0 \\ -1 & -4 & -2 & -1 & -4 & -2 & 0 \\ -1 & -6 & -1 & -6 & -1 & -6 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & 0 \\ -1 & -3 & -2 & -6 & -4 & -5 & 0 \\ -1 & -5 & -4 & -6 & -2 & -3 & 0 \end{pmatrix}$$

We now verify whether transition matrix from normal basis to polynomial basis is the coefficient matrix produced from our algorithm.

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & -2 & -4 & -1 & -2 & -4 & 0 \\ -1 & -4 & -2 & -1 & -4 & -2 & 0 \\ -1 & -6 & -1 & -6 & -1 & -6 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & 0 \\ -1 & -3 & -2 & -6 & -4 & -5 & 0 \\ -1 & -5 & -4 & -6 & -2 & -3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 4 & 2 & 6 & -6 & -2 & -4 \\ 0 & 2 & 4 & 1 & 1 & 4 & 2 \\ 0 & 1 & 1 & 6 & -6 & -1 & -1 \\ 0 & 4 & 2 & 1 & 1 & 2 & 4 \\ 0 & 2 & 4 & 6 & -6 & -4 & -2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We conclude that our algorithm works.

4.3 Complexity of the Algorithm

Let M denote Multiplication in Prime field $\mathbb{F}_p$ and let A denote addition in prime field $\mathbb{F}_p$ also let $\alpha \in \mathbb{F}_{q^p}$ where $q = p^n$ and $\{\alpha_1, \alpha_2, \ldots, \alpha_p\}$ be a basis of $\mathbb{F}_{q^p}$. Then $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_p\alpha_p$ for $a_i \in \mathbb{F}_q$ for $i \in \{1, 2, \ldots, p\}$. Let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_q$. Then for each i, $a_i = b_{0,i}\beta_1 + b_{1,i}\beta_2 + \cdots + b_{n-1,i}\beta_n$ where $b_{j,i} \in \mathbb{F}_p$ for $j \in \{0, \ldots, n-1\}$ and $i \in \{1, \ldots, p\}$. Therefore, the number of prime field multiplication for each a_i is n and the number of prime field multiplication is npM.
Similarly the number of addition for each a_i is n and the number of additions to represent $\alpha \in \mathbb{F}_{q^p}$ is np. Therefore the number of operation for one round is $(4np + 4)M$ and $4npA$. Since we have $(\frac{p-1}{2})(\frac{p-1}{2})$ rounds in our algorithm, the estimated cost of the algorithm is:

$$4pnA(\frac{p-1}{2})^2 + (4pn + 4)M(\frac{p-1}{2})^2 = O(p^3nA + p^3nM).$$

Our two algorithms have the same complexity.

4.3.1 Comparaison of the Previous Results with ours

Since there are some algorithms in the literature for conversion between polynomial basis to normal basis and vice versa over some field extensions, we compare our result to these suggestions in the table below.

Table 4.1: Cost for Conversion in Extension field

Algorithm	Burton[2]	Riaz[16]	Our Method
Storage Complexity	$O(m)$	O(1)	O(1)
Field Operations	$O(mr \log p)$	$O(p^2)$	$O(p^3n)$

CHAPTER 5

Conclusion

In this thesis we provided conditions for irreducible polynomials to be normal polynomial in $\mathbb{F}_{q^p}$. Furthermore, we used the irreducible polynomial $x^p - x + 1 \in \mathbb{F}_p[x]$ over $\mathbb{F}_q$ where $q = p^n$ and p is an odd prime with $\gcd(p, n) = 1$ to construct the polynomial basis of $\mathbb{F}_{q^p}$. We realised that the polynomial $x^p - x + 1 \in \mathbb{F}_p[x]$ is not normal in $\mathbb{F}_{q^p}$. So in order to construct normal basis of $\mathbb{F}_{q^p}$, we used the reciprocal polynomial $x^p - x^{p-1} + 1 \in \mathbb{F}_p[x]$ which is also irreducible over $\mathbb{F}_q$ and is a normal polynomial in $\mathbb{F}_{q^p}$. We then constructed two algorithms to convert from polynomial basis to normal basis and vice versa. These two algorithms have the same time complexity and require no extra memory.

5.1 Future Work

- We shall extend this technique to convert Polynomial basis or Normal basis to optimal Normal basis for particular extension fields and later compare the complexity with the existing methods.
- Instead of using normal element in $\mathbb{F}_{q^p}$, we will try to use a completely normal element and then try to perform the conversion from normal basis to polynomial basis.

REFERENCES

[1] Akleylek Sedat, *On the representation of Finite Fields*, Phd Thesis, Middle East Technical University, 2010.

[2] Burton S.kaliski Jr., Yiqun Lisa Yin, *Storage Efficient finite fields Basis Conversion*, SAC '98 Proceedings of the Selected Areas in Cryptography, Pages $81-93$ Springer-Verlag London, UK 1999.

[3] Chealsea Richards, *Algorithms for squaring square free polynomials over finite fields*, August 7, 2009.

[4] Chih-Hua Chien, Trieu-Kien Truong, Yaotsu Chang and Chih- Hsuan Chen, *A Fast Algorithm to Determine Normal polynomial over Finite Fields*, International MultiConference of Engineers and Computer Scientists; 2007, p1341.

[5] David S. Dummit and Richard M.Foote *Abstract Algebra 3rd Edition*.

[6] Din Y. Pei, Charles C. Wang and Jimk. Omura, Normal Basis of Finite Field of $GF(2^n)$, IEEE Transactions on Information Theory Impact Factor: 2.62.01/1986;32: 285-287

[7] Dirk Hachenberger, *Finite Fields, Normal Bases and Completely Free Element*, The Springer International Series in Engineering and Computer Science, Vol. 390, 1997.

[8] *G.Eisentein, Galoissche Theorie und Darstellungstheorie, Math.Ann.* $107(1993), 140-144$

[9] Harald Niederreiter and Rudolf Lidl, Introduction to Finite fields and its applications, Cambridge University Press, 1986.

[10] Hoffman and Kunze, *Linear Algebra*, Second Edition.

[11] Joachim Von Zur Gathen, *Irreducible Trinomials over finite fields*, Journal of Symbolic Computation archive Volume 29 Issue 6, June 2000 Pages, $879-889$.

[12] K.Hensel, *Über die Darstellung der Zahlen eines Gattungsbereiches für einen Primdivisor*, J. Reine Angew. Math., $103(1888)$, pp. $230^{\smile}237$.

[13] N.A CARELLA, *Topics of Nornmal bases over Finite fields*, http://arxiv.org/abs/1304.0420.

[14] Ömer Eğecioğlu and Çetin Kaya Koç, *Reducing Complexity of Normal Basis Multiplication*, Department of Computer Science University of California Santa Barbara, https://eprint.iacr.org/$2014/687$.pdf.

[15] Perlis S, *Normal bases of cyclic fields of prime power*, Duke Mathematical Journal $9(1942)$, no. $3, 507 - 517$.

[16] Sial Muhammmed Riaz, *FGPA based Cryptography Computation and Basis Coversion in Composite finite fields*, Phd Thesis, Middle East Technical University, 2013.

[17] Shushong Gao, *Normal Bases over Finite Fields*, PhD thesis, University of Waterloo, 1993.

[18] Sunil K. Chebou, *Counting irreducible polynomials over Finite fields*, 2011. using the inclusion and exclusion principle.

[19] Stefan Schwarz, *Irreducible Polynomials over Finite Fields with Linearly Independent roots*, Mathematica Slovaca $38.2(1988)$: $147 - 158$.