Spring 5-9-2015

Frobenius-Like Permutations and Their Cycle Structure

Adil B. Virani

FROBENIUS-LIKE PERMUTATIONS AND THEIR CYCLE STRUCTURE

by

ADIL VIRANI

Under the Direction of Florian Enescu, PhD

ABSTRACT

Polynomial functions over finite fields are a major tool in computer science and electrical engineering and have a long history. Some of its aspects, like interpolation and permutation polynomials are described in this thesis. A complete characterization of subfield compatible polynomials ($f \in E[x]$ such that $f(K) \subseteq L$ where K, L are subfields of E) was recently given by J. Hull. In his work, he introduced the Frobenius permutation which played an important role. In this thesis, we fully describe the cycle structure of the Frobenius permutation. We generalize it to a permutation called a monomial permutation and describe its cycle factorization. We also derive some important congruences from number theory as corollaries to our work.

INDEX WORDS: Finite fields, subfield compatible polynomials, Frobenius permutation, permutation polynomials, shift permutation, monomial permutation

FROBENIUS-LIKE PERMUTATIONS AND THEIR CYCLE STRUCTURE

by

ADIL VIRANI

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science

in the College of Arts and Sciences

Georgia State University

2015

FROBENIUS-LIKE PERMUTATIONS AND THEIR CYCLE STRUCTURE

by

ADIL VIRANI

Committee Chair: Florian Enescu

Committee: Yongwei Yao

Zhongshan Li

Electronic Version Approved:

Office of Graduate Studies

College of Arts and Sciences

Georgia State University

May 2015

DEDICATION

This thesis is dedicated to

My Advisor

Thank you for your support.

ACKNOWLEDGMENTS

I would like to thank everyone who helped me in the process of creating this thesis. I am grateful beyond expression for my advisor, Dr. Florian Enescu, for his careful and patient instruction. I would also like to thank my committee members, Drs. Yongwei Yao and Zhongshan Li, for their comments and suggestions in the editing process.

In addition I would like to thank the NSF for the support by the mean of grant CCF-1320385.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

In this chapter, we will develop the basic theory of finite fields and basic number theory. We will discuss basic definitions and theorems, most of them without proof. Most of the results in this chapter can be found in [2], [3], [5].

1.1 Finite fields

Definition 1.1.1. A *field* is a set $\mathbb{F}$ along with two operations, addition $(+)$ and multiplication $(\cdot)$, satisfying:

- $(\mathbb{F}, +)$ is an abelian group with identity element 0
- $(\mathbb{F}^\times, \cdot)$ is an abelian group with identity element 1 where $\mathbb{F}^\times = F - \{0\}$
- $\forall\, a, b, c \in \mathbb{F}$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

A *field* with finitely many elements is called a *finite field*.

Example 1.1.2. $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ is a finite field with p elements.

Definition 1.1.3. A field containing no proper subfields is called a *prime field*. Intersection of all the subfields of a field $\mathbb{F}$ is called the *prime field* of $\mathbb{F}$.

Definition 1.1.4. The *characteristic* of a field $\mathbb{F}$ is defined to be the smallest positive integer p such that $p \cdot 1_{\mathbb{F}} = 0$ if such p exists and is defined to be 0 otherwise.

Theorem 1.1.5. *Let $\mathbb{F}$ be a finite field. Then,*

(i) *The characteristic of* $\mathbb{F}$ *is a prime number* p *and the prime field of* $\mathbb{F}$ *is* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(ii) *The number of elements of* $\mathbb{F}$ *is* p^n *for prime* p *and some positive integer* n.

We will denote a finite field of characteristic p and cardinality p^n as $\mathbb{F}_{p^n}$, $\mathbb{F}_p$ will denote the *prime field* of $\mathbb{F}_{p^n}$. The *algebraic closure* of $\mathbb{F}_p$ is $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$ and will be denoted as $\overline{\mathbb{F}_p}$.

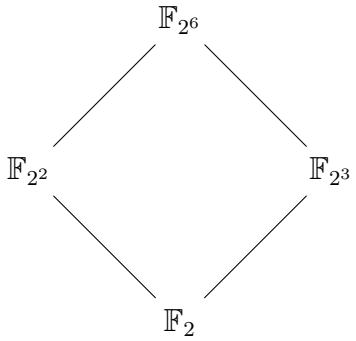
Definition 1.1.6. Let F be a finite field. If $f \in F[x]$ splits completely into linear factors in E, *i.e* $f(x) = (x - a_1)\cdots(x - a_n)$ and $E = F(a_1, \ldots, a_n)$ then E is called the *splitting field* of f over F.

Theorem 1.1.7. *Any finite field* $\mathbb{F}$ *with* p^n *elements is the splitting field of* $x^{p^n} - x \in \mathbb{F}_p[x]$. *Consequently, any two finite fields with* p^n *elements are isomorphic.*

By Theorem 1.1.7 above, the elements of the finite field of cardinality p^n are the p^n distinct roots of the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$. The uniqueness part of the theorem allows us to talk about *the finite field* of order p^n with prime characteristic p, which is denoted as $\mathbb{F}_{p^n}$ here. The next theorem shows that any subfield of $\mathbb{F}_{p^n}$ of order p^m for a positive divisor m of n, is the unique field $\mathbb{F}_{p^m}$ containing precisely the roots of the polynomial $x^{p^m} - x \in \mathbb{F}_p[x]$.

Theorem 1.1.8. *Let* $E = \mathbb{F}_{p^n}$ *be the finite field. Then every subfield of* E *has cardinality* p^m, *where* m *is a positive divisor of* n. *Conversely, if* m *is a positive divisor of* n, *then there is exactly one subfield of* E *with* p^m *elements.*

Example 1.1.9. The subfields of the finite field $\mathbb{F}_{2^6}$ can be given by the following diagram:



Definition 1.1.10. Let G be a group. For any $a \in G$, the *order of* a is the smallest positive integer n such that $a^n = 1$. We will denote order of $a \in G$ by $ord(a)$.

Throughout the paper, for positive integer m and n, the *greatest common divisor* of m and n will be denoted by (m, n) and the *least common multiple* of m and n will be denoted by $[m, n]$.

Proposition 1.1.11. *Let G be an Abelian group and $a, b \in G$. Then*

(i) *If $ord(a) = m$ and $ord(b) = n$, then there exist an element $c \in G$ such that $ord(c) = [m, n]$.*

(ii) *For a positive integer n, if $ord(a) = m$ then $ord(a^n) = \frac{m}{(m,n)}$.*

Theorem 1.1.12. ([2]) The multiplicative group $(\mathbb{F}^\times, \cdot)$ of a finite field $\mathbb{F}$ is cyclic.

Proof. By Proposition 1.1.11, there exist an element $\alpha \in \mathbb{F}^\times$ whose order is k, the *l.c.m.* of orders of all the elements in $\mathbb{F}^\times$. Then $a^k = 1$ for all $a \in \mathbb{F}^\times$. That is, each element of $\mathbb{F}^\times$ is a root of the polynomial $x^k - 1$, which has at most k roots. Hence $|\mathbb{F}^\times| \leq k$. On the other hand, $\{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$ are all distinct and are elements of $\mathbb{F}^\times$. Hence α generates $\mathbb{F}^\times$. □

Definition 1.1.13. Let $\mathbb{F}$ be a finite field. A generator of the multiplicative group $\mathbb{F}^\times$ is called a *primitive element* of $\mathbb{F}$.

Definition 1.1.14. A polynomial $f \in \mathbb{F}[x]$ is *irreducible* if the degree of $f \geq 1$ and if $f = g \cdot h$ for some g, $h \in \mathbb{F}[x]$ then either $g \in \mathbb{F}$ or $h \in \mathbb{F}$. A polynomial f is *monic* if the leading coefficient of f is 1. A monic irreducible polynomial f is called a *primitive polynomial* if the roots of f are primitive elements of $\mathbb{F}$.

Theorem 1.1.15. *Let $\mathbb{F}_q$ be the finite field of order q.*

(i) ([5],Thm 3.25) The number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n is given by $\frac{1}{n} \sum_{d|n, d>0} \mu(d) q^{n/d}$, where μ is the Möebius μ-function.

(ii) ([7],Thm 7.7)The number of primitive polynomials in $\mathbb{F}_q[x]$ of degree n is given by $\frac{\phi(q^n-1)}{n}$, where ϕ is Euler's totient function.

The Euler's totient function and the Mobius μ-function are defined in the next section.

Lemma 1.1.16. *If α is a primitive element of $\mathbb{F}_q$ then α^k is a primitive element of $\mathbb{F}_q$ if and only if (k,q-1)=1.*

Remark 1.1.17. By Lemma 1.1.16, it follows that there are exactly $\phi(q-1)$ primitive elements in $\mathbb{F}_q$ where ϕ is Euler's totient function.

Since primitive elements are the defining elements of the finite field, finding primitive elements in an arbitrary finite field has been extensively studied over the time. In fact, in case of a finite field $\mathbb{F}_p$ with p prime, the primitive elements of $\mathbb{F}_p$ are exactly *primitive roots modulo p*. We have that for a finite field $\mathbb{F}_p[x]/(f(x))$ with $f \in \mathbb{F}_p[x]$ a primitive polynomial, the roots of f are primitive elements of the finite field. Finding a primitive element in arbitrary finite field with an efficient algorithm is still an open problem, in spite of the great density(Remark 1.1.17) of primitive elements.

Definition 1.1.18. Let E be a field. A field K is a simple extension of E if $K = E(\alpha)$ for some $\alpha \in K$.

The next result is Strong Hilbert Nullstellensatz over finite fields which is a very important result in the theory of rings. Before we write Hilbert Nullstellensatz, we need to define some terms.

Definition 1.1.19. Let $\mathbb{F}$ be a field. Take S a set of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Define $\mathcal{Z}(S) = \{x \in \mathbb{F}^n \mid f(x) = 0, \text{ for all } f \in S\}$. $V \subseteq \mathbb{F}[x_1, \ldots, x_n]$ is an *affine algebraic set* if $\exists\, S \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that $V = \mathcal{Z}(S)$.

Definition 1.1.20. Let $V \subseteq \mathbb{F}^n$ and $A = \mathbb{F}[x_1, \ldots, x_n]$ for a field $\mathbb{F}$. The *vanishing ideal* of V is the set $\mathcal{I}(V) = \{f \in A \mid f(x) = 0 \text{ for all } x \in V\}$.

Theorem 1.1.21. [Strong Hilbert-Nullstellensatz over finite fields] [4] Let $\mathbb{F}_q$ be a finite field with $q = p^k$ elements for some prime p and positive integer k. Let $J \leq \mathbb{F}_q[x_1, \ldots, x_n]$. Then

$$\mathcal{I}(\mathcal{Z}(J)) = J + (x_1^q - x_1, \ldots, x_n^q - x_n).$$

Next we will state the Lagrange Interpolation Formula, which will allow us to regard any function over a finite field as a polynomial function over the finite field.

Theorem 1.1.22. [Lagrange Interpolation Formula] ([5], Thm 1.71) For $n \geq 0$, let $a_0, \ldots, a_n$ be $n+1$ elements of F, and let $b_0, \ldots, b_n$ be $n+1$ arbitrary elements of F. Then there exists exactly one polynomial $f \in F[x]$ of degree $\leq n$ such that $f(a_i) = b_i$ for $i = 0, \ldots, n$. This polynomial is given by

$$f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} \frac{x - a_k}{a_i - a_k}.$$

The formula above is an alternative representation of Newton's general interpolation formula. It was first published by Waring in 1779, rediscovered by Euler in 1783 and published by Lagrange in 1795 [8]. Our next proposition gives another way to write an interpolating polynomial for a given function over a finite field.

Proposition 1.1.23. ([5]) Let $\mathbb{F}_q$ be a finite field. Any function $\phi(x) \in \mathbb{F}_q[x]$ can uniquely be represented by a polynomial $f \in \mathbb{F}_q[x]$ of degree $\leq q-1$ in the sense that $f(a) = \phi(a)$ for all $a \in \mathbb{F}_q$. This polynomial is given by

$$f(x) = \sum_{a \in \mathbb{F}_q} \phi(a) \left(1 - (x-a)^{q-1}\right).$$

Definition 1.1.24. Let R be a ring and $X, Y \subseteq R$. Let $g : X \to Y$ be a function. A polynomial $f \in R[x]$ *represents* g *on* X if $f(a) = g(a)$ for all $a \in X$.

Theorem 1.1.25. *Let E be a finite field. Any function $\phi : E \to E$ can be represented by a polynomial $f \in E[x]$ of degree less than $|E|$.*

Proof. Let E be the finite field of order q. Then clearly f as above formula represents ϕ. □

1.2 Basic number theory

Theorem 1.2.1. [The Division Algorithm] Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique

$q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < b.$$

Here q stands for quotient and r stands for remainder. For $a, b \in \mathbb{Z}$ with $b > 0$, we will denote $a \ div \ b$ to be the integer quotient q obtained when a is divided by b.

Theorem 1.2.2. [Fundamental Theorem of Arithmetic] Every integer greater than 1 can be expressed in the form $p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ with $p_1, p_2, \ldots, p_n$ distinct prime numbers and $r_1, r_2, \ldots, r_n$ positive integers. This form is said to be the prime factorization of the integer. This prime factorization is unique except for the arrangement of the $p_i^{r_i}$.

Definition 1.2.3. Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Then a is said to be *congruent to b modulo* m, denoted $a \equiv b \bmod m$, if $m|a - b$.

Theorem 1.2.4. [Fermat's Little Theorem] Let p be a prime number and let $a \in \mathbb{Z}$. Then $a^p \equiv a \bmod p$.

Definition 1.2.5. Let $n \in \mathbb{Z}$ with $n > 0$. The *Euler's totient function*, denoted $\phi(n)$, is the number of positive integers less than or equal to n that are relatively prime to n.

Theorem 1.2.6. [Euler's Theorem] Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \bmod m$.

Definition 1.2.7. Let $n \in \mathbb{Z}$ with $n > 0$. The Möbius μ-function, denoted as $\mu(n)$, is

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{if } p^2|n \text{ with } p \text{ prime} \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ with } p_1, p_2, \ldots, p_r \text{ distinct prime numbers.} \end{cases}$$

Proposition 1.2.8. ([3]) Let $n \in \mathbb{Z}$ with $n > 0$. Then

$$\sum_{d|n, d>0} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Definition 1.2.9. Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. The *multiplicative order of a modulo m* is the smallest positive integer t for which $a^t \equiv 1 \bmod m$. We denote the multiplicative order of a modulo m as $ord_m(a)$.

Proposition 1.2.10. *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^n \equiv 1$ mod m for some positive integer n if and only if $ord_m(a)|n$. In particular, $ord_m(a)|\phi(m)$.*

Definition 1.2.11. Let $r, m \in \mathbb{Z}$ with $m > 0$ and $(r, m) = 1$. Then r is said to be a *primitive root modulo m* if $ord_m(r) = \phi(m)$.

Theorem 1.2.12. [Primitive Root Theorem] [3] Let n be a positive integer. Then a primitive root modulo n exists if and only if n is equal to $1, 2, 4, p^m,$ or $2p^m$ where p is an odd prime number and m is a positive integer.

Theorem 1.2.13. [The Inclusion-Exclusion Principle] Let $A_1, A_2, \ldots, A_n$ be n finite subsets of the set X. Then

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} A_i\right|$$

Chapter 2

SUBFIELD COMPATIBLE POLYNOMIALS

The goal of this chapter is to discuss the subfield compatibility property of a polynomial function over a finite field and characterize subfield compatible polynomials completely following the work of J. Hull. In section 2, we will introduce the Frobenius permutation which was first defined by J. Hull in his paper [1]. In the last section, we will discuss the basic facts about the permutation polynomials over finite field.

2.1 Compatibility property of a function

Let E be a finite field. Denote $E[x]$ to be the ring of polynomials with coefficients in E. Let K and L be subfields of E.

Definition 2.1.1. Let $g : E \to E$ be a function. We say g is K *to* L *compatible* if $g(K) \subseteq L$. That is, $g(a) \in L,$ for all $a \in K$.

Consider a function $g : K \to L$. Every extension of g to E will be K to L compatible. For example, consider $g' : E \to E$ defined as $g'(a) = g(a)$ if $a \in K$ and $g'(a) = 0$ otherwise. Then g' equals g on K. By Theorem 1.1.22, we can construct a polynomial $f \in E[x]$ which represents g' and hence represents g on K. Then $f \in E[x]$ is a K to L compatible polynomial that represents g on K. That is, we can construct a K to L compatible polynomial for a given function from K to L, but this is not unique as there are numerous ways to extend the function.

A natural question to ask is, the polynomial we just constructed, is it special? In other words, what does this subfield compatible polynomial look like? The other way to ask the

question is considering the converse problem. Given a polynomial over larger field, when and under what conditions the polynomial will be compatible over given subfields. This question was considered and answered by J. Hull in his paper [1]. We will reproduce the characterization of subfield compatible polynomials given by J. Hull following his work.

We will first introduce the notion of a *minimal representation of a polynomial*. We will show that the subfield compatibility property of a polynomial depends solely on the form of its minimal representation.

2.2 Minimal representation of a polynomial

Let $\mathbb{F}_p$ be a finite field with p elements and fix $\overline{\mathbb{F}_p}$ an algebraic closure of it. Let $f \in \overline{\mathbb{F}_p}[x]$ be a polynomial. Denote the *degree of* f to be *deg* (f). Consider the finite fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$. In what follows next, the finite field $\mathbb{F}_{p^n}$, respectively $\mathbb{F}_{p^m}$, will be thought of as the splitting field of the polynomial $x^{p^n} - x$, respectively $x^{p^m} - x$, over $\mathbb{F}_p$. These splitting fields lie naturally inside $\overline{\mathbb{F}_p}$.

If f is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible, we have $f(a) \in \mathbb{F}_{p^m}, \forall a \in \mathbb{F}_{p^n}$. If the polynomial f has monomials of the form x^k with k greater or equal to p^n, then we can write $x^k = x^{p^n} \cdot x^{k-p^n}$. By using that the elements of $\mathbb{F}_{p^n}$ are the roots of the polynomial $x^{p^n} - x$ we can substitute x^{p^n} by x in the expression of f until we obtain a different polynomial representation of the function defined by f that now has degree strictly less than p^n.

In other words, if we divide f to $x^{p^n} - x$, there exists $g \in \overline{\mathbb{F}_p}[x]$ of degree less than p^n such that $f - g$ is divisble by $x^{p^n} - x$. Therefore, $f(a) = g(a)$ for all $a \in \mathbb{F}_{p^n}$ and g has now degree less than p^n.

This leads to the following natural definition.

Definition 2.2.1. Let $f \in \overline{\mathbb{F}_p}[x]$ be a polynomial. We say $f_r \in \overline{\mathbb{F}_p}[x]$ is the *minimal representation of* f *with respect to* $\mathbb{F}_{p^n}$ if $0 \leq deg(f_r) < p^n$ and $f(x) = q(x)(x^{p^n} - x) + f_r(x)$ for some $q(x) \in \overline{\mathbb{F}_p}[x]$. If $f = f_r$, we say that f is *minimally represented with respect to* $\mathbb{F}_{p^n}$.

Hence a minimally represented polynomial with respect to $\mathbb{F}_{p^n}$ is one that has degree less than p^n.

Note that minimal representation of a polynomial is uniquely determined as a consequence of the division and remainder theorem for polynomials. Moreover, the following lemma explains that if f is minimally represented with respect to $\mathbb{F}_{p^n}$, then any other polynomial that is minimally represented with respect to $\mathbb{F}_{p^n}$ and agrees with f on all the elements of $\mathbb{F}_{p^n}$ must be f.

Lemma 2.2.2. *Let $f, g \in \overline{\mathbb{F}_p}[x]$ be minimally represented with respect to $\mathbb{F}_{p^n}$. If $g(a) = f(a)$, for all $a \in \mathbb{F}_{p^n}$, then $f = g$.*

Proof. Since f, g are minimally represented with respect to $\mathbb{F}_{p^n}$, $0 \leq deg(f) < p^n$ and $0 \leq deg(g) < p^n$. Then $0 \leq deg(f-g) < p^n$ and we have $g(a) = f(a)$, for all $a \in \mathbb{F}_{p^n}$. Then $(f-g)(a) = 0$, for all $a \in \mathbb{F}_{p^n}$. Hence by Theorem 1.1.21, $f - g = 0$ because $0 \leq deg(f-g) < p^n$. □

Proposition 2.2.3. *Let $f \in \overline{\mathbb{F}_p}[x]$. If f_r is the minimal representation of f with respect to $\mathbb{F}_{p^n}$, then $f(a) = f_r(a)$, for all $a \in \mathbb{F}_{p^n}$.*

Proof. Let f_r be the minimal representation of f with respect to $\mathbb{F}_{p^n}$. Then for some $q(x) \in \overline{\mathbb{F}_p}[x], f(x) = q(x)(x^{p^n} - x) + f_r(x)$ and $deg(f_r) \leq p^n - 1$. Then for all $a \in \mathbb{F}_{p^n}, f(a) = q(a)(a^{p^n} - a) + f_r(a)$. Since $a \in \mathbb{F}_{p^n}$, $a^{p^n} - a = 0$. Hence $f(a) = f_r(a)$. □

Corollary 2.2.4. *Let $f \in \overline{\mathbb{F}_p}[x]$ and let f_r be the minimal representation of f with respect to $\mathbb{F}_{p^n}$. Then f is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible if and only if f_r is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible.*

In the view of Corollary 2.2.4, the subfield compatibility property of a polynomial is preserved in the minimal representation of the polynomial. Hence it is enough to study minimally represented subfield compatible polynomials which in turn represents all the subfield compatible polynomials. In the next section, we will completely characterize the subfield compatible polynomials.

2.3 Compatibility characterization

In the previous section, we have already narrowed down our focus on minimally represented subfield compatible polynomials. So most of the results in this section will deal with minimally represented polynomials.

Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be two finite fields of characteristic $p > 0$ inside $\overline{\mathbb{F}_p}$ an algebraic closure of $\mathbb{F}_p$. The *composite field* of $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ is the smallest field containing both. By Theorem 1.1.8, it is easy to see that the composite field of $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ is $\mathbb{F}_{p^{[m,n]}}$.

Proposition 2.3.1. *Let $f_r \in \overline{\mathbb{F}_p}[x]$ be the minimal representation of $f \in \overline{\mathbb{F}_p}[x]$ with respect to $\mathbb{F}_{p^n}$. Then*

(i) *Each coefficient of f_r is a sum of coefficients of f.*

(ii) *If f is an $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial that is minimally represented with respect to $\mathbb{F}_{p^n}$, then f has coefficients in $\mathbb{F}_{p^{[m,n]}}$.*

Proof. To prove 1, first suppose $deg(f) \geq p^n$, otherwise $f = f_r$ and we have nothing to prove. Now reduce down all the powers of x that are greater than $p^n - 1$ by replacing $x^{p^n} = x$. Call the resulting polynomial g. Then $0 \leq deg(g) < p^n$ and coefficients of g are nothing but sums of coefficients of f. Since $a^{p^n} = a$, for all $a \in \mathbb{F}_{p^n}$, by the construction we have $f(a) = g(a), \forall a \in \mathbb{F}_{p^n}$. Then by Lemma 2.2.2, $f_r = g$ and hence the result.

To prove 2, let f be $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible polynomial that is minimally represented with respect to $\mathbb{F}_{p^n}$. Let $\{a_0, a_1, \ldots, a_{p^n-1}\} = \mathbb{F}_{p^n}$. Also let $f(a_i) = b_i$ for all $0 \leq i \leq p^n - 1$. Note that $b_i \in \mathbb{F}_{p^m}$ for all i. Then by formula in Theorem 1.1.22 consider,

$$g(x) = \sum_{i=0}^{p^n-1} b_i \prod_{\substack{k=0 \\ k \neq i}}^{p^n-1} \frac{x - a_k}{a_i - a_k}.$$

Then $g(a_i) = b_i = f(a_i)$ for all i. Since $deg(g) < p^n$, g is minimally represented with respect to $\mathbb{F}_{p^n}$. So by Lemma 2.2.2, $f = g$. Clearly, the coefficients of g are in $\mathbb{F}_{p^{[m,n]}}$. Hence f has

coefficients in $\mathbb{F}_{p^{[m,n]}}$. □

Proposition 2.3.1 gives a very important, yet not complete, characterization of the subfield compatible polynomials. In order to characterize them completely, we require more tools which we shall introduce first.

Definition 2.3.2. Define *Frobenius Endomorphism* $F : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ such that for $\alpha \in \overline{\mathbb{F}_p}, F(\alpha) = \alpha^p$.

Note that $F|_{\mathbb{F}_{p^n}}$ is an automorphism on $\mathbb{F}_{p^n}$. Moreover, n-th iteration of F is the identity function on $\mathbb{F}_{p^n}$. The Frobenius map can be represented by the polynomial $f \in \overline{\mathbb{F}_p}[x]$, $f(x) = x^p$. In the next section we will discuss the permutation polynomials. The Frobenius map is a permutation monomial, with exponent equals to p.

Definition 2.3.3. (The Frobenius Permutation) Let p be a prime and n be positive integer. Let $S = \{0, 1, \ldots, p^n - 1\}$. Define the function $\phi : S \to S$ so that for $i \in S$, $\phi(i) = q + r$ where $pi = p^n q + r$.

Proposition 2.3.4. *The function ϕ defined above is a permutation of order n on the set S. Moreover, for all $\alpha \in \mathbb{F}_{p^n}$ $F(\alpha^i) = \alpha^{\phi(i)}$ where $i \in S$ and F is the Frobenius endomorphism.*

Proof. We will prove that ϕ is a permutation of order n on the set S in the next chapter, where we will consider more general form of the same function. For the latter part, let α be an element of $\mathbb{F}_{p^n}$. Then for all $i \in S$

$$F(\alpha^i) = (\alpha^i)^p = (\alpha)^{pi} = (\alpha)^{p^n q + r} = (\alpha^{p^n})^q \cdot \alpha^r = (\alpha)^{q+r} = \alpha^{\phi(i)}.$$

□

Proposition 2.3.4 explains the origin of the permutation ϕ and its name *The Frobenius Permutation*. Now consider a polynomial $f \in \overline{\mathbb{F}_p}[x]$ that is minimally represented with respect to $\mathbb{F}_{p^n}$. Since the Frobenius Permutation permutes the elements of the set

$\{0, 1, \ldots, p^n - 1\}$, $f(x) = \sum_{i=0}^{p^n-1} a_i x^i$ can equivalently be written as $f(x) = \sum_{i=0}^{p^n-1} a_{\phi(i)} x^{\phi(i)}$. And similarly $f(x) = \sum_{i=0}^{p^n-1} a_{\phi^m(i)} x^{\phi^m(i)}$ is also equivalent to f for any positive integer m.

Proposition 2.3.5. ([1]) Let $f \in \overline{\mathbb{F}_p}[x]$ be minimally represented with respect to $\mathbb{F}_{p^n}$. If $f(x) = \sum_{i=0}^{p^n-1} a_i x^i$, then for all nonnegative integers k, the minimal representation of the k^{th} power of the Frobenius enodomorphism applied to f is given by the polynomial $f(x) = \sum_{i=0}^{p^n-1} a_i^{p^k} x^{\phi^k(i)}$ where ϕ is the Frobenius permutation of order n.

Proof. We proceed by induction on k. Basis case, $k = 0$, f is minimally represented with respect to $\mathbb{F}_{p^n}$ and there is nothing to show. Assume that the statement is true for $k \geq 0$. Consider the case $k + 1$. Since ϕ is a permutation on the set $\{0, 1, \ldots, p^n - 1\}$, after applying the $(k+1)^{th}$ power of the Frobenius endomorphism on f, the resulting polynomial $g(x) = \sum_{i=0}^{p^n-1} a_i^{p^{k+1}} x^{\phi^{k+1}(i)}$ is of degree strictly less than p^n. Then g is minimally represented with respect to $\mathbb{F}_{p^n}$. To show that g is the minimal representation of $F^{k+1}(f)$ with respect to $\mathbb{F}_{p^n}$, we only need to show function equality on $\mathbb{F}_{p^n}$. By inductive hypothesis, we have $F^k(f)_r = \sum_{i=0}^{p^n-1} a_i^{p^k} x^{\phi^k(i)}$, that is $F^k(f)_r(\alpha) = F^k(f)(\alpha) = \sum_{i=0}^{p^n-1} a_i^{p^k} \alpha^{\phi^k(i)}$ for all $\alpha \in \mathbb{F}_{p^n}$. Then for all $\alpha \in \mathbb{F}_{p^n}$:

$$\begin{aligned}
F^{k+1}(f)(\alpha) &= F(F^k(f)(\alpha)) \\
&= F(\sum_{i=0}^{p^n-1} a_i^{p^k} \alpha^{\phi^k(i)}) \\
&= \sum_{i=0}^{p^n-1} F(a_i^{p^k} \alpha^{\phi^k(i)}) \\
&= \sum_{i=0}^{p^n-1} (a_i^{p^k})^p \alpha^{\phi(\phi^k(i))} \\
&= \sum_{i=0}^{p^n-1} a_i^{p^{k+1}} \alpha^{\phi^{k+1}(i)} \\
&= g(\alpha)
\end{aligned}$$

Hence $F^{k+1}(f)_r(x) = g(x) = \sum_{i=0}^{p^n-1} a_i^{p^{k+1}} x^{\phi^{k+1}(i)}$ by Lemma 2.2.2. Hence by induction, the statement is true for all nonnegative integers k. □

We now have all the required tools to derive the main result of J. Hull. The next theorem provides the necessary and sufficient condition for a polynomial in $\overline{\mathbb{F}_p}[x]$ to be $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible.

Theorem 2.3.6. (Thm 3.8, [1]) Let $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ be two finite fields. Let $f \in \overline{\mathbb{F}_p}[x]$ be minimally represented with respect to $\mathbb{F}_{p^n}$. Then f is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible if and only if $a_i^{p^m} = a_{\phi^k(i)}$ for each $i \in \{0, \ldots, p^n - 1\}$ where ϕ is the Frobenius permutation of order n and $m \equiv k \bmod n$, $0 \leq k < n$.

Proof. Let $f = \sum_{i=0}^{p^n-1} a_i x^i$ be a minimally represented polynomial with respect to $\mathbb{F}_{p^n}$. Then f is $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ compatible if and only if $f(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_{p^m}$ if and only if for all $\alpha \in \mathbb{F}_{p^n}$, $(f(\alpha))^{p^m} = f(\alpha)$ if and only if $F^m(f(\alpha)) = f(\alpha)$ if and only if $F^m(f)_r(\alpha) = f(\alpha)$ if and only if $F^m(f)_r = f$ in $\overline{\mathbb{F}_p}[x]$. By Proposition 2.3.5, $F^m(f)_r = \sum_{i=0}^{p^n-1} a_i^{p^m} x^{\phi^m(i)}$. Then

$$\sum_{i=0}^{p^n-1} a_i^{p^m} x^{\phi^m(i)} = F^m(f)_r(x) = f(x) = \sum_{i=0}^{p^n-1} a_i x^i.$$

It follows that $a_i^{p^m} = a_{\phi^m(i)}$ for each $i \in \{0, \ldots, p^n - 1\}$. Since order of ϕ is n and $m \equiv k \bmod n$, $\phi^m(i) = \phi^k(i)$ for all i and hence the result. □

Theorem 2.3.6 gives complete characterization of the subfield compatible polynomials. From Proposition 2.3.1, we already concluded that the coefficients of minimally represented subfield compatible polynomial are from the composite field. Theorem 2.3.6 further explains how the coefficients are related through the Frobenius permutation.

Example 2.3.7. Consider $p = 2$, $m = 3$, $n = 2$. Let α be the root of the irreducible polynomial $g(x) = x^6 + x^5 + 1 \in \mathbb{F}_2[x]$ so that $\mathbb{F}_{2^6} \cong \mathbb{F}_2[x]/(g(x))$. Here g is in fact a primitive polynomial hence α is a primitive element in $\mathbb{F}_{2^6}$. Refer to Appendix A which lists all the elements of the field in terms of α. Consider the following polynomial

$$f(x) = \alpha^{56}x^6 + \alpha^{54}x^5 + \alpha^{61}x^4 + \alpha^{39}x^3 + \alpha^{58}x^2 + \alpha^{33}x + \alpha^{45}$$

Then by reducing $x^4 = x$ we get the minimal representation of f with respect to $\mathbb{F}_{2^2}$ which is:

$$\sum_{i=0}^{3} a_i x^i = f_r(x) = \alpha^9 x^3 + \alpha^{34} x^2 + \alpha^{20} x + \alpha^{45}$$

Now the Frobenius permutation of order 2 is $\phi_2 = (0)(1\ 2)(3)$. Note that here $k = 1$. Then according to Theorem 2.3.6, we must have, $a_3^8 = a_3$, $a_2^8 = a_1$, $a_1^8 = a_2$ and $a_0^8 = a_0$. Which is satisfied for f_r in our example. Hence f is $\mathbb{F}_{2^2}$ to $\mathbb{F}_{2^3}$ compatible, that is $f(\mathbb{F}_{2^2}) \subseteq \mathbb{F}_{2^3}$.

2.4 Permutation polynomials

Permutation polynomials over a finite field have been studied by a number of mathematicians over the time for its important applications in various fields. We here will discuss few known results and classes of permutation polynomials over a finite field. The Frobenius map belongs to the class of permutation monomials. Most of the results in this section can be found in [5].

Definition 2.4.1. Let $\mathbb{F}_q$ be the finite field of q elements. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if $f(x) = a$ has a solution in $\mathbb{F}_q$ for all $a \in \mathbb{F}_q$.

The general study of permutation polynomials started with Hermite who considered the case of finite prime fields. Permutation polynomials of arbitrary finite fields were first studied by Dickson [5]. Permutation polynomials have important applications in various fields including cryptography, combinatorics, coding theory, and many other areas of mathematics and engineering [6]. Over the time, permutation polynomials have been studied by many mathematicians to answer some questions like, producing an efficient algorithm to test whether a given polynomial is a permutation polynomial of $\mathbb{F}_q$, finding new classes of permutation polynomials, and many others [6].

The following proposition gives several equivalent ways of defining a permutation polynomial over a finite field $\mathbb{F}_q$.

Proposition 2.4.2. *Let $\mathbb{F}_q$ be the finite field of q elements. Let $f \in \mathbb{F}_q[x]$. The following are equivalent:*

(i) *f is a permutation polynomial on $\mathbb{F}_q$.*

(ii) *the function $f : c \mapsto f(c)$ is onto.*

(iii) *the function $f : c \mapsto f(c)$ is one-to-one.*

(iv) *$f(x) = a$ has a solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.*

(v) *$f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.*

Example 2.4.3. Consider the polynomial $f(x) = x^3 + 1$ in $\mathbb{F}_7[x]$. Computing the value of f on the set $\{0, \ldots, 6\} = \mathbb{F}_7$,

x	0	1	2	3	4	5	6
f(x)	1	2	2	0	2	0	0

f is not onto on $\mathbb{F}_7$, hence not a permutation polynomial on $\mathbb{F}_7$.

Example 2.4.4. Consider the polynomial $g(x) = x^5 + 1$ in $\mathbb{F}_7[x]$. Computing the value of g on the set $\{0, \ldots, 6\} = \mathbb{F}_7$,

x	0	1	2	3	4	5	6
g(x)	1	2	5	6	3	4	0

We see that, g is a bijection on $\mathbb{F}_7$, hence a permutation polynomial on $\mathbb{F}_7$.

Example 2.4.5. Let $h(x) = x^5 + 2x^3 + 5x$ in $\mathbb{F}_7[x]$. Then the value of h on the set $\{0, \ldots, 6\} = \mathbb{F}_7$ is as following:

x	0	1	2	3	4	5	6
h(x)	0	1	2	4	3	5	6

Hence h is a permutation polynomial on $\mathbb{F}_7$.

By Theorem 1.1.22, for every function $\phi : \mathbb{F}_q \to \mathbb{F}_q$ there exists a unique polynomial $g \in \mathbb{F}_q[x]$ of degree at most $q - 1$, that represents ϕ in the sense that $g(a) = \phi(a)$ for all

$a \in \mathbb{F}_q$. Hence every function over the finite field $\mathbb{F}_q$ can be regarded as a polynomial function of degree at most $q-1$.

The next result characterizes a class of permutation polynomials of the form x^n for a positive integer n.

Theorem 2.4.6. *Let $n > 0$ be an integer. The monomial x^n is a permutation polynomial of $\mathbb{F}_q$ if and only if $(n, q-1) = 1$.*

Proof. $f(x) = x^n$ is a permutation polynomial of $\mathbb{F}_q$ if and only if function $f : \mathbb{F}_q \to \mathbb{F}_q$ is onto. Clearly, $f(0) = 0$. Then f is a permutation polynomial on $\mathbb{F}_q$ if and only if $f(\mathbb{F}_q^\times) = \mathbb{F}_q^\times$. Let $a \in \mathbb{F}_q^\times$ be the generator of $\mathbb{F}_q^\times$. Then by Proposition 1.1.11(ii), a^n generates $\mathbb{F}_q^\times$ if and only if $(n, q-1) = 1$. □

By Theorem 2.4.6, for the finite field $\mathbb{F}_q$ with $q = p^n$, $f(x) = x^p$ is a permutation polynomial on $\mathbb{F}_q$ since $(p, p^n - 1) = 1$. This polynomial f is exactly the Frobenius map.

Note that for permutation polynomials $f, g \in \mathbb{F}_q[x]$, composition of f and g is again a permutation polynomial on $\mathbb{F}_q$. It is known that if $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ then $f_1(x) = af(x+c) + b$, $a, b, c \in \mathbb{F}_q$ and $a \neq 0$, is again a permutation polynomial of $\mathbb{F}_q$ [5]. To address the question if a given polynomial is a permutation polynomial, the first, and the most useful criterion was given by Hermite for q prime, and by Dickson for general q [5]. We first give following lemma in order to prove Hermite's Criterion.

Lemma 2.4.7. ([5], 7.3) Let $a_0, a_1, \ldots, a_{q-1}$ be elements of $\mathbb{F}_q$. The following are equivalent:

(i) $\{a_0, a_1, \ldots, a_{q-1}\} = \mathbb{F}_q$.

(ii) $\displaystyle\sum_{i=0}^{q-1} a_i^j = \begin{cases} 0 & \text{for } j = 0, 1, \ldots, q-2 \\ -1 & \text{for } j = q-1 \end{cases}$

Proof. For fixed i with $0 \leq i \leq q-1$, consider the polynomial

$$g_i(x) = 1 - \sum_{j=0}^{q-1} a_i^j x^{q-1-j}.$$

Then $g_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i^{q-1} = 1 - \sum_{j=0}^{q-1} 1 = 1 - 0 = 1$. And $g_i(b) = 0$ for all $b \in \mathbb{F}_q$ with $b \neq a_i$. To see this, let $b \in \mathbb{F}_q$ with $b \neq a_i$ and $b \neq 0$, we have:

$$g_i(b) = 1 - \sum_{j=0}^{q-1} a_i^j b^{q-1-j} = 1 - \sum_{j=0}^{q-1} (a_i b^{-1})^j = 1 - \frac{1 - (a_i b^{-1})^q}{1 - (a_i b^{-1})} = 1 - 1 = 0.$$

Consider the polynomial,

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = \sum_{i=0}^{q-1} \left(1 - \sum_{j=0}^{q-1} a_i^j x^{q-1-j} \right) = \sum_{j=0}^{q-1} \left(- \sum_{i=0}^{q-1} a_i^j \right) x^{q-1-j}.$$

Note that if $a_j = a_k$ for some $0 \leq j, k \leq q-1$, then $g(a_j) = \sum_{i=0}^{q-1} g_i(a_j) = g_j(a_j) + g_k(a_j) = 2$. Hence it is easy to see that $\{a_0, a_1, \ldots, a_{q-1}\} = \mathbb{F}_q$ if and only if g maps each element of $\mathbb{F}_q$ into 1. Since $deg(g) \leq q-1$, g is minimally represented with respect to $\mathbb{F}_q$, by Lemma 2.2.2 $g(x) = 1$, which is equivalent to (ii). □

Theorem 2.4.8. [Hermite's Criterion] ([5], 7.4) Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:

(i) f has exactly one root in $\mathbb{F}_q$.

(ii) For each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \bmod p$, the minimal representation of $f(x)^t$ with respect to $\mathbb{F}_q$ has degree $\leq q-2$.

Proof. Let $f_{r,t} = \sum_{i=0}^{q-1} b_i^{(t)} x^i$ be the minimal representation of $f(x)^t$ with respect to $\mathbb{F}_q$. Note that, By Proposition 1.1.23,

$$f_{r,t} = \sum_{c \in \mathbb{F}_q} f(c)^t (1 - (x-c)^{q-1}).$$

Then $b_{q-1}^{(t)} = - \sum_{c \in \mathbb{F}_q} f(c)^t$.
Now let f be a permutation polynomial of $\mathbb{F}_q$. Then (i) is trivially true. Since f is a

permutation polynomial on $\mathbb{F}_q$, by Lemma 2.4.7, for $1 \leq t \leq q-2$, $b_{q-1}^{(t)} = 0$, hence (ii) follows.

Conversely, suppose (i) and (ii) hold, then (i) implies $\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = q-1 = -1$. Also, (ii) implies $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ for $1 \leq t \leq q-2$, with $t \not\equiv 0 \bmod p$. For $t \equiv 0 \bmod p$, $t = kp^s$ such that $k \not\equiv 0 \bmod p$ and $1 \leq k \leq q-2$. Then,

$$\sum_{c\in\mathbb{F}_q} f(c)^t = \sum_{c\in\mathbb{F}_q} f(c)^{kp^s} = \left(\sum_{c\in\mathbb{F}_q} f(c)^k\right)^{p^s} = 0.$$

Note that for $t = 0$, $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ holds trivially. Then by Lemma 2.4.7, we see that $\{f(c) \mid c \in \mathbb{F}_q\} = \mathbb{F}_q$. Hence, f is a permutation polynomial of $\mathbb{F}_q$. □

Corollary 2.4.9. *There is no permutation polynomial of $\mathbb{F}_q$ of degree $d > 1$ such that $d \mid q-1$.*

Proof. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree $d > 1$ such that $d \mid q-1$. Then $q-1 = kd$ for some positive integer k. Then $deg(f^k) = kd = q-1$. Since $d > 1$, $k \leq q-2$. Then condition (ii) in Theorem 2.4.8 does not hold for $t = k$. Hence f is not a permutation polynomial of $\mathbb{F}_q$. □

In view of Corollary 2.4.9, we can see why Example 2.4.3 is not a permutation polynomial of $\mathbb{F}_7$. Condition (i) in Theorem 2.4.8 may be replaced by following;

Theorem 2.4.10. *Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

(i) *The minimal representation of $f(x)^{q-1}$ with respect to $\mathbb{F}_q$ is monic with degree $q-1$.*

(ii) *For each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0$ mod p, the minimal representation of $f(x)^t$ with respect to $\mathbb{F}_q$ has degree $\leq q-2$.*

Proof. It is suffices to show that condition (i) in Theorem 2.4.8 is equivalent to condition (i) in this theorem. That is, we want to show that f has exactly one root in $\mathbb{F}_q$ if and only if the minimal representation of f with respect to $\mathbb{F}_q$ has degree $q-1$. Assume f has exactly

k roots in $\mathbb{F}_q$. Following the same notations as in Theorem 2.4.8, $f_{r,q-1}$ is monic of degree $q-1$ implies $b_{q-1}^{(q-1)} = -\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = -(q-k) = k$. Then $f_{r,q-1}$ is monic of degree $q-1$ if and only if $k = 1$. □

Example 2.4.11. (Revisit Ex 2.4.4):

$$\begin{aligned}
g_{r,1} &= x^5 + 1 \\
g_{r,2} &= 2x^5 + x^4 + 1 \\
g_{r,3} &= 3x^5 + 3x^4 + x^3 + 1 \\
g_{r,4} &= 6x^5 + 4x^4 + 6x^3 + x^2 + 1 \\
g_{r,5} &= 5x^5 + 3x^4 + 3x^3 + 5x^2 + x + 1 \\
g_{r,6} &= x^6 + 6x^5 + x^4 + 6x^3 + x^2 + 6x + 1
\end{aligned}$$

By Theorem 2.4.10, g is a permutation polynomial on $\mathbb{F}_7$.

Chapter 3

THE CYCLE STRUCTURE OF THE FROBENIUS PERMUTATION

In the previous chapter, we characterized subfield compatible polynomials and we noticed that how the Frobenius permutation turned to play a crucial role. The characterization involves the cycle decomposition of the Frobenius permutation. The motivation for this chapter is to describe the cycle structure of the Frobenius permutation. In order to achieve the goal, we first will generalize the Frobenius permutation and examine the cycle structure of these generalized permutations.

3.1 Shift permutation $\tau_{m,n}$

Let m, n be positive integers different from 1. Let $S = \{0, 1, \ldots, m^n - 1\}$. Consider the base m presentation of the elements of S. Each element $i \in S$ has a unique representation in base m as follows:

$$i = \sum_{j=0}^{n-1} a_j m^j, \text{ where } 0 \leq a_j < m, \text{ for all } j.$$

Then we write $i = (a_{n-1}, a_{n-2}, \ldots, a_1, a_0)$ as an n-tuple in base m.

Definition 3.1.1. Let m and n be positive integers different from 1. For the set $S = \{0, 1, \ldots, m^n - 1\}$ define the function $\tau_{m,n} : S \to S$ so that for all $i \in S$, $\tau_{m,n}(i) = q + r$ where $mi = m^n q + r$ with $0 \leq r \leq m^n - 1$.

Proposition 3.1.2. *Let $\tau_{m,n}$ be the function on the set S defined above. Then $\tau_{m,n}$ is a permutation on the set S. Moreover, $\tau_{m,n}$ generalizes the Frobenius permutation.*

Proof. First we shall show that $\tau_{m,n}$ is a well defined map on the set S. We first must show that $q + r \in S$, that is, $0 \leq q + r \leq m^n - 1$. Clearly $q + r \geq 0$. We claim that $q \leq m - 1$. If not, $q \geq m$ and $mi = m^n q + r \geq m^n m$ which implies that $i - m^n \geq 0$ contradicting the fact that $i \in S$. We also claim that $r \leq m^n - m$. Since $mi = m^n q + r$, $r \equiv 0 \bmod m$. Then $r = km$ for some nonnegative integer k. Now $0 \leq r < m^n$, if $k \geq m^{n-1}$ then $r = km \geq m^n$, which is false. Hence $k \leq m^{n-1} - 1$ and hence $r \leq m^n - m$. Consequently, $0 \leq q + r \leq m - 1 + m^n - m = m^n - 1$. Hence, $q + r \in S$. Hence $\tau_{m,n}$ is a well defined map on the set S.

Let $i, j \in S$ and suppose $\tau_{m,n}(i) = \tau_{m,n}(j)$. Let $\tau_{m,n}(i) = q_1 + r_1$ and $\tau_{m,n}(j) = q_2 + r_2$ where $mi = m^n q_1 + r_1$ and $mj = m^n q_2 + r_2$. Then $q_1 + r_1 = q_2 + r_2$ implies $q_1 - q_2 = r_2 - r_1$. Also $mi = m^n q_1 + r_1$ and $mj = m^n q_2 + r_2$ implies $m(i - j) = m^n(q_1 - q_2) + (r_1 - r_2)$. Consequently, $m(i - j) = (r_2 - r_1)(m^n - 1)$. Note that $(m, m^n - 1) = 1$. Which implies $(m^n - 1)|(i - j)$. But $i, j \in S$. Hence $i = j$. Hence $\tau_{m,n}$ is an injection. As the set S is finite, $\tau_{m,n}$ is a bijection and hence a permutation on the set S.

Note that for $m = p$ permutation $\tau_{p,n}$ is the Frobenius permutation discussed in the previous chapter which was introduced by J. Hull in his paper [1]. Hence $\tau_{m,n}$ generalizes the Frobenius permutation. □

Definition 3.1.3. A permutation ψ is a *(left) shift permutation* on a tuple if $\psi(a_n, \ldots, a_1) = (a_{n-1}, \ldots, a_1, a_n)$. That is ψ shifts all the elements of a tuple by 1 place to the left, with the element shifted off the beginning inserted back at the end.

Proposition 3.1.4. *The permutation $\tau_{m,n}$ defined above is a shift permutation on the n-tuple expression of $i \in S$ in base m.*

Proof. For $i \in S$, let $i = (a_{n-1}, a_{n-2}, \ldots, a_1, a_0)$ be the unique n-tuple expression of i in base

m. Then,

$$\begin{aligned} i &= \sum_{j=0}^{n-1} a_j m^j \\ &= a_{n-1}m^{n-1} + a_{n-2}m^{n-2} + \cdots + a_1 m + a_0 \\ mi &= a_{n-1}m^n + a_{n-2}m^{n-1} + \cdots + a_1 m^2 + a_0 m \\ &= m^n(a_{n-1}) + (a_{n-2}m^{n-1} + \cdots + a_1 m^2 + a_0 m) \end{aligned}$$

Then, $q = a_{n-1}$ and $r = a_{n-2}m^{n-1} + \cdots + a_1 m^2 + a_0 m$, and clearly $0 \leq r < m^n$.
So, $\tau_{m,n}(i) = q + r = a_{n-1} + a_{n-2}m^{n-1} + \cdots + a_1 m^2 + a_0 m = (a_{n-2}, a_{n-3}, \ldots, a_1, a_0, a_{n-1})$.
Hence, $\tau_{m,n}$ is a shift permutation on the n-tuple expression of the elements of S, which shifts components of the tuple by 1 place. □

From now onwards, we will identify $\tau_{m,n}$ as a shift permutation on the n-tuple expression in base m of the elements of S.

Definition 3.1.5. The *order* of a permutation ϕ defined on a set S, is the smallest positive integer k such that $\phi^k(i) = i$ for all $i \in S$.

Definition 3.1.6. The *order* of an element $i \in S$ under the permutation ϕ, denoted as $\mathcal{O}(i)$, is the smallest number d such that $\phi^d(i) = i$.

Proposition 3.1.7. *The order of $\tau_{m,n}$ is n.*

Proof. Since $\tau_{m,n}$ is a shift permutation on the n-tuple expression of the elements of S which shifts components of the tuple by 1 place, n^{th} iteration of $\tau_{m,n}$ will yield the original n-tuple. For any $k = 1, 2, \ldots, n-1$, $\mathcal{O}(1) \neq k$. Hence the order of $\tau_{m,n}$ is n. □

Proposition 3.1.8. (Proposition 2.3.4 Revisited) The function $\phi : \{0, 1, \ldots, p^n - 1\} \to \{0, 1, \ldots, p^n - 1\}$ defined by $\phi(i) = q + r$ for all $i \in \{0, 1, \ldots, p^n - 1\}$, where $pi = p^n q + r$, $0 \leq r < p^n$, is a permutation of order n.

Proof. Proof is clear. □

3.2 The cycle structure of $\tau_{m,n}$

In this section, we will give the cycle decomposition of the shift permutation $\tau_{m,n}$ and in particular we will obtain the cycle decomposition of the Frobenius permutation.

Let S_n be the symmetric group on n letters. For $\sigma \in S_n$, σ fixes $i \in \{1, 2, ..., n\}$ if $\sigma(i) = i$, and σ moves i if $\sigma(i) \neq i$.

Definition 3.2.1. A *cycle* is a permutation which maps a finite subset $\{i_1, i_2, ..., i_k\}$ by

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$$

and fixes the rest of the element in the set. Such a cycle is denoted by $(i_1\, i_2\, \cdots\, i_k)$. In this case we say the cycle has *length* k.

Two permutations $\sigma, \mu \in S_n$ are called *disjoint* if every i moved by one is fixed by the other. Observe that disjoint permutations commute under multiplication, that is if $\sigma, \mu \in S_n$ are disjoint then $\sigma\mu = \mu\sigma$.

Proposition 3.2.2. *Every permutation $\sigma \in S_n$ is either a cycle or the product of disjoint cycles.*

Definition 3.2.3. A *complete factorization* of a permutation σ is a factorization of σ into disjoint cycles that contains a cycle of length one for every i fixed by σ.

Proposition 3.2.4. *For any $\sigma \in S_n$, the order of σ is the least common multiple of the lengths of the disjoint cycles in the complete factorization of σ.*

Proposition 3.2.5. *For every positive divisor k of n, there is a cycle of length k in the complete factorization of $\tau_{m,n}$ defined earlier.*

Proof. Let k be a positive divisor of n. Then $n = tk$ for some positive integer t. Consider $i \in S$ that has the n-tuple expression in base m with string $0, 0, ..., 0, 1$ of length k concatenated t times. Then k-th iteration of $\tau_{m,n}$ will yield the same tuple as an output. Also k is the

smallest such integer for which $\tau_{m,n}(i) = i$. Then $\mathcal{O}(i) = k$. Since an element of order k produces a cycle of length k, we conclude that for every positive divisor k of n, there is at least one cycle of length k in the complete factorization of $\tau_{m,n}$. □

Proposition 3.2.5 and shifting behavior of $\tau_{m,n}$ provides important informations about the cycle structure of $\tau_{m,n}$. To describe the cycle structure of $\tau_{m,n}$ completely, only question that needs to be answered is following:

Question 3.2.6. Let k be any positive divisor of n. What is the number of cycles of length k in the cycle decomposition of $\tau_{m,n}$?

In the rest of the section we will answer this question.
For a positive integer k, consider the following subsets of S:

$$\begin{aligned} T_k(\tau) &= \{i \in S \,|\, \mathcal{O}(i) = k\} \\ &= \{i \in S \,\big|\, \tau_{m,n}^k(i) = i \text{ and } \tau_{m,n}^{k'}(i) \neq i, \text{ for any } k' < k\} \\ A_k(\tau) &= \{i \in S \,|\, \mathcal{O}(i) = d, \text{ for all } d > 0 \text{ and } d|k\} \\ &= \{i \in S \,\big|\, \tau_{m,n}^k(i) = i\} \\ &= \bigcup_{d|k, d>0} T_d(\tau) \end{aligned}$$

Proposition 3.2.7. *Let $\tau_{m,n}, A_k(\tau)$ and $T_k(\tau)$ as defined above.*

(i) *For any positive divisor d of k, $A_k(\tau) \supseteq A_d(\tau)$.*

(ii) *For any positive divisor k of n, $A_k(\tau) \supseteq T_k(\tau)$.*

(iii) *$|A_k(\tau)| = m^k$.*

Proof. Statements (i) and (ii) are clear. For (iii), note that for any divisor d of k, element of order d has a repeating string of length d in the n-tuple expression in base m which can also be seen as an element which has a repeating string of length k in the n-tuple expression in base m. For example, for $m = 2, n = 8, k = 4$ and $d = 2$, $i = (10101010)$ has repeating

string $-10-$ of length 2 but can also be seen as repeating string $-1010-$ of length 4. Hence all the elements in $A_k(\tau)$ have a repeating string of length k in the n-tuple expression in base m. Since $0 \leq a_j < m$, we have exactly m choices for each place in the repeating string of length k. Hence $|A_k(\tau)| = m^k$. □

Let m, n be positive integers greater than 1. Let $n = \prod_{i=1}^{t} p_i^{r_i}$ be prime factorization of n, where p_i are distinct primes and r_i positive integers. Consider Euler's totient function ϕ, which is given by

$$\phi(n) = \prod_{i=1}^{t} p_i^{r_i-1} \cdot (p_i - 1), \qquad (\star)$$

which can be viewed as a polynomial in t variables $\{p_1, p_2, ..., p_t\}$. Let P^α be the monomial term in $\phi(n)$ with multidegree $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_t)$ and total degree $|\alpha| = \sum_{i=1}^{t} \alpha_i$. Note that for all the monomial terms $r_i - 1 \leq \alpha_i \leq r_i$ for all $i = 1, 2, \ldots, t$. Then the expansion of $\phi(n)$ can be described as follow:

$$\phi(n) = \begin{cases} \sum\limits_{r_i-1 \leq \alpha_i \leq r_i} (-1)^{|\alpha|} P^\alpha & \text{if } \sum\limits_{i=1}^{t} r_i \ \textit{is even} \\ \sum\limits_{r_i-1 \leq \alpha_i \leq r_i} (-1)^{|\alpha|+1} P^\alpha & \text{if } \sum\limits_{i=1}^{t} r_i \ \textit{is odd} \end{cases}$$

Also let $sgn(P^\alpha)$ be sign function which expresses sign of P^α in the polynomial expression of $\phi(n)$ given in $(\star)$.

Denote $F(m, n) = \sum sgn(P^\alpha) \cdot m^{P^\alpha}$ where summation runs over all monomials P^α in the polynomial expression of $\phi(n)$ given in $(\star)$.

Example 3.2.8. Let $n = p_1^3 p_2^3$. Then $\phi(n) = p_1^3 p_2^3 - p_1^3 p_2^2 - p_1^2 p_2^3 + p_1^2 p_2^2$. Then we get,

$$F(m, n) = m^{p_1^3 p_2^3} - m^{p_1^3 p_2^2} - m^{p_1^2 p_2^3} + m^{p_1^2 p_2^2}$$

Note that $F(m, n)$ can equivalently be written as follows:

$$F(m, n) = m^n - m^{n/p_1} - m^{n/p_2} + m^{n/p_1 p_2}$$

This equivalent way of writing $F(m,n)$ can be found in ([9], page 84). For arbitrary m and n, $F(m,n)$ can be written as follows:

$$\begin{aligned} F(m,n) &= m^n - \sum_{i=1}^{t} m^{n/p_i} + \sum_{i<j} m^{n/p_i p_j} - \sum_{i<j<k} m^{n/p_i p_j p_k} + \cdots + (-1)^t m^{n/p_1 \cdots p_t} \\ &= \sum_{d|n, d>0} \mu(d) m^{n/d} \end{aligned}$$

where μ is the Möbius μ-function.

We will show next that $F(m,n)$ gives the number of elements of order exactly n under the permutation $\tau_{m,n}$. That is $F(m,n) = |T_n(\tau)|$ where $T_n(\tau)$ is as defined earlier. Fix positive integers m and n different than 1. Let $n = \prod_{i=1}^{t} p_i^{r_i}$ be prime decomposition of n, where p_i are distinct primes. Let $\tau_{m,n}$, $F(m,n)$, $A_n(\tau)$ and $T_n(\tau)$ as defined earlier.

Denote $q_i = \frac{n}{p_i}$, $i = 1, 2, \ldots, t$. For example, if $n = p_1 p_2 p_3$ then $q_1 = p_2 p_3$, $q_2 = p_1 p_3$ and $q_3 = p_1 p_2$. Note that $|A_{q_i}(\tau)| = m^{n/p_i}$.

Proposition 3.2.9. *The set* $\bigcap_{i=1}^{l} A_{q_i}(\tau) = A_{n/p_1 \cdots p_l}(\tau)$, $1 \leq l \leq t$.

Proof. We will proceed by induction on l. Claim holds trivially for $l = 1$. Assume that the claim holds for $l \geq 1$. Consider the case $l+1$. Then,

$$\begin{aligned} \bigcap_{i=1}^{l+1} A_{q_i}(\tau) &= \left(\bigcap_{i=1}^{l} A_{q_i}(\tau) \right) \bigcap A_{q_{l+1}}(\tau) \\ &= A_{n/p_1 \cdots p_l}(\tau) \bigcap A_{n/p_{l+1}}(\tau) \\ &= \{ i \in S | \mathcal{O}(i) = d \text{ under } \tau_{m,n}, \text{ for all } d \text{ such that } d|(n/p_1 \cdots p_l) \text{ and } d|(n/p_{l+1}) \} \\ &= \{ i \in S | \mathcal{O}(i) = d \text{ under } \tau_{m,n}, \text{ for all } d \text{ such that } d|(n/p_1 \cdots p_l p_{l+1}) \} \\ &= A_{n/p_1 \cdots p_{l+1}}(\tau) \end{aligned}$$

Hence by mathematical induction, claim holds. □

Corollary 3.2.10. *Let $\Lambda = \{1, 2, \ldots, t\}$ be the set of indices. For any subset $\lambda \subseteq \Lambda$,*

$$\bigcap_{i \in \lambda} A_{q_i}(\tau) = A_{(n/\prod\limits_{i \in \lambda} p_i)}(\tau).$$

Proof. We can rename all the primes p_i such that $\lambda = \{1, 2, \ldots, l\}$ for $1 \leq l \leq t$. Then by Proposition 3.2.9, we can derive the required equality. □

Remark 3.2.11. Cardinality of $\bigcap\limits_{i \in \lambda} A_{q_i}(\tau)$ is $m^{(n/\prod\limits_{i \in \lambda} p_i)}$ for $\lambda \subseteq \Lambda$.

Lemma 3.2.12. *Let m and n be integers greater than 1. Let k be a positive divisor of n. Let $k = \prod\limits_{i=1}^{s} p_i^{r_i}$ be the prime decomposition of k. Then $T_k(\tau) = A_k(\tau) - \left(\bigcup\limits_{i=1}^{s} A_{q_i}(\tau)\right)$ where $q_i = \frac{k}{p_i}$ for all $i = 1, 2, \ldots, s$.*

Proof. Note that, $\frac{k}{q_i} = p_i$ for all i. Then there does not exist a divisor k' of k such that $q_i < k' < k$ for all i. Then for an element $c \in T_k(\tau)$,

$$\begin{aligned} c \in T_k(\tau) &\Leftrightarrow c \in A_k(\tau) \text{ and } c \notin A_{k'}(\tau) \text{ for all } k' | k \\ &\Leftrightarrow c \in A_k(\tau) \text{ and } c \notin A_{q_i}(\tau) \text{ for all } q_i \\ &\Leftrightarrow c \in A_k(\tau) - \left(\bigcup_{i=1}^{s} A_{q_i}(\tau)\right) \end{aligned}$$

□

Theorem 3.2.13. *Let m, n be positive integers greater than 1. Let $n = \prod\limits_{i=1}^{t} p_i^{r_i}$ be prime factorization of n, where p_i are distinct primes and r_i positive integers. Let $\tau_{m,n}$, $A_k(\tau)$, $T_k(\tau)$ and $F(m, n)$ be as defined previously. Then $|T_n(\tau)| = F(m, n)$. That is there are exactly $F(m, n)$ many elements of order n in the set S under $\tau_{m,n}$.*

Proof. For simplification of writing, we call $A_k(\tau) = A_k$ and $T_k(\tau) = T_k$. By Lemma 3.2.12 we have,

$$T_n = \left(\bigcup_{i=1}^{t} A_{q_i}\right)^c.$$

Then,

$$\begin{aligned}
|T_n| &= \left|\left(\bigcup_{i=1}^{t} A_{q_i}\right)^c\right| \\
&= |S| - \left|\left(\bigcup_{i=1}^{t} A_{q_i}\right)\right| \\
&= |S| - \left(\sum_{i=1}^{t} |A_{q_i}| - \sum_{i<j} |A_{q_i} \cap A_{q_j}| + \sum_{i<j<k} |A_{q_i} \cap A_{q_j} \cap A_{q_k}| - \cdots + (-1)^{t+1} \left|\bigcap_{i=1}^{t} A_{q_i}\right|\right) \\
&= |S| - \sum_{i=1}^{t} |A_{q_i}| + \sum_{i<j} |A_{q_i} \cap A_{q_j}| - \sum_{i<j<k} |A_{q_i} \cap A_{q_j} \cap A_{q_k}| + \cdots - (-1)^{t+1} \left|\bigcap_{i=1}^{t} A_{q_i}\right| \\
&= m^n - \sum_{i=1}^{s} m^{n/p_i} + \sum_{i<j} m^{n/p_i p_j} - \sum_{i<j<h} m^{n/p_i p_j p_h} + \cdots - (-1)^{t+1} m^{n/p_1 \cdots p_t} \\
&= F(m,n)
\end{aligned}$$

□

Theorem 3.2.13 yields following important corollaries.

Corollary 3.2.14. *Let the setup be same as Theorem 3.2.13. Then* $m^n = \sum_{d|n, d>0} F(m,d)$.

Proof. For any divisor d of n, $d = \prod_{i \in \lambda} p_i^{r'_i}$, where $\lambda \subseteq \Lambda = \{1, 2, \ldots, t\}$. Then by the similar argument as Theorem 3.2.13, $|T_d(\tau)| = F(m,d)$. Now $|S| = \sum_{d|n, d>0} |T_d(\tau)|$. Hence $m^n = \sum_{d|n, d>0} F(m,d)$. Here $F(m,1) = m$. □

Corollary 3.2.15. *Let the setup be the same as Theorem 3.2.13. Then for any positive divisor* d *of* n *there are exactly* $\frac{F(m,d)}{d}$ *many cycles of length* d *in the cycle decomposition of* $\tau_{m,n}$.

Proof. From Theorem 3.2.13, for any positive divisor d of n, $|T_d(\tau)| = F(m,d)$. That is there are exactly $F(m,d)$ many elements of order exactly d under $\tau_{m,n}$. Since these elements produces cycle of length d in the cycle decomposition of $\tau_{m,n}$, there are exactly $\frac{F(m,d)}{d}$ many cycles of length d. □

Corollary 3.2.16. *Let m, n be positive integers different from* 1. *Then $F(m,n) \equiv 0$ mod n. That is $n|F(m,n)$.*

Proof. It is clear from Corollary 3.2.15. □

Corollary 3.2.17. (Fermat's Little Theorem) If p is a prime number, then for any integer a, $a^p \equiv a \bmod p$.

Proof. Let $m = a$ and $n = p$ and apply Theorem 3.2.13. Then $F(a,p) = a^p - a$. By Corollary 3.2.16, $F(a,p) \equiv 0 \bmod p$. That is $a^p \equiv a \bmod p$. □

Corollary 3.2.18. (Case of Euler's Theorem) If p is a prime and s is a positive integer, then for any integer a such that (a,p)=1, $a^{\phi(p^s)} \equiv 1 \bmod p^s$.

Proof. Let $m = a$ and $n = p^s$ and apply Theorem 3.2.13. Then $F(a,p^s) \equiv 0 \bmod p^s$. That is $a^{p^s} - a^{p^{s-1}} \equiv 0 \bmod p^s$. Which implies $a^{p^{s-1}}\left(a^{p^s-p^{s-1}} - 1\right) \equiv 0 \bmod p^s$. Since $(a,p) = 1$, we get $a^{p^s-p^{s-1}} - 1 \equiv 0 \bmod p^s$. That is $a^{\phi(p^s)} \equiv 1 \bmod p^s$. □

According to Dickson [9] the congruence in Corollary 3.2.16, for prime p instead of any integer m, was first noted by Gauss and was published in his posthumous paper in 1863. Schönemann proved it for prime powers in 1844 and Serret in 1854 proved the congruence for any integer m. During 1880-1883, four independent proofs for all integer m were given by Kantor, Weyr, Lucas, and Pellet. In 1986, Smyth [10] gave a coloring proof of the congruence by generalizing the idea of Peterson's proof of Fermat's little theorem. More recently Isaacs and Pournaki [11] proved the congruence via group theory in 2005

Corollary 3.2.15 answers Question 3.2.6 and gives us the missing piece of information for cycle decomposition of $\tau_{m,n}$.

Considering the Frobenius permutation ϕ which is $\tau_{p,n}$, the cycle decomposition of ϕ has exactly $\frac{F(p,d)}{d}$ many cycles of length d for every positive divisor d of n.

Example 3.2.19. Consider the finite field $\mathbb{F}_{2^{30}}$. Let $S = \{0, 1, \ldots, 2^{30} - 1\}$ and $\phi : S \to S$ be the Frobenius permutation of order n. Here $m = 2$ and $n = 30 = 2 \cdot 3 \cdot 5 = p_1 \cdot p_2 \cdot p_3$.

Then

$$\begin{aligned} F(2,30) &= 2^n - 2^{p_1 \cdot p_2} - 2^{p_1 \cdot p_3} - 2^{p_2 \cdot p_3} + 2^{p_1} + 2^{p_2} + 2^{p_3} - 2^1 \\ &= 2^{30} - 2^6 - 2^{10} - 2^{15} + 2^2 + 2^3 + 2^5 - 2 \end{aligned}$$

and

$$\begin{aligned} F(2,15) &= 2^{15} - 2^3 - 2^5 + 2 \\ F(2,10) &= 2^{10} - 2^2 - 2^5 + 2 \\ F(2,6) &= 2^6 - 2^2 - 2^3 + 2 \\ F(2,5) &= 2^5 - 2 \\ F(2,3) &= 2^3 - 2 \\ F(2,2) &= 2^2 - 2 \\ F(2,1) &= 2 \end{aligned}$$

We see that $2^{30} = |S| = \sum_{d|30} F(2,d)$. We can count number of cycles of length d for each divisor d of 30 according to Corollary 3.2.15.

3.3 The monomial permutation $\sigma_{m,n}$ and its cycle structure

Fix the finite field $\mathbb{F}_{p^n}$ of order p^n with prime field $\mathbb{F}_p$ and an algebraic closure $\overline{\mathbb{F}_p}$. The Frobenius map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(x) = x^p$ is a permutation monomial on $\mathbb{F}_{p^n}$. By Theorem 2.4.6, we know that for a positive integer m such that $(m, p^n - 1) = 1$, $f_m : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $f_m(x) = x^m$ is also a permutation monomial on $\mathbb{F}_{p^n}$.

The origin of the Frobenius permutation lies in the Frobenius map, which is a permutation monomial. So it is natural to think about permutations that can be extended to all the permutation monomials f_m over $\mathbb{F}_{p^n}$ for a positive integer m with $(m, p^n - 1) = 1$. In the previous section, we generalized the Frobenius permutation by replacing p with any integer m and produced the shift permutation $\tau_{m,n}$. In this section we will generalize the Frobenius

permutation in a different way to give similar structure as the Frobenius permutation for all the permutation monomials f_m. In fact, we will show that this new permutation further generalizes the shift permutation $\tau_{m,n}$.

Definition 3.3.1. Let m and n be positive integers greater than 1 such that $(m, n) = 1$. For the set $S = \{0, 1, \ldots, n\}$ define the function $\sigma_{m,n} : S \to S$ so that for $i \in \{1, 2, \ldots, n-1\}$, $\sigma_{m,n}(i) = r$ where $mi \equiv r \bmod n$ with $1 \leq r < n$, and $\sigma_{m,n}(i) = i$ for $i \in \{0, n\}$.

Proposition 3.3.2. *The function $\sigma_{m,n}$ defined above is a permutation on the set S. Moreover, $\sigma_{m,n}$ generalizes the shift permutation $\tau_{m,n}$ and in turn generalizes the Frobenius permutation.*

Proof. Let $S' = \{1, 2, \ldots, n-1\}$. First of all we want to show that $r \in S'$. Clearly $0 \leq r < n$. So $r \neq n$. If $\sigma_{m,n}(i) = r = 0$ for some $i \in S'$, then $mi \equiv 0 \bmod n$. Since $(m, n) = 1$, we conclude that n divides i, which is false. Hence $r \in S'$. Now assume that $\sigma_{m,n}(i) = \sigma_{m,n}(j)$ for some $i, j \in S'$. Then $mi \equiv mj \bmod n$. That is $m(i - j) \equiv 0 \bmod n$. Since $(m, n) = 1$, we conclude that $i = j$. Hence $\sigma_{m,n}$ is an injection on S. Since S is a finite set, $\sigma_{m,n}$ is a bijection on S and hence a permutation on S.

Now consider σ_{m,m^n-1} by replacing n with $m^n - 1$. We claim that σ_{m,m^n-1} is the shift permutation $\tau_{m,n}$ on the set S. Clearly $(m, m^n - 1) = 1$. We already have that $\tau_{m,n}(0) = 0$. Consider $\tau_{m,n}(m^n - 1) = q + r$ where $m(m^n - 1) = m^n q + r$. But $m(m^n - 1) = m^{n+1} - m = m^{n+1} - m^n + m^n - m = m^n(m - 1) + (m^n - m) = m^n q_1 + r_1$. Note that $q_1 + r_1 \in S$ and $0 \leq r_1 < p^n$. Since $\tau_{m,n}$ is a permutation on the set S, $q_1 + r_1 = q + r$. Thus $\tau_{m,n}(m^n - 1) = m^n - 1$. Now consider $\tau_{m,n}$ on S'. For $i \in S'$, we rewrite $mi = m^n q + r = (m^n - 1)q + (q + r)$. Then $\tau_{m,n}(i) = q + r$ and $mi \equiv q + r \bmod m^n - 1$. Since $i \in S'$, we have $0 < q + r < m^n - 1$. Hence $q + r \in S'$. Hence $\tau_{m,n}$ and σ_{m,m^n-1} are same function on S. Hence $\sigma_{m,n}$ generalizes the shift permutation $\tau_{m,n}$ on the set S and hence generalizes the Frobenius permutation. □

Proposition 3.3.3. *Let $\mathbb{F}_{p^n}$ be the finite field of characteristic p and order p^n. Let $\sigma_{m,n'}$ be the permutation on the set S as defined earlier where $n' = p^n - 1$. Then $f_m \in \mathbb{F}_{p^n}[x]$, $f_m(x) = x^m$ is a permutation monomial on $\mathbb{F}_{p^n}$. Also for any $\alpha \in \mathbb{F}_{p^n}$, $f_m(\alpha^i) = \alpha^{\sigma_{m,n'}(i)}$ for all $i \in S$.*

Proof. Since $(m, p^n - 1) = 1$, $f_m(x) = x^m$ is a permutation monomial on $\mathbb{F}_{p^n}$. Let $\alpha \in \mathbb{F}_{p^n}$ be any element in $\mathbb{F}_{p^n}$. Then for $i \in S$, $f_m(\alpha^i) = (\alpha^i)^m = \alpha^{mi} = \alpha^{q(p^n-1)+r} = (\alpha^{p^n-1})^q \cdot \alpha^r = \alpha^r = \alpha^{\sigma_{m,n'}(i)}$. □

Now back to our original goal of giving complete factorization of the Frobenius permutation. Although we already described the cycle factorization of the Frobenius permutation in the previous section, we would like to examine the same in the view of our new permutation $\sigma_{m,n}$ which generalizes the Frobenius permutation.

Definition 3.3.4. A permutation ψ is called a *cyclic permutation* if the complete factorization of ψ has exactly one nontrivial cycle.

Proposition 3.3.5. *Let $\sigma_{m,n}$ be the permutation on the set S as defined earlier. Then the order of $\sigma_{m,n}$ is $ord_n(m)$. Moreover if n is a prime and if m is a primitive root modulo n then $\sigma_{m,n}$ is a cyclic permutation.*

Proof. Let the order of $\sigma_{m,n}$ be t. Then for all $i \in S$, $\sigma^t_{m,n}(i) = i$. That is $m^t i \equiv i \bmod n$. Which implies $(m^t - 1)i \equiv 0 \bmod n$ for all $i \in S$. We know that $(m^{ord_n(m)} - 1)i \equiv 0 \bmod n$ for all $i \in S$. Then $t \leq ord_n(m)$. Suppose $t < ord_n(m)$. Then for $i = 1$, $m^t - 1 \equiv 0 \bmod n$, which is false. Hence $t = ord_n(m)$.

Now suppose n is a prime and m is a primitive root modulo n. Then $t = ord_n(m) = \phi(n) = n - 1$. Hence the order of $\sigma_{m,n}$ is $n - 1$ which implies the complete factorization of $\sigma_{m,n}$ has a cycle of length $n - 1$. That is $\sigma_{m,n}$ is a cyclic permutation. □

Note that order of σ_{p,p^n-1} is exactly n because $ord_{p^n-1}(p) = n$, which is consistent with the order of the Frobenius permutaion. For the rest of the section, we will use t as the order of $\sigma_{m,n}$ which is $ord_n(m)$. Now that we know the order of the permutation $\sigma_{m,n}$ we can further study the complete factorization of $\sigma_{m,n}$. It follows from Proposition 3.2.4 that for a positive integer k, if the complete factorization of $\sigma_{m,n}$ has a cycle of length k then k divides the order of $\sigma_{m,n}$.

In the case of $\tau_{m,n}$ the converse is also true. But the converse is not always true for $\sigma_{m,n}$. The simplest counterexample would be the cyclic permutation mentioned in Proposition 3.3.5.

Example 3.3.6. Let $n = 7$ and $m = 3$. Note that $ord_7(3) = 6$, hence m is a primitive root modulo n. Then by Proposition 3.3.5, $\sigma_{3,7}$ is a cyclic permutation with only nontrivial cycle of length 6. Note that for $2|6$ and for $3|6$ there are no cycles of length 2 or 3 in the cycle decomposition of $\sigma_{3,7}$. In fact $\sigma_{3,7} = (0)(1\ 3\ 2\ 6\ 4\ 5)(7)$.

Since we already have that $0, n \in S$ produces cycles of length 1 under $\sigma_{m,n}$, we will examine the cycle structure of $\sigma_{m,n}$ on S'. Note that $|S'| = n - 1$.

Theorem 3.3.7. *Let $\sigma_{m,n}$ be a permutation of the order t on the set S as defined earlier. For a positive divisor k of t, let $(m^k - 1, n) = b$. Then there exist an element of order k in the set S' if and only if $b \neq 1$ and $ord_b(m) = k$.*

Proof. Let k be a positive divisor of t and $b = (m^k - 1, n)$. For the forward direction, let $i \in S'$ be such that $\mathcal{O}(i) = k$. We want to show that $b \neq 1$ and $ord_b(m) = k$. Now $\mathcal{O}(i) = k$ implies $\sigma^k_{m,n}(i) = i$, that is $m^k i \equiv i \bmod n$. Then $(m^k - 1)i \equiv 0 \bmod n$. If $b = 1$ then n divides i, which is false. Hence $b \neq 1$. Now assume that $ord_b(m) \neq k$. Let $ord_b(m) = k'$. Since $m^k - 1 \equiv 0 \bmod b$, we see that $k' \leq k$. By assumption $k' \neq k$, hence $k' < k$. Now for $b|n$, let z be the positive integer such that $bz = n$. Then $(m^k - 1)i \equiv 0 \bmod n$ and $(m^k - 1, n) = b$, both together implies that $z|i$. Then let y be the positive integer such that $yz = i$. Since $ord_b(m) = k'$, $m^{k'} - 1 \equiv 0 \bmod b$, which implies $b|(m^{k'} - 1)$. Let w be the positive integer such that $bw = m^{k'} - 1$. Then $(m^{k'} - 1)i = (bw)(yz) = (wy)(bz) \equiv 0 \bmod n$. Hence $m^{k'} i \equiv i \bmod n$, which contradicts the fact that $\mathcal{O}(i) = k$. Hence $ord_b(m) = k$.

Conversely, for a positive divisor k of t, let b be different than 1 and $ord_b(m) = k$. We want to show that there exists an element of order k in the set S'. Let z be as above so that $bz = n$. Since $b|m^k - 1$, let u be the positive integer such that $bu = m^k - 1$. Since $b \neq 1$ and $bz = n$, we have $z \in S'$. Let $\mathcal{O}(z) = l$. We claim that $l = k$. Since $(m^k - 1)z = (bu)z = u(bz) \equiv 0 \bmod n$, we conclude that $l \leq k$. Suppose $l < k$, then

$(m^l - 1)z \equiv 0 \bmod n$ implies $m^l - 1 \equiv 0 \bmod b$, which is false because $ord_b(m) = k$. Hence $l = k$ and thus $z \in S'$ is an element of order k. □

Corollary 3.3.8. *Let $\sigma_{m,n}$ be a permutation of the order t on the set S as defined earlier. For a positive divisor k of t, let $(m^k - 1, n) = b$. There exist a cycle of length k in the complete factorization of $\sigma_{m,n}$ if and only if $b \neq 1$ and $ord_b(m) = k$.*

Proof. Since an element of order k generates a cycle of length k, result follows from the theorem above. □

Note that the Frobenius permutation σ_{p,p^n-1} has the order n, and for any positive divisor k of n, $(p^k - 1, p^n - 1) = p^k - 1$ which is different from 1 and $ord_{p^k-1}(p) = k$. Thus the complete factorization of σ_{p,p^n-1} has a cycle of length k for any positive divisor k of n which we already concluded in Proposition 3.2.5.

To give the complete factorization of $\sigma_{m,n}$, the only question that remains to answer is following.

Question 3.3.9. If there exists an element of order k in the set S', then exactly how many elements have order k in the set S'?

Before we go further, let us recall and fix some notations. Fix positive integers m and n greater than 1 such that $(m, n) = 1$ and let $S = \{0, 1, \ldots, n\}$ and $S' = \{1, 2, \ldots, n - 1\}$. Consider the permutation $\sigma_{m,n}$ as defined earlier. Let $t = ord_n(m)$ be the order of $\sigma_{m,n}$.

For a positive divisor k of t, denote $(m^k - 1, n) = b_k$. Since $b_k | n$, denote c_k to be the integer such that $b_k c_k = n$. Denote $Q(k)$ to be the non negative integer such that $n - 1 = c_k Q(k) + r_k$ where $0 \leq r_k < c_k$. Note that for $b_k = 1$, $Q(k) = 0$.

Example 3.3.10. Consider $\sigma_{5,36}$, order of which is $t = 6$. Then,

k	b_k	c_k	$Q(k)$
1	4	9	3
2	12	3	11
3	4	9	3
6	36	1	35

Now as we denoted in the previous section, for a positive divisor k of t, consider the following subsets of S':

$$\begin{aligned} T_k(\sigma) &= \{i \in S' \,|\, \mathcal{O}(i) = k\} \\ &= \{i \in S' \,|\, \sigma_{m,n}^k(i) = i \text{ and } \sigma_{m,n}^{k'}(i) \neq i, \text{ for any } k' < k\} \\ A_k(\sigma) &= \{i \in S' \,|\, \mathcal{O}(i) = d, \text{ for all } d \text{ such that } d|k\} \\ &= \{i \in S' \,|\, \sigma_{m,n}^k(i) = i\} \\ &= \bigcup_{d|k, d>0} T_d \end{aligned}$$

Our goal is to find the cardinality of $T_k(\sigma)$ for a positive divisor k of t. First consider the following lemma.

Lemma 3.3.11. *Let the set up be as above. For a positive divisor k of t, $i \in A_k(\sigma)$ if and only if $c_k|i$.*

Proof. Let $i \in A_k(\sigma)$, then $\sigma_{m,n}^k(i) = i$. That is $(m^k - 1)i \equiv 0 \bmod n$. Since $(m^k - 1, n) = b_k$, we conclude that $c_k|i$. Conversely if $c_k|i$ for some $i \in S'$, let u_k and y_k be positive integers such that $u_k b_k = m^k - 1$ and $c_k y_k = i$, then $(m^k - 1)i = (u_k b_k)(c_k y_k) = (u_k y_k)(b_k c_k) \equiv 0 \bmod n$. Hence $\sigma_{m,n}^k(i) = i$. Thus $i \in A_k(\sigma)$. □

Proposition 3.3.12. *Let the set up be as above for the permutation $\sigma_{m,n}$.*

(i) *For any positive divisor d of k, $A_k(\sigma) \supseteq A_d(\sigma)$.*

(ii) *For any k, $A_k(\sigma) \supseteq T_k(\sigma)$.*

(iii) $|A_k(\sigma)| = Q(k)$.

(iv) *For* $\sigma_{m,m^n-1} = \tau_{m,n}$, $|A_k(\sigma)| = m^k - 2$.

Proof. Statements (i) and (ii) are clearly true. To prove (iii), first note that there are exactly $Q(k)$ many elements in S' that are divisible by c_k. From Lemma 3.3.11, we can conclude that $|A_k(\sigma)| = Q(k)$.

Now the order of σ_{m,m^n-1} is n. For any positive divisor k of n, $(m^k - 1, m^n - 1) = m^k - 1 = b_k$. Then,

$$\begin{aligned}(m^k-2)\left(\frac{m^n-1}{m^k-1}\right)+\left(\left(\frac{m^n-1}{m^k-1}\right)-1\right) &= (m^k-1-1)\left(\frac{m^n-1}{m^k-1}\right)+\left(\left(\frac{m^n-1}{m^k-1}\right)-1\right)\\ &= (m^n-1)-\left(\frac{m^n-1}{m^k-1}\right)+\left(\left(\frac{m^n-1}{m^k-1}\right)-1\right)\\ &= m^n-2\end{aligned}$$

Note that $0 \leq \left(\frac{m^n-1}{m^k-1}\right) - 1 < \frac{m^n-1}{m^k-1}$. Then $Q(k) = m^k - 2$. Hence $|A_k(\sigma)| = m^k - 2$. □

In the case of $\sigma_{m,m^n-1} = \tau_{m,n}$, we have $|A_k(\sigma)| = |A_k(\tau)| - 2$. This is because we excluded 0 and $m^n - 1$ in the case of $A_k(\sigma)$.

Now fix a positive divisor k of t. We want to find $|T_k(\sigma)|$. Let $k = \prod_{i=1}^{s} p_i^{r_i}$ be the prime decomposition of k for distinct primes p_i and positive integers r_i. Define $G(m, n, k)$ to be the following number:

$$\begin{aligned}G(m,n,k) &= Q(k) - \sum_{i=1}^{s} Q\left(\frac{k}{p_i}\right) + \sum_{i<j} Q\left(\frac{k}{p_ip_j}\right) - \sum_{i<j<h} Q\left(\frac{k}{p_ip_jp_h}\right) + \cdots + (-1)^s Q\left(\frac{k}{\prod_{i=1}^{s} p_i}\right)\\ &= \sum_{d|k,d>0} \mu(d) Q\left(\frac{k}{d}\right)\end{aligned}$$

where μ is the Mobius function.

Denote $q_i = \frac{k}{p_i}$, $i \in \Lambda = \{1, 2, \ldots, s\}$. By Proposition 3.3.17$(iii)$, we have $|A_{q_i}(\sigma)| = Q(q_i)$. The next proposition and corollary are identical to the Proposition 3.2.9 and Corollary 3.2.10 in the previous section.

Proposition 3.3.13. *The set* $\bigcap_{i=1}^{l} A_{q_i} = A_{k/p_1 \cdots p_l}$, $1 \leq l \leq s$.

Proof. Similar line of argument as in Proposition 3.2.9. □

Corollary 3.3.14. *Let the set of indices* $\Lambda = \{1, 2, \ldots, s\}$. *For any subset* $\lambda \subseteq \Lambda$,

$$\bigcap_{i \in \lambda} A_{q_i} = A_{(k/\prod_{i \in \lambda} p_i)}.$$

Proof. Similar argument as in Corollary 3.2.10. □

Remark 3.3.15. Cardinality of $\bigcap_{i \in \lambda} A_{q_i}$ is $Q\left(\frac{k}{\prod_{i \in \lambda} p_i}\right)$ for $\lambda \subseteq \Lambda$.

Remark 3.3.16. Let m and n be integers greater than 1 so that $(m, n) = 1$. Let k be a positive divisor of $t = ord_n(m)$. Let $k = \prod_{i=1}^{s} p_i^{r_i}$ be the prime decomposition of k. Following the same argument as Lemma 3.2.12, we have $T_k(\sigma) = A_k(\sigma) - \left(\bigcup_{i=1}^{s} A_{q_i}(\sigma)\right)$ where $q_i = \frac{k}{p_i}$ for all $i = 1, 2, \ldots, s$.

Theorem 3.3.17. *Let* m *and* n *be positive integers greater than* 1 *such that* $(m, n) = 1$. *Let* $\sigma_{m,n}$ *be as defined earlier on the set* S. *Let* $t = ord_n(m)$ *be the order of* $\sigma_{m,n}$. *For a positive divisor* k *of* t, *let* $k = \prod_{i=1}^{s} p_i^{r_i}$ *be prime factorization of* k, *where* p_i *are distinct primes and* r_i *are positive integers. Let* $A_k(\sigma)$, $T_k(\sigma)$ *and* $G(m, n, k)$ *be as defined previously. Then* $|T_k(\sigma)| = G(m, n, k)$. *That is there are exactly* $G(m, n, k)$ *many elements of order* k *in the set* S' *under* $\sigma_{m,n}$.

Proof. For convenience of writing we call $A_k(\sigma) = A_k$ and $T_k(\sigma) = T_k$ for this theorem. By Proposition 3.3.12 we know that $A_k \supseteq T_k$ and $A_k \supseteq A_{q_i}$ for all $i \in \Lambda$. By Remark 3.3.16 we have,

$$T_k = A_k - \left(\bigcup_{i=1}^{s} A_{q_i}\right).$$

Then we have,

$$\begin{aligned}
|T_k| &= \left| A_k - \left(\bigcup_{i=1}^{s} A_{q_i} \right) \right| \\
&= |A_k| - \left| \left(\bigcup_{i=1}^{s} A_{q_i} \right) \right| \\
&= |A_k| - \left(\sum_{i=1}^{s} |A_{q_i}| - \sum_{i<j} |A_{q_i} \cap A_{q_j}| + \sum_{i<j<h} |A_{q_i} \cap A_{q_j} \cap A_{q_h}| - \cdots + (-1)^{s+1} \left| \bigcap_{i=1}^{s} A_{q_i} \right| \right) \\
&= |A_k| - \sum_{i=1}^{s} |A_{q_i}| + \sum_{i<j} |A_{q_i} \cap A_{q_j}| - \sum_{i<j<h} |A_{q_i} \cap A_{q_j} \cap A_{q_h}| + \cdots - (-1)^{s+1} \left| \bigcap_{i=1}^{s} A_{q_i} \right| \\
&= Q(k) - \sum_{i=1}^{s} Q\left(\frac{k}{p_i}\right) + \sum_{i<j} Q\left(\frac{k}{p_i p_j}\right) - \sum_{i<j<h} Q\left(\frac{k}{p_i p_j p_h}\right) + \cdots - (-1)^{s+1} Q\left(\frac{k}{\prod_{i=1}^{s} p_i}\right) \\
&= G(m,n,k)
\end{aligned}$$

□

Corollary 3.3.18. *Let the set up be same as in Theorem 3.3.17. If there exist an element of order k in the set S', then there are exacly $\frac{G(m,n,k)}{k}$ many cycles of length k in the complete factorization of $\sigma_{m,n}$, excluding trivial cycles generated by 0 and n. Also, $n-1 = \sum_{d|t,d>0} G(m,n,d)$.*

Proof. By Theorem 3.3.17, for any positive divisor k of t, we have $|T_k(\sigma)| = G(m,n,k)$. Since element of order k generates a cycle of length k, it follows that there are exactly $\frac{G(m,n,k)}{k}$ many cycles of length k in the complete factorization of $\sigma_{m,n}$. □

Recall that for integers a and $b > 0$, a *div* b is the integer quotient q obtained when a is divided by b.

Corollary 3.3.19. *Let m and n be any positive integer different from 1 so that $(m,n) = 1$. Let $t = ord_n(m)$. Then for any positive divisor k of t, $G(m,n,k) = \sum_{d|k,d>0} \mu(d) Q\left(\frac{k}{d}\right) \equiv 0$ mod k where $Q\left(\frac{k}{d}\right)$ is $(n-1)$ div $\frac{n}{(m^{\frac{k}{d}}-1,n)}$. In particular, $G(m,n,t) \equiv 0$ mod t.*

Proof. Result follows from Corollary 3.3.18. □

Corollary 3.3.20. *Let m and n be positive integers different from 1. For any positive divisor $k > 1$ of n, $F(m,k) = G(m, m^n - 1, k)$.*

Proof. Since $\tau_{m,n}$ is the same permutation as σ_{m,m^n-1}, number of cycles of length k are equal in cycle factorization of both the permutations. Hence $|T_k(\sigma)| = |T_k(\tau)|$. And hence $F(m,k) = G(m, m^n - 1, k)$. In fact,

$$\begin{aligned} G(m, m^n - 1, k) &= \sum_{d|k, d>0} \mu(d) Q\left(\frac{k}{d}\right) \\ &= \sum_{d|k, d>0} \mu(d) \left(m^{k/d} - 2\right) \\ &= \sum_{d|k, d>0} \mu(d) m^{k/d} - 2\left(\sum_{d|k, d>0} \mu(d)\right) \\ &= F(m,k) \end{aligned}$$

□

Example 3.3.21. Revisiting Example 3.3.10, we get following for $\sigma_{5,36}$.

k	b_k	c_k	$Q(k) = \lvert A_k(\sigma)\rvert$	$G(5, 36, k) = \lvert T_k(\sigma)\rvert$
1	4	9	3	3
2	12	3	11	11 - 3 = 8
3	4	9	3	3 - 3 = 0
6	36	1	35	35 - 3 - 11 + 3 = 24

In fact $\sigma_{5,36}$ = (0) (1 5 25 17 13 29) (2 10 14 34 26 22) (3 15)(4 20 28 32 16 8)
(6 30) (7 35 31 11 19 23) (9) (12 24) (18) (21 33) (27) (36)

Note that there are exactly $\frac{24}{6} = 4$ cycles of length 6, $\frac{8}{2} = 4$ cycles of length 2 and $\frac{3}{1} = 3$ cycles of length 1 excluding cycles generated by 0 and 36.

REFERENCES

[1] J. Hull, Subfield-Compatible Polynomials over Finite Fields, *Rose-Hulman Undergraduate Mathematics Journal*, Volume 14, no. 2, 2013

[2] P. B. Bhattacharya, S. K. Jain, and S. R. Nagpaul, *Basic Abstract Algebra*, Cambridge University Press, 1995

[3] J. K. Strayer, *Elementary Number Theory*, Waveland Press, 2001

[4] A. J. Preslicka, The Topology and Algebraic Functions on Affine Algebraic Sets Over an Arbitrary Field *Masters thesis, Georgia State University*, 2012

[5] R. Lidl, *Finite fields*, Cambridge University Press, 1997

[6] R. Lidl, G. Mullen, When does a polynomial over a finite field permute the elements of the field? *American Mathematical Monthly*, JSTOR, 1988

[7] Z. Wan, *Lectures on finite fields and Galois rings*, World Scientific Singapore, 2003

[8] E. Meijering, A chronology of interpolation: from ancient astronomy to modern signal and image processing, *Proceedings of the IEEE*, Volume 90, no. 3, 2002

[9] L. E. Dickson, *History of the Theory of Numbers, vol. 1*, Chelsea, New York, 1966

[10] C. J. Smyth, A coloring proof of a generalisation of Fermat's Little Theorem, *American Mathematical Monthly*, 1986

[11] I. Isaacs, M. Pournaki, Generalizations of Fermat's Little Theorem via Group Theory *American Mathematical Monthly*, JSTOR, 2005

[12] W. A. Stein et al., *Sage Mathematics Software (Version 6.5)*, The Sage Development Team, 2015, `http://www.sagemath.org`.

APPENDIX A

The finite field $\mathbb{F}_{2^6} = \mathbb{F}_2[x]/(f(x))$ where $f(x) = x^6 + x^5 + 1$.

k	a^k	k	a^k
0	0	16	$a^5 + a^3 + a$
1	a	17	$a^5 + a^4 + a^2 + 1$
2	a^2	18	$a^3 + a + 1$
3	a^3	19	$a^4 + a^2 + a$
4	a^4	20	$a^5 + a^3 + a^2$
5	a^5	21	$a^5 + a^4 + a^3 + 1$
6	$a^5 + 1$	22	$a^4 + a + 1$
7	$a^5 + a + 1$	23	$a^5 + a^2 + a$
8	$a^5 + a^2 + a + 1$	24	$a^5 + a^3 + a^2 + 1$
9	$a^5 + a^3 + a^2 + a + 1$	25	$a^5 + a^4 + a^3 + a + 1$
10	$a^5 + a^4 + a^3 + a^2 + a + 1$	26	$a^4 + a^2 + a + 1$
11	$a^4 + a^3 + a^2 + a + 1$	27	$a^5 + a^3 + a^2 + a$
12	$a^5 + a^4 + a^3 + a^2 + a$	28	$a^5 + a^4 + a^3 + a^2 + 1$
13	$a^4 + a^3 + a^2 + 1$	29	$a^4 + a^3 + a + 1$
14	$a^5 + a^4 + a^3 + a$	30	$a^5 + a^4 + a^2 + a$
15	$a^4 + a^2 + 1$	31	$a^3 + a^2 + 1$

k	a^k	k	a^k
32	$a^4 + a^3 + a$	48	$a^3 + a^2 + a + 1$
33	$a^5 + a^4 + a^2$	49	$a^4 + a^3 + a^2 + a$
34	$a^3 + 1$	50	$a^5 + a^4 + a^3 + a^2$
35	$a^4 + a$	51	$a^4 + a^3 + 1$
36	$a^5 + a^2$	52	$a^5 + a^4 + a$
37	$a^5 + a^3 + 1$	53	$a^2 + 1$
38	$a^5 + a^4 + a + 1$	54	$a^3 + a$
39	$a^2 + a + 1$	55	$a^4 + a^2$
40	$a^3 + a^2 + 1$	56	$a^5 + a^3$
41	$a^4 + a^3 + a^2$	57	$a^5 + a^4 + 1$
42	$a^5 + a^4 + a^3$	58	$a + 1$
43	$a^4 + 1$	59	$a^2 + a$
44	$a^5 + a$	60	$a^3 + a^2$
45	$a^5 + a^2 + 1$	61	$a^4 + a^3$
46	$a^5 + a^3 + a + 1$	62	$a^5 + a^4$
47	$a^5 + a^4 + a^2 + a + 1$	63	1

The table has been constructed with the help of SageMathCloud [12] by compiling the following command:

sage: k = GF(2**6, name='a', modulus=$x^6 + x^5 + 1$)

sage: for i,x in enumerate(k): print i,x