8-2009

Discrete Dynamics over Finite Fields

Jang-woo Park
Clemson University, jpark@clemson.edu

Discrete Dynamics over Finite Fields

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematics

---

by
Jang-Woo Park
August 2009

Accepted by:
Dr. Shuhong Gao, Committee Chair
Dr. Neil J. Calkin
Dr. Kevin L. James
Dr. Hiren Maharaj
Dr. Gretchen L. Matthews

Abstract

A dynamical system consists of a set V and a map $f : V \to V$. The primary goal is to characterize points in V according to their limiting behaviors under iteration of the map f. Especially understanding dynamics of nonlinear maps is an important but difficult problem, and there are not many methods available. This work concentrates on dynamics of certain nonlinear maps over finite fields. First we study monomial dynamics over finite fields. We show that determining the number of fixed points of a boolean monomial dynamics is $\#P-complete$ problem and consider various cases in which the dynamics can be explained efficiently. We also extend the result to the monomial dynamics over general finite fields. Then we study the dynamics of a simple nonlinear map, $f(x) = x + x^{-1}$, on fields of characteristic two. The main idea is to lift the map f to a proper finite covering map whose dynamics is easier to understand. We lift the map of f to an isogeny g on an elliptic curve where the dynamics of g can be further reduced to that of a linear map on $\mathbb{Z}-$module. As an application of finite covering, we construct a new family of permutation maps over finite fields from the known permutation maps.

Dedication

To my mother and father,

whose constant and unconditional love has made me who I am.

Acknowledgments

The writing of a dissertation can be a lonely and isolating experience, yet it is obviously not possible without the support and encouragement of numerous people.

First of all, I am very grateful to my doctoral advisor, Dr. Shuhong Gao for his encouragement, advice, mentoring, and research support throughout my doctoral study. I also truly appreciate his patience and tolerance during my numerous mishaps. I also thank my committee members, Dr. Neil Calkin, Dr. Kevin James, Dr. Hiren Maharaj, and Dr. Gretchen Matthews. I am fortunate to have received their time and suggestions for my research over the years. I am especially grateful to Dr. Kevin James for his timely corrections and suggestions that helped make this dissertation better.

I would like to thank Dr. Judith Cottingham and Dr. Timothy Teitloff for writing me recommendation letters regarding my teaching skills. I also thank Professor Eric Bach who showed me how wonderful mathematics is and led me where I am now. I am also grateful to Professor Hendrik W. Lenstra, Jr. for his valuable insight which has been crucial to the main chapter of this work.

I am thankful to numerous friends who supported and nourished me in many different ways. Among them, I am especially thankful to Sundeep Samson, my co-instructor and coffee buddy who made this long procedure enjoyable and encouraged me during a hard time. I also thank Ethan and Andrea Smith for their helps and

kindness. I also thank my officemates through the years, especially Ray Heindl and Mingfu Zhu for countless hours of good conversation. I thank Mr. Woo-Young Ryu, Mr. Sang-Ouk Wee, and Professor Jeong-Han Kim who have been great friends throughout my graduate studies. I am especially grateful to my two best friends, Tae-Hee Lee and Won-Jin Lee who have encouraged me with unfading friendship for decades.

I thank Johann Sebastian Bach for Goldberg Variations which has been both musical and mathematical inspiration to me for long time, Glenn Gould and Dong-Hyek Lim whose interpretations of Goldberg Variations have nourished my soul, and Frédèric Chopin whose brilliant work, Polonaise, Op. 53, has widen my perspective on life. I also thank my favorite guitarists, Pat Metheny, Paul Gilbert, Guthrie Govan and Billy McLaughlin who provided wonderful music with the instrument that I love the most.

Finally, I would like to thank the most important people in my life, my family. I am grateful to my sisters, Young-Woo Park, Jung-Woo Park, Eun-Woo Park for the support and the encouragement. I would also like to thank my aunts and uncles for their prayers. I am deeply indebted to my parents, Chan-Kyo Park and Kum-Soon Kim who have trusted and supported me for my whole life with their unconditional love.

Table of Contents

List of Figures

Chapter 1

Introduction

Dynamical systems are ubiquitous in science and engineering. They may represent the motions of stars in the sky in astronomy, the fluctuation of stock markets in business, the heart beat in medical science, gene evolution in genetics, or traffic in a highway system or in a city. Dynamical systems have long been studied by many scholars in science, engineering, and mathematics, and they are active areas of research full of unknowns and challenges.

In simple terms, a dynamical system consists of a set V and a map $f : V \to V$. We write

$$f^i = \underbrace{f \circ f \circ \cdots \circ f}_{i} = i_{th} \text{ iteration of } f,$$

and f^0 denotes the identity map on V by convention. For a given point $v \in V$, the **orbit of** v **under** f is the set of $f^i(v)$'s for all $i \geq 0$. A point $v \in V$ is called **periodic** or **cyclic** if there exists $m \geq 1$ such that $f^m(v) = v$. In this case, the orbit of v under f is a cycle and the smallest such m is called the cycle length of v. A point $v \in V$ is called **preperiodic** if there exist $0 \leq i < j$ such that $f^i(v) = f^j(v)$. In this case, the orbit of v is depicted as in Figure 1.1. The number i in Figure 1.1 is called **tail**

length and the number $j - i$ is called the **cycle length** of v. In applications, it is desirable to understand cycle lengths, tail lengths, and their distributions.

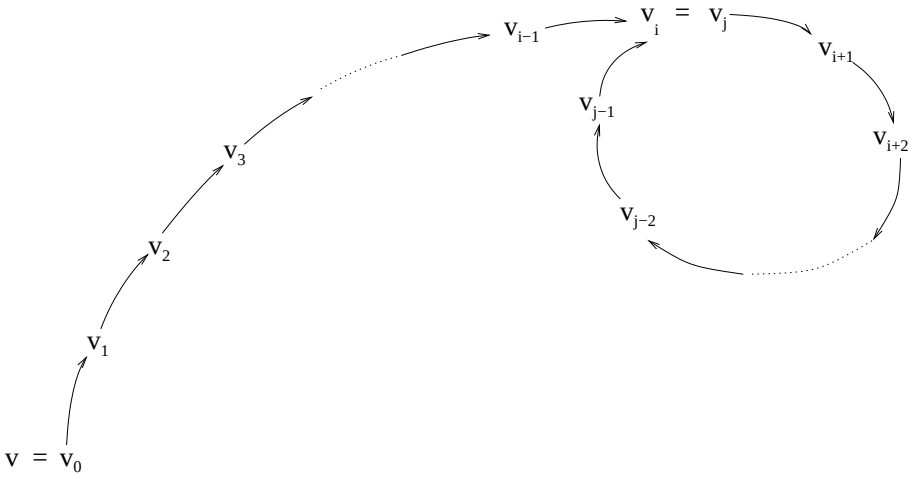


Figure 1.1: Orbit of v under a map f.

In a classical dynamical system, V is a topological and metric space. A point $v \in V$ is called stable if, whenever $u \in V$ is "close" to v, the orbit of u stays "close" to that of v. The **Fatou set** of f consists of all the stable points of V. The **Julia set** of f is the complement of the Fatou set. So points in Julia set tend to move away from each other under iteration of f and they behave chaotically. The important subjects in a classical dynamical system are the limiting behaviors of two close points and finding the Julia set. For more on classical dynamical system, we recommend [Devaney, 2003] and [Robinson, 1998].

Understanding the discrete dynamics on finite sets requires different techniques. When V is finite, every point is preperiodic. So the "stability" and "chaos" in classical dynamical systems are irrelevant in finite dynamical systems. We view the discrete dynamics of f on a finite set V as a directed graph. The graph has V as a vertex set and, for any pair of $v, w \in V$, there is an edge from v to w if and only if $f(v) = w$. Figure 1.2 shows a dynamical system over a finite field.

Example 1.0.1. *Let* $f : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ *be* $f(x_1, x_2, x_3, x_4, x_5) = (x_2x_3, x_1x_4, x_3, x_4, x_4)$. *The dynamics of* f *is shown in Figure 1.2.*

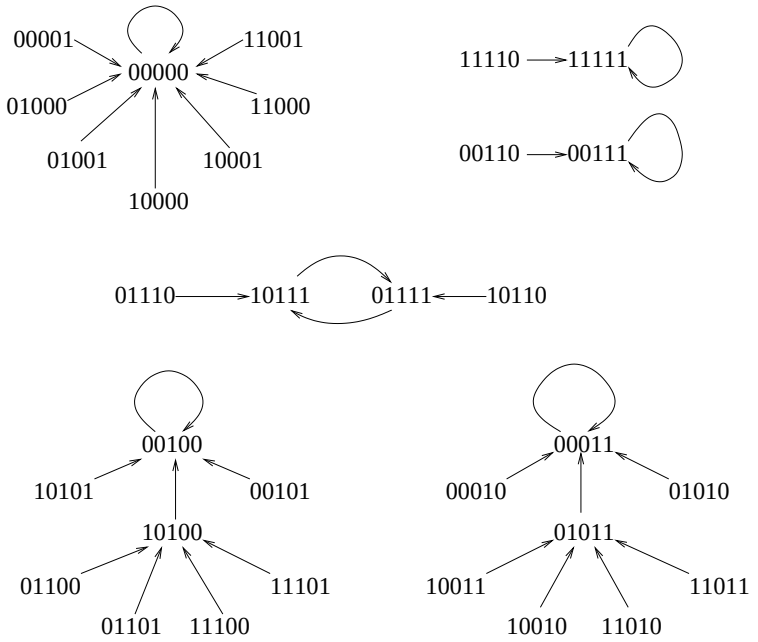


Figure 1.2: Dynamics of f on $\mathbb{F}_2^5$

Notice that the dynamics of f consists of disjoint cycles with trees attached to them. As can be seen in Figure 1.2, it has five fixed points, one cycle of length 2, the maximum tail length is 2, and the maximum in-degree is 8. It is also noticeable that there are regularities in the tree structure. We are interested in dynamics over finite sets, especially over finite fields. We are interested in the following questions:

- How many cycles are in the dynamics of f on V?
- What are the cycle lengths ?
- What are the heights of trees ?
- What are the in-degrees ?

Although we can get answers for all the questions above by enumerating all points, we are interested in the underlying mathematical theory. The goal is to analyze the dynamics without actually enumerating all state transitions, since enumerating has exponential complexity in the number of model variables. In this work, we are particularly interested in monomial dynamics and using finite covering to investigate the dynamics of nonlinear maps over finite fields.

The following is a brief survey of some known results on various discrete dynamics. For linear finite dynamical systems, Elspas [1959] examined the dynamics of linear systems over prime fields and showed that cycle structure can be determined by the elementary divisor of the matrix, and Hernandez-Toledo [2005] generalized Elspas's results to arbitrary finite fields and also showed that tree structure can be determined by the nilpotent part of the map. Based on these results, Jarrah et al. [2006] presented an algorithms which describes the phase spaces. Xua and Zoub [2009] have presented an efficient algorithm to analyze cycle structure of the dynamics of linear systems over finite commutative rings. Studying dynamics of nonlinear maps is very challenging task. Only a few cases have been well understood. Zieve [1996] investigated the cycle lengths of polynomial maps over various rings. Even dynamics of quadratics polynomials over finite fields are still open except $f(x) = x^2$ and $f(x) = x^2 - 2$. The square map over prime fields was studied in [Rogers, 1996] and the dynamics of $f(x) = x^2 - 2$ over prime fields was analyzed in [Gilbert et al., 2001], [Park, 2003], and [Vasiga and Shallit, 2004]. For monomial dynamics, Jarrah et al. [2008] provided an analysis of boolean monomial dynamical systems and Colón-Reyes et al. [2006] showed the structure of fixed points of monomial dynamics over general finite fields can be reduced to boolean monomial dynamics.

A map is called a permutation map if it is bijective on V. Permutation maps have applications in diverse areas such as coding theory, combinatorics, and cryp-

tography. If V is finite, then the dynamics of permutation maps consist of only cycles. Especially for permutation maps over finite fields, due to the fact that every map over a finite field can be expressed by a polynomial, it was natural to focus on maps defined by polynomials. Since Hermite [1863] investigated permutation polynomials over finite prime fields and Dickson [1897] studied them over general finite fields, numerous mathematicians and engineers have shown their interests in permutation polynomials. For more background material on permutation polynomials, we refer the readers to Chapter 7 of [Lidl and Niederreiter, 1997] and, for a detailed survey and some open problems, to [Lidl and Mullen, 1988, 1993]. Two well-known classes of permutation polynomials are monomials x^k over $\mathbb{F}_q$ with $k \geq 1$ and $\gcd(k, q-1) = 1$ and Dickson's polynomials over $\mathbb{F}_q$ with degrees relatively prime to $q^2 - 1$. Binomial polynomials of certain forms have been studied by several scholars; see [Akbary and Wang, 2006], [Masuda et al., 2006], [Masuda and Zieve, 2007, 2009], [Turnwald, 1998], and [Wang, 2002]. For permutation polynomials in more general forms, see [Akbary and Wang, 2005], [Park and Lee, 1998], and [Wan and Lidl, 1991].

In this work we focus on studying dynamics of special nonlinear maps over finite fields and its theoretical application. In Chapter 2, we study monomial dynamics over finite fields. A map f is called a **monomial map** if $f = (f_1, f_2, \ldots, f_m)$ where each f_i is a monomial. Colón-Reyes et al. [2004] studied fixed point structure of f over $\mathbb{F}_2$ by associating the dynamics of f with its dependency graph χ_f. They also introduced a loop number of a strongly connected component which plays important role in their investigation of cycle structure of monomial dynamics in [Jarrah et al., 2008]. Jarrah et al. [2008] proved that a component with the loop number t in χ_f would decompose into t/d components in χ_{f^d} for d dividing t. They showed possible lengths of cycles and their distributions when χ_f has only one component. From this,

they presented lower and upper bound for the number of cycles of a given length for general boolean monomial dynamics. When χ_f has more than one component, the obstacle in studying the exact cycle structure of f is that structure of cycles of length $d \geq 1$ depends on not only how components decompose in χ_{f^d} but also on how components are connected in χ_f. It is even difficult to determine the number of fixed points of boolean monomial dynamics. We show that the problem of counting fixed points of a monomial dynamics over $\mathbb{F}_2$ is $\#P - complete$, for which no efficient algorithm is known. This is proved by a $1-1$ correspondence between fixed points of f and antichains of the poset of strongly connected components of χ_f. We also extend the results of boolean monomial dynamics to monomial dynamics over general finite fields. To determine fixed points of a monomial map f over $\mathbb{F}_q$, we work on zero component and nonzero components separately. We find the zero components by examining the dependency graph of f as done in boolean monomial dynamics. We show how nonzero components of f can be reduced to a linear map over $\mathbb{Z}_{q-1}$ by using logarithmic representation of f. Hence deciding the values of nonzero components of fixed points is equivalent to solving linear systems over $\mathbb{Z}_{q-1}$.

In Chapter 3, we apply finite covering to analyze dynamics of nonlinear maps over finite fields. We are particularly interested in the dynamics of $f(x) = x+x^{-1}$ over $\mathbb{F}_{2^n} \cup \{\infty\}$. We lift f to an isogeny $g = I + \sigma$ on the elliptic curve $E : y^2 + xy = x^3 + 1$ where I is an identity map and σ is the Frobenius map. For a positive integer n, let $E(\mathbb{F}_{2^n})$ be the set of $\mathbb{F}_{2^n}$-rational points of E and $E_p(\mathbb{F}_{2^n})$ a $p - subgroup$ of $E(\mathbb{F}_{2^n})$ where p is a prime. Since $E(\mathbb{F}_{2^n})$ is a finite abelian group, $E(\mathbb{F}_{2^n})$ can be decomposed as direct sum of $E_p(\mathbb{F}_{2^n})$'s where p is a prime dividing $\#E(\mathbb{F}_{2^n})$.

We show that all the tails of g come from the the dynamics g on $E_2(\mathbb{F}_{2^n})$. It is known that $E_2(\mathbb{F}_{2^n})$ is isomorphic to $\mathbb{Z}/(2^{h_2})$ for some h_2. We prove that h_2 is equal to $\nu_2(n) + 2$ and every tree attached to a periodic points is a complete binary tree of

height $\nu_2(n)+1$.

For an odd prime p, g is an automorphism on $E_p(\mathbb{F}_{2^n})$. Hence all cycle lengths are explained by the dynamics of g on $E_p(\mathbb{F}_{2^n})$. Note that $E_p(\mathbb{F}_{2^n})$ is isomorphic to $\mathbb{Z}/(p^{a_p}) \times \mathbb{Z}/(p^{b_p})$ where a_p and b_p depend on the factorization of $\sigma^n - 1$ in $\mathbb{Z}[\sigma]$. We show that the dynamics of g on $E_p(\mathbb{F}_{2^n})$ can be reduced to that of a linear map $M = \left(\begin{smallmatrix} 0 & 1 \\ -2 & 1 \end{smallmatrix}\right)$ on a $\mathbb{Z} - module$. We distinguish three cases:

(a) For $p = 7$, we show that $\#E(\mathbb{F}_{2^n})$ is divisible by 7 if and only $6|n$ and, for that $n = 6 \cdot 7^e \cdot w$ with $e \geq 0$ and $7 \nmid w$, $E_7(\mathbb{F}_{2^n})$ is isomorphic to $\mathbb{Z}/(7^e) \times \mathbb{Z}/(7^{e+1})$. We show that all the cycle lengths of g on $E_7(\mathbb{F}_{2^n})$ can be obtained from the multiplicative order of M modulo 7^c where c runs from 1 to $e+1$.

(b) For odd prime p's with $\left(\frac{p}{7}\right) = -1$, we show that $E_p(\mathbb{F}_{2^n})$ is isomorphic to $\mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$ with $e = \nu_p(\#E(\mathbb{F}_{2^n}))/2$ and the dynamics of g on $E_p(\mathbb{F}_{2^n})$ is identical to that of M over $\mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$.

(c) For odd prime p's with $\left(\frac{p}{7}\right) = 1$, it is difficult to analyze the cycle lengths of g on $E_p(\mathbb{F}_{2^n})$ because the structure of $E_p(\mathbb{F}_{2^n})$ can be arbitrary. But we show that when $E_p(\mathbb{F}_{2^n})$ is isomorphic to $\mathbb{Z}/(p^e)$, g on $E_p(\mathbb{F}_{2^n})$ can be reduced to a multiplication map on $\mathbb{Z}/(p^e)$, and when $E_p(\mathbb{F}_{2^n})$ is isomorphic to $\mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$, the dynamics of g on $E_p(\mathbb{F}_{2^n})$ is identical to that of M on $\mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$.

Using this information, we show that, in the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$, the length of a cycle projected from an even cycle in the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ is the half of the cycle length and the length of a cycle projected from an odd cycle has the same cycle length. We also show that there are three different tail structures in the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$:

(a) The tree structure attached to ∞ is as follows: a complete binary tree of height

$\nu_2(n)$ is attached to 0 and 0 is attached to ∞.

(b) Structure of a tree projected from a tree attached to a periodic point $P = (x, y) \in E(\mathbb{F}_{2^{2n}})$ with $x \in \mathbb{F}_{2^n}$, $y \notin \mathbb{F}_{2^n}$ is a tree of height 0.

(c) Structure of a tree projected from a tree attached to a periodic point $P \in E(\mathbb{F}_{2^n}) \setminus \{\mathcal{O}\}$ is a complete binary tree of height $\nu_2(n) + 1$.

In Chapter 4, we present an interesting application of finite coverings. We construct a new family of permutation maps over finite fields with odd characteristic from the known family of permutation maps using finite covering. The key idea is that we project $n-th$ power map g using a proper projection map π which is different from one used to construct Dickson's polynomials and obtain a new family of maps h satisfying $\pi \cdot g = h \cdot \pi$. We show the exact condition for new maps to be permutation maps.

Finally in Chapter 5, we recapitulate the results given in this work and consider the possible questions for future research.

Chapter 2

Monomial Dynamics over Finite Fields

2.1 Introduction

For this chapter, we focus on the case when $V = \mathbb{F}_q^n$ and the map $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is defined by

$$f = (f_1, f_2, \ldots, f_n)$$

where

$$f_i = c_i \cdot x_1^{m_{i1}} x_2^{m_{i2}} \cdots x_n^{m_{in}}, \quad 1 \leq i \leq n,$$

with $c_i \in \mathbb{F}_q$ and $m_{ij} \in \mathbb{N}$. Then f is called a monomial map over $\mathbb{F}_q$ and the dynamics f a **monomial dynamics**.

Since our work extends that of Colón-Reyes et al. [2004]; Jarrah et al. [2008], we will use their definitions and basic setup in most of cases. We associate f with a digraph χ_f, called the **dependency graph of** f which has vertex set $\{1, 2, \ldots, n\}$, and there is a directed edge from j to i if and only if $c_i \neq 0$ and $x_j | f_i$. Note that j is

adjacent to i if and only if the value of x_j affects f_i and we allow self-loops in χ_f.

Example 2.1.1. *Let f be defined over $\mathbb{F}_2$ as*

$$f = (x_2, x_3x_4, x_2, x_5x_{12}, x_6, c, x_8x_{11}, x_3x_9, x_{10}, x_6, x_9, x_{12})$$

where c in $\mathbb{F}_2$. The dependency graph χ_f of f is as follows:

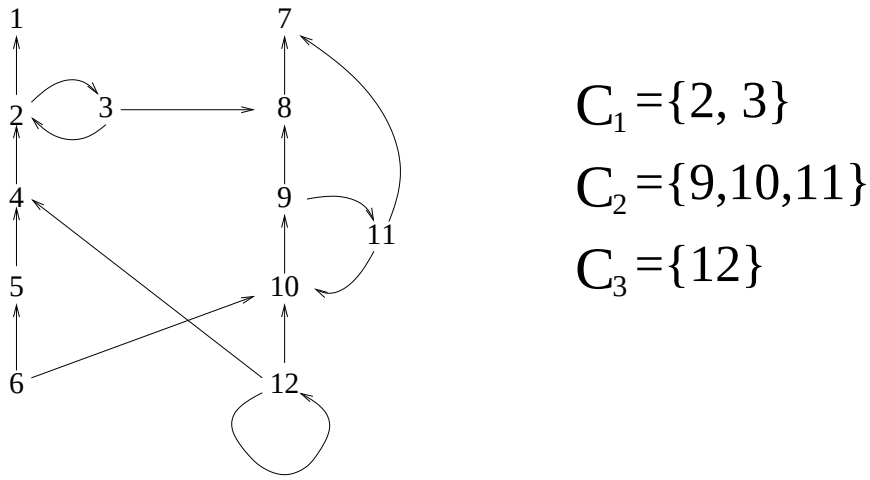


Figure 2.1: Dependency Graph χ_f of f and its Strongly Connected Components

When $c = 1$, the fixed points of f are :

$$(1,1,1,1,1,1,1,1,1,1,1,1),$$

$$(0,0,0,1,1,1,0,0,1,1,1,1),$$

$$(1,1,1,1,1,1,0,0,0,0,0,1),$$

$$(0,0,0,0,1,1,0,0,0,0,0,0),$$

$$(0,0,0,1,1,1,0,0,0,0,0,1).$$

When $c = 0$, the fixed points of f are :

$$(0,0,0,0,0,0,0,0,0,0,0,0),$$
$$(0,0,0,0,0,0,0,0,0,0,0,1).$$

Let χ be any digraph. For any two vertices $i, j \in \chi$, if there is a **directed path**, or **dipath** for short, from i to j and a dipath from j to i then we say i and j are **strongly connected**. A subset of vertices is called strongly connected if each pair of vertices in the subset is strongly connected. Any maximal strongly connected subset of vertices of χ is called a **strongly connected component** of χ, or simply a **component** of χ. Note that a vertex itself is a component if and only if it has a self-loop.

Note that different components of χ have disjoint vertices, and there may be vertices in χ that do not lie on any component. For any vertex i not on any component, either there is a dipath from i to some component or there is a dipath from some component to i, but not both. Similary, for any two components, if there are paths for one component to the other, then there is no path going to the opposite direction. We say a component C_1 is above, or greater than, another component C_2 if there is a dipath from C_2 to C_1. This makes the set of all the components of χ into a **partially ordered set**, i.e., a **poset**.

Example 2.1.1.(revisited). *Suppose that we have the dependency graph χ_f as in Figure 2.1.1. Then, for $c = 1$, the poset is as in Figure 2.1.*

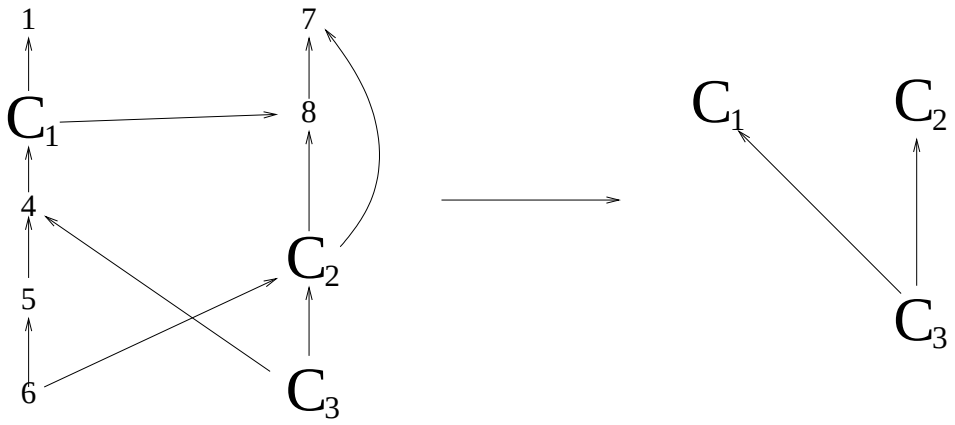


Figure 2.2: Poset of the Dependency Graph χ_f

Let G be a set. A partial order is a binary relation " $\leq$ " over G which satisfies reflexive, antisymmetric, and transitive. With a partial order, G is called a partially ordered set. A pair of elements x and y in G are comparable if $x \leq y$ or $y \leq x$. A subset A of G is called an **antichain** if no two elements in A are comparable. Note that the empty subset is an antichain and any singleton subset is an antichain as well.

Example 2.1.2. *Suppose that G is as below:*

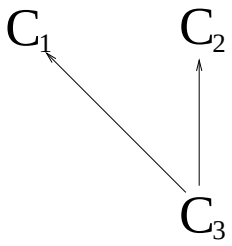


Figure 2.3: Poset of the Strongly Connected Components of χ_f

Then all the possible antichains of G are:

$$\emptyset\ ,\ \{C_1\}\ ,\ \{C_2\}\ ,\ \{C_3\}\ ,\ \textit{and}\ \ \{C_1, C_2\}.$$

Note that G in Figure 2.1.2 is obtained from the poset of the dependency graph χ_f in Figure 2.1 by considering only components. For a given dependency graph χ_f of f, we define G_f as the poset of strongly connected components in χ_f and we call G_f the **component poset** of χ_f. Let A be a subset of a partially ordered set G. A is **upper closed** if for any $x \in A$ and $y \in G$, $x \leq y$ implies that $y \in A$ too. Similarly, A is **lower closed** if for any $x \in A$ and $y \in G$, $x \geq y$ implies that $y \in A$ too. Let k be an arbitrary field. For any point $P = (a_1, a_2, \ldots, a_n) \in k^n$, we define subsets $S_0(P)$ and $S_1(P)$ of χ_f as

$$S_0(P) = \{1 \leq i \leq n : a_i = 0\}, \quad S_1(P) = \{1 \leq i \leq n : a_i \neq 0\}.$$

Then fixed points of monomial dynamics have the following unique property.

Proposition 2.1.1. *Let k be an arbitrary field and $f : k^n \to k^n$ be a monomial map. Suppose $P = (a_1, a_2, \ldots, a_n) \in k^n$ is a fixed point of f. Then $S_0(P)$ is upper closed and $S_1(P)$ is lower closed.*

Proof. Since $P = f(P)$, for each j in the dependency graph χ_f, we have $a_j = f_j(P)$. For any vertex i that has an edge to j, if $a_i = 0$ then $a_j = 0$. Also, if $a_j \neq 0$ then $a_i \neq 0$ for all vertices i adjacent to j. The proposition follows by chasing the dipaths in χ_f. □

This property gives us a different way to recognize fixed points of monomial dynamics and we will investigate the structure of fixed points using this property.

2.2 Fixed Points over $\mathbb{F}_2$

In this section, we study how to find all fixed points of the dynamics of a given map f over $\mathbb{F}_2$ and delve into the related combinatorial problems.

Theorem 2.2.1. *Let $f = (f_1, f_2, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let χ_f be the dependency graph of f. Assume that no f_i's are constant. Then there exists a $1-1$ correspondence between the set of fixed points of f and the set of antichains of the component poset G_f of χ_f.*

Proof. Suppose P is a fixed point of f. Then, by Proposition 2.1.1, $S_1(P)$ is lower closed. So the set of maximal strongly connected components among the strongly connected components contained in $S_1(P)$ forms an antichain. Now, suppose A is an antichain of the component poset. Then, for all $1 \leq i \leq n$, set $j_i = 0$ if $j_i \geq C$ for some $C \in A$ and set $j_i = 1$ otherwise. Let $P_A = (j_1, j_2, \ldots, j_n)$. Note that if $j_i = 0$, then since $j = 0$ for all $j \geq j_i$, $f_i(P_A) = 0$. Also, if $j_i = 1$, then since $j = 1$ for all $j \leq j_i$, $f_i(P_A) = 1$. This implies that $f(P_A) = P_A$, i.e. P_A is a fixed point. □

Example 2.1.1.(revisited). *Suppose that f is defined in Example 2.1.1. Recall that we have already seen the component poset G_f of χ_f in Figure 2.1.2 and the corresponding antichains. From this, we can find all the fixed points of f:*

$$
\begin{aligned}
\emptyset &\longleftrightarrow (1,1,1,1,1,1,1,1,1,1,1,1),\\
\{C_1\} &\longleftrightarrow (0,0,0,1,1,1,0,0,1,1,1,1),\\
\{C_2\} &\longleftrightarrow (1,1,1,1,1,1,0,0,0,0,0,1),\\
\{C_3\} &\longleftrightarrow (0,0,0,0,1,1,0,0,0,0,0,0),\\
\{C_1, C_2\} &\longleftrightarrow (0,0,0,1,1,1,0,0,0,0,0,1).
\end{aligned}
$$

So, if we can compute the number of antichain of the component poset, then we know the number of fixed points of given boolean monomial dynamics.

Definition 2.2.1 (Valiant [1979])**.** *$\#P$ is the class of functions that can be computed by counting Turing machines of polynomial time complexity.*

A problem is $\#P - complete$ if and only if it is in $\#P$, and every problem in $\#P$ can be reduced to it by a polynomial-time counting reduction. There is no known algorithms to solve $\#P - complete$ problem efficiently. Provan and Ball [1983] showed that computing the number of antichains of given poset is a $\#P - complete$ problem and Knuth and Ruskey [2003] studied some special cases where the counting can be done efficiently. In the following, we present a simple algorithm to count the number of antichains of a given poset.

2.2.1 Counting the Number of Antichains of a Poset

Let G be a poset and $\tau(G)$ be the number of antichains of G. Note that any subset of a poset is a poset too. Then there are two basic properties of the number of antichains. First, if G is a disjoint union of G_1 and G_2, then

$$\tau(G) = \tau(G_1) \cdot \tau(G_2).$$

Suppose $v \in G$. Then

$$\tau(G) = \tau(G_1) + \tau(G_2)$$

where G_1 and G_2 are defined as following:

- $G_1 = G \setminus \{u \in G : u \text{ comparable to } v\}$ and
- $G_2 = G \setminus \{v\}$, but keeps the connections.

The following example will clarify the definitions of G_1 and G_2.

Example 2.2.1. *Suppose that a poset G is as following:*

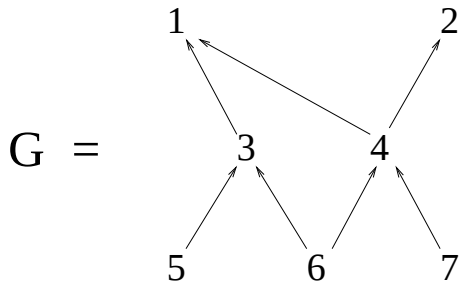


Figure 2.4: Poset G

If we pick the vertex 3*, then the corresponding G_1 and G_2 are as in Figure 2.5:*

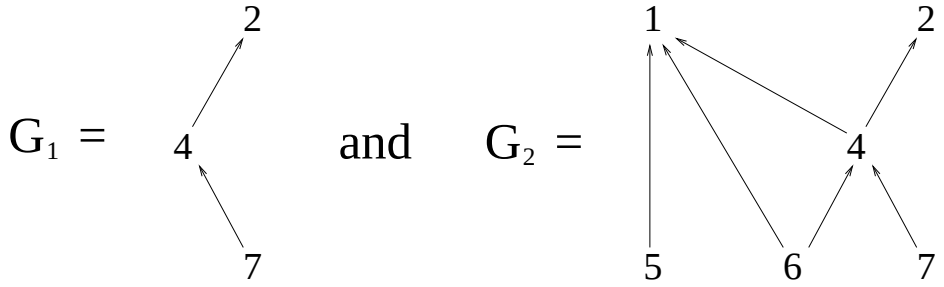


Figure 2.5: G_1 and G_2 for the Vertex 3 of G

Note that if G is a tree of height 1 with n leaves, then $\tau(G) = 1 + 2^n$. Thus, with these properties, we can develop a recursive algorithm for counting the number of antichains in any poset.

- *Algorithm 1*

Input : a poset G.

Output : $\tau(G)$ (= the number of antichains).

$ALG_1(G)$:

1. If G is a tree of height 1 with n leaves, then **return** $(1 + 2^n)$.

2. Pick any maximal(or minimal) element $v \in G$. Define G_1 and G_2 as follows:

   - $G_1 := G \setminus \{u \in G : u < v\}$(or $G \setminus \{u \in G | u > v\}$, respectively).
   - $G_2 := G \setminus \{v\}$.

3. **return** $(ALG_1(G_1) + ALG_1(G_2))$.

End of $ALG_1(G)$ Note that using maximal or minimal element in the above algorithm does not change the result or the performance of the algorithm. Although counting the number of antichains is generally known as a difficult problem, there are certain cases in which we can count it efficiently [Knuth and Ruskey, 2003]. Here, we list some of those special types of posets.

1. Suppose that T is a tree. T is called a complete $n - ary$ tree of height h if if every node of T except leaves has the same in-degree, n, and every leaf has the same depth, h. Let $T(n, h)$ be a complete $n - ary$ tree of height h. Then the properties above gives us the linear time algorithm to count the number of antichains of the tree $T(n, h)$. Let $u \in T(n, h)$ be the root. Then since it is $n - ary$ complete tree, there are n $T(n, h-1)$'s attached to u. Thus

$$\tau(T(n, h)) = 1 + (\tau(T(n, h-1)))^n.$$

   Same reasoning works for a inverted complete $n - ary$ tree of height h. Here is an example of a complete $n - ary$ tree. For instance, consider $T(3, 3)$, a complete tertiary tree of height 3 in Figure 2.6. Using the above recurrence

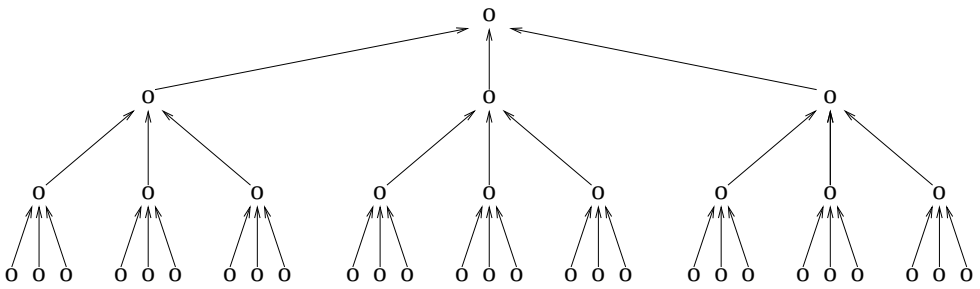


Figure 2.6: Complete Tertiary Tree of height 3

relation, we have

$$\tau(T(3,3)) = 1 + (\tau(T(3,2)))^3 = 1 + \left(1 + (\tau(T(3,1)))^3\right)^3$$
$$= 1 + \left(1 + \left(1 + 2^3\right)^3\right)^3 = 389017001.$$

2. For positive integers m and n, define $M(m,n)$ by a $m-$*partite* graph where each level has n vertices and each level is completely connected only with adjacent levels. $M(4,3)$ is shown in Figure 2.7. Then, by choosing a vertex in the highest(or lowest level), we have

$$\tau(M(m,n)) = 2^{n-1}+2^{n-2}+\ldots+2+1+\tau(M(m-1,n)) = 2^n-1+\tau(M(m-1,n)).$$

Thus

$$\tau(M(m,n)) = (m-1)(2^n-1) + \tau(M(1,n)).$$

Note that $G(1,n)$ is just a poset with n singletons. So

$$\tau(M(m,n)) = (m-1)(2^n-1) + 2^n = m \cdot 2^n - m + 1.$$

Then using the above formula, we know

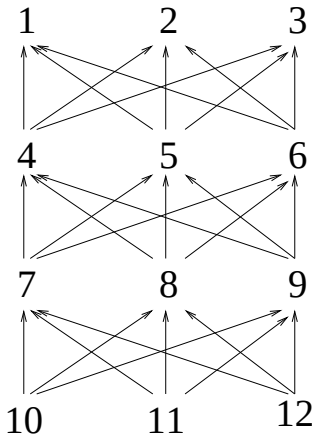


Figure 2.7: Special Quadripartite Graph

$$\tau(M(4,3)) = 4 \cdot 2^3 - (4-1) = 29.$$

2.3 Cycles of Lengths Greater than One over $\mathbb{F}_2$

In this section, we want to discuss how to determine cycles of length greater than one in boolean monomial dynamics. Note that if f has a cycle of length m, then f^m has m new fixed points which are not fixed points of f. This implies that the dependency graph of f^m has more components than that of f. To be precise, we need to study when components of χ_f can be decomposed into smaller components of f^m. The dependency graph of f^m will be denoted by χ_{f^m}. Note that if a vertex is not on any component of χ_f, then it is not on any component of χ_{f^m}. Hence all components of χ_{f^m} come from those of χ_f.

The following example shows the difficulty of studying cycle structure of the dynamics of f when χ_f has more than one component.

Example 2.3.1. *Suppose we have the following dependency graphs χ_f and χ_g.*

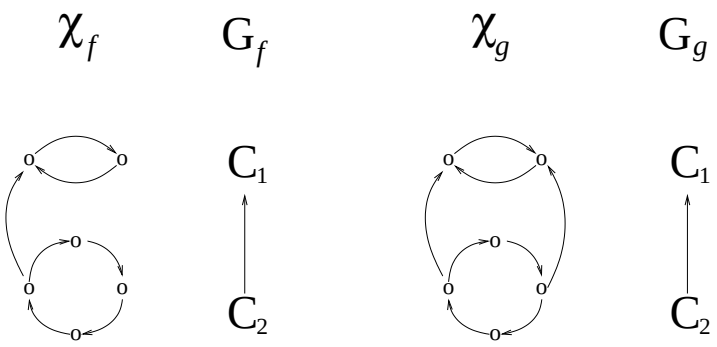


Figure 2.8: Dependency Graphs of f and g

As we see in Figure 2.3.1, the component posets G_f and G_g are identical. This implies that, in this example, the set of fixed points are same in both dynamics. Now consider the dependency graphs of f^2 and g^2.

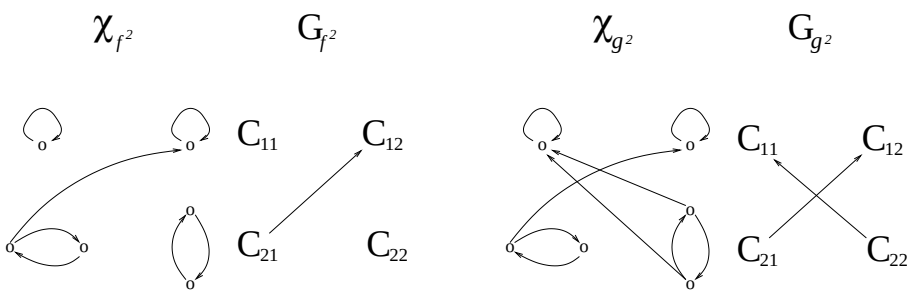


Figure 2.9: Dependency Graphs of f^2 and g^2

Although f and g have the same fixed points, the cycle structure of f and g are different since the component posets G_{f^2} and G_{g^2} are different.

Example 2.3.1 shows that to find out the component poset G_{f^m}, we need precise information on how vertices are connected to others in χ_f. In the rest of this chapter, we focus on the case when χ_f has only one component. To investigate further, we need the following definition.

Definition 2.3.1 (Loop Number [Colón-Reyes et al., 2004])**.** *The loop number of a vertex $v \in \chi_f$ is the minimum of all numbers $t \geq 1$ where $t = |p| - |q|$ for all closed walks $p, q : v \to v$. If there is no closed walk from v to v then we set the loop number to be zero.*

It was also shown in [Colón-Reyes et al., 2004] that all elements in a component have the same loop number, which implies that the loop number is a property of the component.

Example 2.3.2. *Suppose a component C is as follows:*

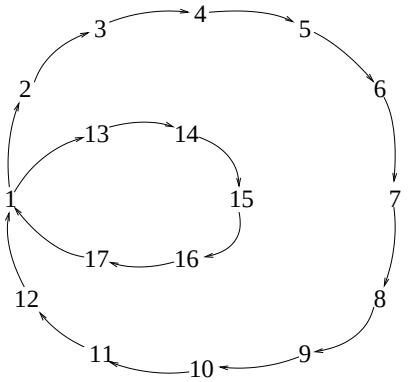


Figure 2.10: Component C

By the definition, the loop number of C is 6.

Proposition 2.3.1. *Suppose $a \in \chi_f$ and its loop number is t. Then, for any two loops l_1 and l_2, passing through a,*

$$|l_1| \equiv |l_2| \pmod{t}.$$

Proof. Without loss of generality, assume that $|l_1| > |l_2|$. Since the loop number is t, there exists closed walks c_1 and c_2 such that $|c_1| - |c_2| = t$. Suppose that $|l_1| - |l_2| = kt + \alpha$ where $0 \leq \alpha < t$. Then we have two closed walks $l_1 + kc_2$ and $l_2 + kc_1$ from a to a,

$$\begin{aligned} |l_1 + kc_2| - |l_2 + kc_1| &= |l_1| + k|c_2| - |l_2| - k|c_1| \\ &= (|l_1| - |l_2|) - k(|c_1| - |c_2|) \\ &= kt + \alpha - kt \\ &= \alpha. \end{aligned}$$

By the minimality of the loop number, we have $\alpha = 0$, hence $|l_1| - |l_2| \equiv 0 \pmod{t}$. $\square$

Definition 2.3.2. *Let $a, b \in \chi_f$. Then directed distance from a to b, denoted by $d(a, b)$, is the length of the shortest path from a to b. We define $d(a, b) = \infty$ if there is no path from a to b.*

Lemma 2.3.2. *Let C be a component of χ_f with loop number t. We define a relation between any two vertices $a, b \in C$ by*

$$a \sim b \quad \text{if } d(a, b) \equiv 0 \pmod{t}.$$

Then $\sim$ is the equivalence relation on C.

Proof. Let c_1 and c_2 be closed walks from a to a with $|c_1| - |c_2| = t$ throughout the proof. For any loop $p : a \to a$, suppose that $|p| = d(a, a) = kt + \alpha$ where $0 \leq \alpha < t$. Then we have closed walks $p + kc_2$ and kc_1 with

$$|p + kc_2| - |kc_1| = |p| - k(|c_1| - |c_2|) = kt + \alpha - kt = \alpha.$$

By the minimality of the loop number, we have $\alpha = 0$. Hence every loop passing through a has length 0 modulo t. In particular, $d(a, a) = 0$.

Suppose that $a \sim b$. Then, by the definition, $d(a, b) \equiv 0 \pmod{t}$. We want to show that $d(b, a) \equiv 0 \pmod{t}$. Let $p_1 : a \to b$ with $|p_1| = k_1 t$ and $p_2 : b \to a$ with $|p_2| = d(b, a)$. Then $p_1 + p_2$ is a loop from a to a. Recall that $|p_1 + p_2| \equiv 0 \pmod{t}$, which implies $|p_2| \equiv 0 \pmod{t}$. Hence $d(b, a) \equiv 0 \pmod{t}$.

Now, suppose $a \sim b$ and $b \sim c$ for $a, b, c \in C$, i.e., there exist a path p_1 from a to b with $|p_1| = d(a, b) = k_1 t$ and a path p_2 from b to c with $|p_2| = d(b, c) = k_2 t$. Let p be any path from c to a. Then we have a loop $p_1 + p_2 + p_3$ from a to a and $|p_1 + p_2 + p| = |p_1| + |p_2| + |p| \equiv 0 \pmod{t}$. Hence, $d(c, a) \equiv 0 \pmod{t}$. □

Now partition C according to its loop number t. Pick $c \in C$ and let C_i be

$$C_i = \{a \in C : d(a, c) \equiv i \pmod{t}\}.$$

It is easy to see that for any $a_1, a_2 \in C$, $a_1 \sim a_2$ if and only if $a_1, a_2 \in C_i$ for some i. Thus C can be decomposed as

$$C = C_0 \cup C_1 \cup C_2 \cup \ldots \cup C_{t-1}.$$

From the definition of C_i's, we can see that the first t steps of the walk from c to itself decides the decomposition and these subcomponents C_i's will not change with the different choice of c. Moreover, for any $a \in C_i$, there exists $b \in C_{i+1}$ such that $d(a, b) = 1$.

Example 2.3.2.(revisited). *Recall that the loop number of C is 6. We can decompose C into two classes as following:*

$$C = C_0 \cup C_1 = \{1, 3, 5, 7, 11, 14, 16\} \cup \{2, 4, 6, 8, 10, 12, 13, 15, 17\}.$$

Theorem 2.3.3. *Each component of the dependency graph χ_f with loop number t decomposes into d components in χ_{f^m} with loop number t/d where $d = \gcd(m, t)$ and the loop number of newly generated components is t/d.*

Proof. This comes directly by the properties of the equivalence classes and the above decomposition. □

Theorem 2.3.3 says that to find out cycles of length greater than 1, it is enough to look at χ_f^m where $\gcd(m, t) > 1$. Thus, to find out cycles of length > 1, we do not have to look χ_{f^m} for all $m > 1$. It is enough to consider χ_{f^m} and the poset of χ_{f^m} for

m such that $m \leq t$ and $\gcd(m, t) > 1$ where t is the loop number of some component in χ_{f^m}. Theorem 3.8. in [Jarrah et al., 2008] showed the number of points of certain period, equivalently the number of cycles of certain length. Here we present simpler proof for the number of cycles of a given length dividing the loop number.

Theorem 2.3.4. *Suppose χ_f has only one component C with the loop number t and k is a positive integer which divides t. Let $\ell(k)$ be the number of cycles whose lengths are exactly k. Then*

$$\ell(k) = \frac{1}{k} \cdot \sum_{d|k} \mu(d) 2^{\frac{dt}{k}}.$$

Proof. For any d, k that divide t, let $A(d)$ be the set of periodic points of period of d as defined in [Jarrah et al., 2008]. Since the set of cycles of length d is pairwise disjoint, $A(d) = d \cdot \ell(d)$. From [Jarrah et al., 2008, Lemma 3.6.], we know

$$\sum_{d|k} d \cdot \ell(d) = \bigcup_{d|k} A(d) = 2^k.$$

Then Móbius inversion gives us

$$k \cdot \ell(k) = \sum_{d|t} \mu(d) 2^{\frac{k}{d}}.$$

Hence

$$\ell(k) = \frac{1}{k} \cdot \sum_{d|k} \mu(d) 2^{\frac{k}{d}}.$$

□

2.4 Monomial Dynamics over General Finite Fields

In this section, we study monomial dynamics over general finite fields. Even though we can apply many techniques that we discussed in the previous chapters, there is limitation to them. Thus, we will study what the difficulties for general finite fields are and how we approach this problem. Note that for cycles of lengths greater than 1, we can convert the problem to finding fixed points of f^m for $m > 1$, we will focus on finding fixed points of f.

Let q be a power of an odd prime and $f = (f_1, f_2, \ldots, f_n) : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a monomial map. Then, for each $i = 1, \ldots, n$,

$$f_i = c_i \cdot x_1^{m_{i1}} x_2^{m_{i2}} \cdots x_n^{m_{in}} = \gamma^{b_i} \cdot x_1^{m_{1i}} x_2^{m_{2i}} \cdots x_n^{m_{ni}}$$

where γ is a primitive element of $\mathbb{F}_q$. Without loss of generality, we assume that $f_i \neq 0$ for all $1 \leq i \leq n$. Since any non-zero element in $\mathbb{F}_q$ can be represented as a certain power of γ, we can take log on both sides and obtain

$$\log_\alpha f_i \equiv b_i + \sum_{j=1}^{n} m_{ij} \cdot \log_\gamma x_j \pmod{q-1}.$$

Let $A = \Big(m_{ij}\Big) \in \mathbb{N}^{n \times n}$. Now we can express the monomial map $f = (f_1, f_2, \ldots, f_n)$ as a matrix representation.

$$\big(\log_\gamma f_1, \log_\gamma f_2, \ldots, \log_\gamma f_n\big) = (b_1, b_2, \ldots, b_n) + \big(\log_\gamma x_1, \log_\gamma x_2, \ldots, \log_\gamma x_n\big) \cdot A.$$

We also write this as

$$\log_\gamma f = b + \log_\gamma x \cdot A$$

where $b = (b_1, b_2, \ldots, b_n), \log_\gamma x = (\log_\gamma x_1, \log_\gamma x_2, \ldots, \log_\gamma x_n)$. Observe that

$$\begin{aligned}
f &\longleftrightarrow b + \log_\gamma x \cdot A, \\
f^2 &\longleftrightarrow b(I + A) + \log_\gamma x \cdot A^2, \\
f^3 &\longleftrightarrow b(I + A + A^2) + \log_\gamma x \cdot A^3, \\
&\vdots \\
f^k &\longleftrightarrow b(I + A + A^2 + \ldots + A^{k-1}) + \log_\gamma x \cdot A^k.
\end{aligned}$$

Next we show how this can be used to find the fixed points of f. Note that we can still find which coordinates are zero in a fixed point by examining the poset of χ_f just as we did over $\mathbb{F}_2$ by using Proposition 2.1.1. After choosing the nonzero components, we need to show how to find the actual values. Without loss of generality, we demonstrate below how to find fixed points x that are nonzero on all components. We call such fixed points nontrivial fixed points. Then a point x is a nontrivial fixed point of f if and only if it satisfies

$$\log_\gamma x \equiv b + \log_\gamma x \cdot A \pmod{q-1},$$

i.e.,

$$\log_\gamma x \cdot (I - A) \equiv b \pmod{q-1}. \tag{2.1}$$

Let $M = I - A$. Then since $\mathbb{Z}/(q-1)$ is a principal ideal domain, we know that there

exists invertible matrices $P, Q \in \mathbb{Z}_{q-1}^{n\times n}$ such that

$$P \cdot M \cdot Q \equiv D \equiv \begin{pmatrix} d_1 & & & & & & \\ & \ddots & & & & & \\ & & d_l & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 \end{pmatrix} \pmod{q-1}$$

where $d_i | q-1$ and $d_i | d_j$ for all $i \leq j$. The matrix D is called a Smith-Normal Form. Thus (2.1) implies that

$$\log_\gamma x \cdot P^{-1} \cdot D \equiv b \cdot Q \pmod{q-1}.$$

Let $y = \log_\gamma x \cdot P^{-1}$ and $\tilde{b} = b \cdot Q$. Then, since P is invertible, x is a fixed point of f if and only the corresponding y is the solution to $y \cdot D = \tilde{b} \pmod{q-1}$. The system has solution if and only if

$$\begin{cases} d_i | \tilde{b_j} & \text{for } 1 \leq i \leq r, \\ 0 \equiv \tilde{b_j} \pmod{q-1} & \text{for } r+1 \leq i \leq n. \end{cases}$$

Thus finding nontrivial fixed points is equivalent to solving the linear equation over a ring provided discrete log problem is relatively easy on given finite field, i.e., this approach works efficiently when $|\mathbb{F}_q|$ is small. Here is an example which explains how to find non-trivial fixed points with this approach.

Example 2.4.1. *Let a monomial dynamical system* $f : \mathbb{F}_5^3 \to \mathbb{F}_5^3$ *be*

$$f(x_1, x_2, x_3) = (x_2, x_1^2 x_2^3 x_3^2, 3x_1^3 x_2^2).$$

Then the dependency graph χ_f *of* f *has only one component so that there is only one trivial fixed point,* $(0, 0, 0)$.

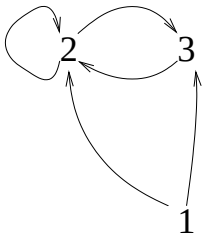


Figure 2.11: Dependency Graph χ_f of f.

Now we want to find nontrivial fixed points of f. *Note that* $\mathbb{F}_5^\times =< 2 >$. *Thus, using the above idea, this monomial system can be represented as the following linear equation:*

$$\log_2 f = (0, 0, 3) + \log_2 x \begin{pmatrix} 0 & 2 & 3 \\ 1 & 3 & 2 \\ 0 & 2 & 0 \end{pmatrix},$$

i.e.,

$$\log_2 f = b + \log_2 x \cdot A.$$

Fixed points of f *satisfy*

$$\log_2 x = b + \log_2 x \cdot A.$$

Let

$$M = I - A = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 2 & 2 \\ 0 & 2 & 1 \end{pmatrix}.$$

Then

$$P \cdot M \cdot Q \equiv D \pmod 4$$

where

$$P = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}, Q = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 2 \end{pmatrix}, \text{ and } D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Note that $\tilde{b} = b \cdot Q \equiv (1, 0, 2) \pmod 4$. *Since* $y \cdot D \equiv (y_1, y_2, 2y_3) \pmod 4$, *the solutions to* $y \cdot D \equiv \tilde{b} \pmod 4$ *are*

$$y = (1, 0, 1) \text{ and } (1, 0, 3).$$

Then $\log_2 x = (1, 1, 0)$ *and* $(3, 3, 2)$, *i.e., the nontrivial fixed points are*

$$x = (2, 2, 1) \text{ and } (3, 3, 4).$$

Note that ring $\mathbb{Z}/(q-1)$ has zero-divisors. Thus it is possible that the dynamics of a given map does not have nontrivial fixed points. The following two examples will show such cases with different reasons.

Example 2.4.2. *Let a monomial dynamical system* $f : \mathbb{F}_5^3 \to \mathbb{F}_5^3$ *be*

$$f(x_1, x_2, x_3) = (x_2, x_1^2 x_2 x_3^2, 3x_1^3 x_2^2).$$

Note that this map is obtained by small modification of the map in Example 2.4.1 and, indeed, the dependency graph of f and its component poset is the same with that given in Example 2.4.1. With the same approach, this monomial system can be represented as the following linear equation:

$$\log_2 f = (0,0,3) + \log_2 x \begin{pmatrix} 0 & 2 & 3 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{pmatrix},$$

i.e.,

$$\log_2 f \equiv b + \log_2 x \cdot A \pmod 4.$$

Fixed points satisfy

$$\log_2 x \equiv b + \log_2 x \cdot A \pmod 4.$$

Let

$$M = I - A = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}.$$

Then

$$P \cdot M \cdot Q \equiv D \pmod 4$$

where

$$P = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}, Q = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 2 \end{pmatrix}, \text{ and } D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Note that $\tilde{b} = b \cdot Q \equiv (1,0,2) \pmod 4$. *Since* $y \cdot D \equiv (y_1, y_2, 0) \pmod 4$, *there is no*

$y \in \mathbb{Z}_4^3$ *satisfying*

$$y \cdot D \equiv (1, 0, 2) \pmod 4.$$

Hence there is no nontrivial fixed points.

Here is the example of dynamics which has no non-trivial fixed points due to the scalar.

Example 2.4.3. *Let a monomial dynamical system* $f : \mathbb{F}_5^3 \to \mathbb{F}_5^3$ *be*

$$f(x_1, x_2, x_3) = (x_2, 3x_1^2x_2^3x_3^2, 3x_1^3x_2^2).$$

To obtain this map, we altered the constant coefficient of f_2 *of the map in Example 2.4.1. Thus the linear equation representing the given systems will be identical except* b*. So we have*

$$\log_2 f = (0, 3, 3) + \log_2 x \begin{pmatrix} 0 & 2 & 3 \\ 1 & 3 & 2 \\ 0 & 2 & 0 \end{pmatrix},$$

i.e.,

$$\log_2 f = b + \log_2 x \cdot A.$$

From Example 2.4.1, we already know that $\tilde{b} = b \cdot Q \equiv (1, 0, 1) \pmod 4$ *and* $y \cdot D \equiv (y_1, y_2, 2y_3) \pmod 4$*. Since* 2 *is not invertible in* $\mathbb{Z}_4$*, there is no* $y \in \mathbb{Z}_4^3$ *such that*

$$y \cdot D \equiv (1, 0, 1) \pmod 4.$$

Hence there is no non-trivial fixed points.

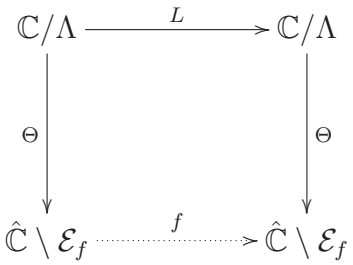
Chapter 3

Finite Coverings

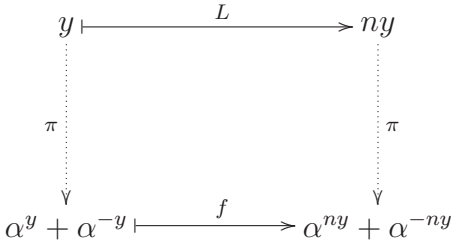
3.1 Introduction

The idea of finite coverings originated from the holomorphic dynamics literature. In this section, we would like to give a brief explanation of it and present examples of dynamical systems over finite fields which can be explained by it. For more general information, it is recommended to read "On the Lattè's Map" by J. Milnor in [Hjorth and Petersen, 2006]. Let f be a rational map of degree two or more from the Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ to itself and $\mathcal{E}_f$ be the set of all points with finite grand orbit under f. f is called a **finite quotient of an affine map** if there exists a discrete additive subgroup Λ of $\mathbb{C}$, an affine map $L : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$, and a finite-to-one holomorphic map $\Theta : \mathbb{C}/\Lambda \to \hat{\mathbb{C}} \setminus \mathcal{E}_f$ such that the following diagram is

commutative:



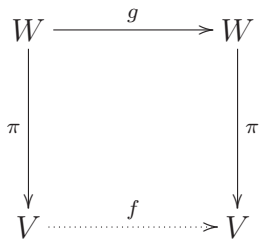
The commutativity of the diagram implies that each orbit of a point in $\mathbb{C}/\Lambda$ is projected by Θ to an orbit of a point in $\hat{\mathbb{C}} \setminus \mathcal{E}_f$ and since L is an affine map, its dynamics are "simpler" than that of f. Especially, when every point in $\hat{\mathbb{C}} \setminus \mathcal{E}_f$ has preimages in $\mathbb{C}/\Lambda$, we say the dynamics of L on $\mathbb{C}/\Lambda$ covers that of f on $\hat{\mathbb{C}} \setminus \mathcal{E}_f$. This provides a great tool to study dynamics of rational maps. Finite quotients of affine maps can be classified as powermaps, Chebyshev maps, and Lattè's maps according to their Julia sets. These three classes can be well extended to over finite fields and the dynamics of them on finite fields can be explained easily. For example, let $\mathbb{F}_q$ be a finite field of q elements where q is a power of prime. It is easy to see that the dynamics of n-th power map on $\mathbb{F}_q^\times$ is covered by that of the multiplication by n on $\mathbb{Z}/(q-1)$ which can be analyzed effortlessly. For Chebyshev maps over finite fields, suppose $L : \mathbb{Z}/(q^2-1) \to \mathbb{Z}/(q^2-1)$ by $L(y) = ny$ for $y \in \mathbb{Z}/(q^2-1)$ and $\pi(y) = \alpha^y + \alpha^{-y}$ where α is a generator of $\mathbb{F}_{q^2}^\times$. Then we have the following commutative diagram:



Notice that the image of π contains $\mathbb{F}_q$ and f is the n-th degree Chebyshev polynomial. As π is a $2-$*cover*, which is the reason to use the quadratic extension, any odd cycle

of L projects via π to a cycle of f of the same length and any even cycle of L projects to a cycle of half length. The cycle lengths of L are the orders of n modulo m where $m|(q^2-1)$. Therefore, the cycle lengths of the n-th degree Chebyshev polynomial on $\mathbb{F}_q$ are determined by the orders of n modulo m with m running through the divisors of q^2-1.

When we restrict V to a finite field, holomorphicity is not defined. There is a possibility that we have maps which are not finite quotients of affine maps but whose dynamics can be explained by this idea. We can generalize this idea as follows: Let V and W be algebraic varieties and $f : V \to V$ and $g : W \to W$ be morphisms. Then g is called an **n-covering of** f if there exists a map $\pi : W \to V$ where for any $x \in V$, $|\pi^{-1}(x)| = n$ (counting multiplicity) such that the following diagram is commutative:



Thus our main concern is to study the dynamics of f over V by exploring a proper covering space W, a covering morphism g, and the projection map π and studying the dynamics of g over W. In the following, we present a map which is not a finite quotient of an affine map over $\mathbb{C}$, but whose dynamics can be analyzed by finite covering.

3.2 A Dynamical System and its Associated Elliptic Curve

Let $f : \mathbb{F}_{2^n} \cup \{\infty\} \to \mathbb{F}_{2^n} \cup \{\infty\}$ be a map defined as

$$f(x) = \begin{cases} x + x^{-1} & \text{if } x \in \mathbb{F}_{2^n}^{\times}, \\ \infty & \text{if } x = 0 \text{ or } \infty. \end{cases}$$

Figure 3.1, Figure 3.2, and Figure 3.3 show the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$ for different values of n.

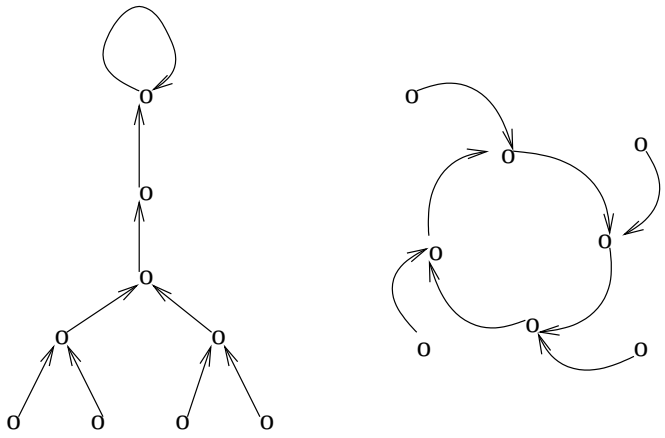


Figure 3.1: Dynamics of $f(x) = x + x^{-1}$ on $\mathbb{F}_{2^4} \cup \{\infty\}$.

As we see in the figures, the dynamics of f show regularities in structures of cycles and trees. H.W. Lenstra, Jr. observed that f can be covered by dynamics of a certain isogeny on a Koblitz curve [Koblitz, 1991]. More precisely, let E be the elliptic curve group over the algebraic closure $\overline{\mathbb{F}}_2$ defined by

$$E : y^2 + xy = x^3 + 1. \tag{3.1}$$

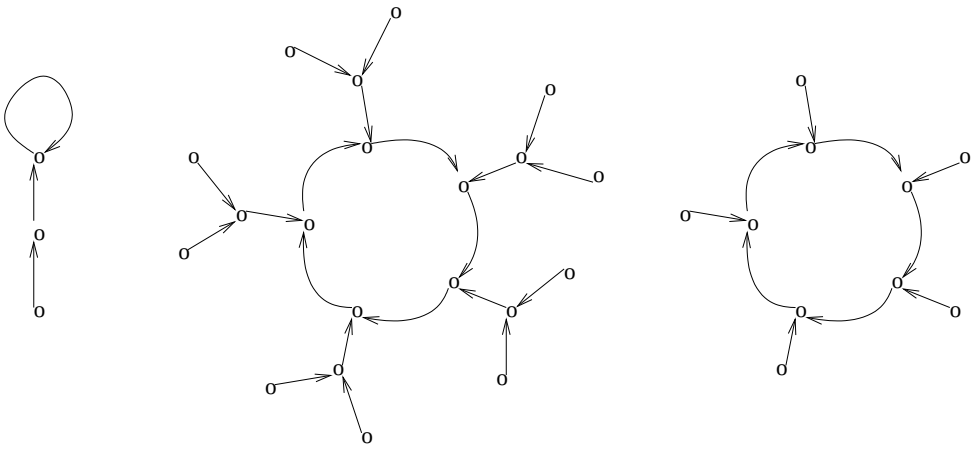


Figure 3.2: Dynamics of $f(x) = x + x^{-1}$ on $\mathbb{F}_{2^5} \cup \{\infty\}$.

Then, with the point $\mathcal{O}$ at the infinity, E forms an abelian group with respect to the addition of points defined as following [Silverman, 1986, Group Law Algorithm 2.3.]: $\mathcal{O}$ is an identity in E. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. If $P \neq \mathcal{O}$, then $-P = (x_1, y_1 + x_1)$. Suppose $Q \neq -P$. Then $P + Q = (x_3, y_3)$ where

$$x_3 = \begin{cases} (\frac{y_1+y_2}{x_1+x_2})^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 & \text{if } P \neq Q, \\ x_1^2 + \frac{1}{x_1^2} & \text{if } P = Q. \end{cases}$$

and

$$y_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + x_3 + y_1 & \text{if } P \neq Q, \\ x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3 & \text{if } P = Q. \end{cases}$$

Let $\sigma : E \to E$ be the Frobenius morphism, that is, for $P = (x, y) \neq \mathcal{O}$, $\sigma(x, y) = (x^2, y^2)$. Define a map $g : E \to E$ by $g(P) = P + \sigma(P)$ where $+$ is the addition of points on the curve. Note that, for $P = (x, y) \neq \mathcal{O}$,

$$g(x, y) = (I + \sigma)(x, y) = (x, y) + (x^2, y^2) = (x', y'),$$

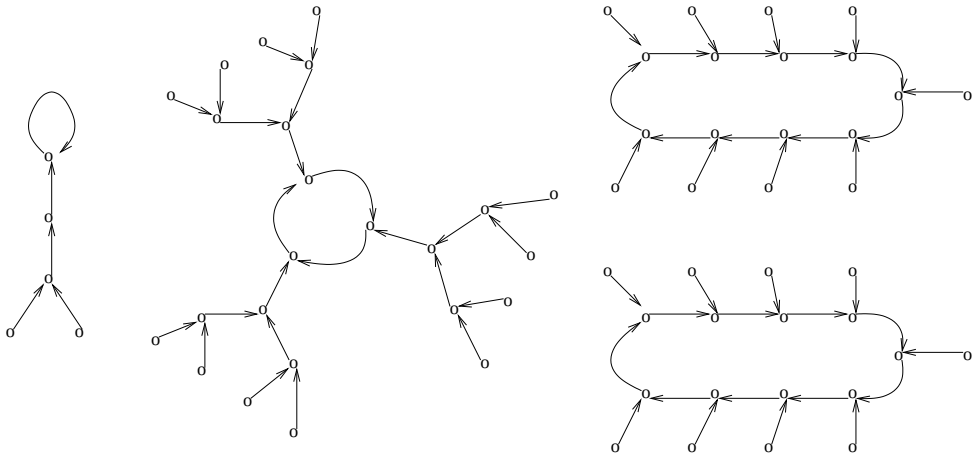


Figure 3.3: Dynamics of $f(x) = x + x^{-1}$ on $\mathbb{F}_{2^6} \cup \{\infty\}$.

where $x' = x + x^{-1}$ and

$$y' = \begin{cases} x^2 + 1 + \frac{1}{x^2} + y + \frac{y}{x^2} & \text{if } (x,y) \neq (x^2, y^2), \\ x + 1 + \frac{1}{x} + y + \frac{y}{x} & \text{if } (x,y) = (x^2, y^2). \end{cases} \tag{3.2}$$

Thus we have the following commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{\quad g \quad} & E \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \pi} \\ \overline{\mathbb{F}}_2 \cup \{\infty\} & \xrightarrow{\quad f \quad} & \overline{\mathbb{F}}_2 \cup \{\infty\} \end{array}$$

where the projection map π is defined as

$$\pi(P) = \begin{cases} x & \text{if } P = (x,y) \neq \mathcal{O}, \\ \infty & \text{if } P = \mathcal{O}. \end{cases}$$

Let $E(\mathbb{F}_{2^{2n}})$ be the set of $\mathbb{F}_{2^{2n}}$-rational points of E. Since for any $x \in \mathbb{F}_{2^n} \cup \{\infty\}$, $\pi^{-1}(x) \in E(\mathbb{F}_{2^{2n}})$, the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ covers that of f on $\mathbb{F}_{2^n} \cup \{\infty\}$. Moreover, g is an isogeny of E, i.e., a group homomorphism on E. This enables us to focus on the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ to understand that of f on $\mathbb{F}_{2^n} \cup \{\infty\}$.

Throughout this chapter, E will denote the elliptic curve as defined in (3.1), $End(E)$ denotes the ring of group endomorphism, $m - torsion$ group of E over algebraic closure is denote by $E[m]$, and, for a field k, $E(k)[m]$ denotes $E[m] \cap E(k)$. For a rational prime p, $E_p(k)$ denotes $p - subgroup$ of $E(k)$, i.e., the order of any elements in $E_p(k)$ is a power of p.

3.3 Properties of g on E

Since I and σ are endomorphisms of E, so is g. Thus $g(P+Q) = g(P)+g(Q)$. One can check that the minimum polynomial $m_\sigma(T)$ of σ is

$$m_\sigma(T) = T^2 + T + 2 \in \mathbb{Z}[T].$$

So the minimum polynomial g is $m_g(T) = T^2 - T + 2 \in \mathbb{Z}[T]$, i.e.,

$$g^2 - g + 2 = 0 \tag{3.3}$$

as a map on E. Since $(0,1)$ is the only point of order 2 and $\mathcal{O}$ is the only fixed point of g, one can show that $\ker g = \{\mathcal{O}, (0,1)\}$. Then we have the following recurrence relation: for any $n \geq 1$,

$$\begin{pmatrix} g^n \\ g^{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} g^{n-1} \\ g^n \end{pmatrix}.$$

Let

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

Then, for any $n \geq 0$ and $P \in E$,

$$\begin{pmatrix} g^n(P) \\ g^{n+1}(P) \end{pmatrix} = M^n \begin{pmatrix} P \\ g(P) \end{pmatrix}. \tag{3.4}$$

Thus the dynamics of g depends on the behavior of M and the subgroups $< P >$ and $< g(P) >$ of E. The following propositions show the basic properties of g.

Proposition 3.3.1. *For any point $P \in E$ with odd order, $g(P)$ has the same order.*

Proof. Suppose the order of P is m which is odd. Since $mP = \mathcal{O}$, $g(mP) = mg(P) = \mathcal{O}$, the order ℓ of $g(P)$ divides m. Also, $g(\ell P) = \ell g(P) = \mathcal{O}$, so ℓP is in the kernel of g. If $\ell P = (0, 1)$, then $2\ell P = \mathcal{O}$, i.e., $2\ell | m$, which contradicts that m is odd. Thus $\ell P = \mathcal{O}$. Hence, $\ell = m$. □

Proposition 3.3.2. *Suppose $P \in E$ and $|P| = m$ with m even. Then $|g(P)| = \frac{m}{2}$.*

Proof. Let $m = 2\ell$. Then

$$mP = 2(\ell P) = \mathcal{O}.$$

Since $(0, 1)$ is the only point of order 2, $\ell P = (0, 1)$. Thus

$$\ell g(P) = g(\ell P) = g((0, 1)) = \mathcal{O},$$

i.e., ℓ divides $|g(P)|$. Note that $|g(P)| < \ell$ implies that $|P| < 2\ell$. Hence, the order of $g(P) = \ell$. □

Proposition 3.3.1 and Proposition 3.3.2 tell us that $E[m]$ is $g - invariant$ for any positive integer m. Although it is enough to consider the group structure of $E(\mathbb{F}_{2^{2n}})$ for our purpose, we investigate the group structure of $E(\mathbb{F}_{2^n})$ for any $n \geq 1$.

3.4 Group Structure of $E(\mathbb{F}_{2^n})$

Suppose

$$\#E(\mathbb{F}_{2^n}) = \prod_p p^{h_p}$$

where p's are rational primes and $h_p \geq 1$. Since $E(\mathbb{F}_{2^n})$ is a finite abelian group, $E(\mathbb{F}_{2^n})$ is decomposed as

$$E(\mathbb{F}_{2^n}) = E_2(\mathbb{F}_{2^n}) + \bigoplus_{p \neq 2} E_p(\mathbb{F}_{2^n})$$

where $E_p(\mathbb{F}_{2^n})$ is $p-$*subgroup* of $E(\mathbb{F}_{2^n})$. As proved in Section 3.3, $E_p(\mathbb{F}_{2^n})$ is $g-$*invariant*. Thus we study the structure of $E_p(\mathbb{F}_{2^n})$ for each prime divisor p of $\#E(\mathbb{F}_{2^n})$. By Theorem 3 in [Rück, 1987],

$$E_2(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(2^{h_2})$$

where $h_2 = \nu_2(n) + 2$, i.e., $E_2(\mathbb{F}_{2^n})$ is a cyclic group of order 2^{h_2}. We will explore the size of $E_2(\mathbb{F}_{2^n})$ in depth in Section 3.5. Now we focus on $E_p(\mathbb{F}_{2^n})$ for $p \neq 2$ rational prime dividing $\#E(\mathbb{F}_{2^n})$. Theorem 3 in [Rück, 1987] also says

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{a_p}) \times \mathbb{Z}/(p^{h_p - a_p})$$

where $0 \leq a_p \leq h_p$.

Recall that $\sigma^2 + \sigma + 2 = 0$ as a map on E. So $\mathbb{Q}(\sigma) \cong \mathbb{Q}(\sqrt{-7})$. Moreover, since $\mathbb{Z}[\sigma]$ is the ring of integers for $\mathbb{Q}(\sigma)$, $End(E) = \mathbb{Z}[\sigma]$. $\mathbb{Z}[\sigma]$ is, in fact, a PID.

Lemma 3.4.1 ([Rück, 1987])**.** *Let m be a positive odd integer. Then $E[m] \subseteq E(\mathbb{F}_{2^n})$ if and only if $\sigma^n - 1 = m \cdot w \in End(E)$ where $w \in End(E)$.*

Proof. Suppose $E[m] \subseteq E(\mathbb{F}_{2^n})$. Then the kernel of multiplication by m is contained in the kernel of $\sigma^n - 1$. Since multiplication by m is separable [Silverman, 1986, Corallary 5.4.], the universal mapping property for Abelian varieties [Weil, 1948, Proposition 10.] shows that $\sigma^n - 1 = m \cdot w$ where $w \in End(E)$.

Suppose $\sigma^n - 1 = w \cdot m \in End(E)$. For any point $P \in E[m]$, $(\sigma^n - 1)(P) = w(mP) = w\mathcal{O} = \mathcal{O}$, which implies that $P \in E(\mathbb{F}_{2^n})$. Thus $E[m] \subseteq E(\mathbb{F}_{2^n})$. □

The factorization of $\sigma^n - 1$ gives us information on the structure of $E(\mathbb{F}_{2^n})$. In this section, we analyze the structure of $E(\mathbb{F}_{2^n})$ by studying the factorization of $\sigma^n - 1$ in $\mathbb{Z}[\sigma]$. For our purpose, we denote $\nu_{\mathfrak{p}}(\cdot)$ the valuation corresponding to a prime $\mathfrak{p}$ in $\mathbb{Z}[\sigma]$. For a rational prime p and for any $\alpha + \beta\sigma \in \mathbb{Z}[\sigma]$ with $\alpha, \beta \in \mathbb{Z}$, we define $\nu_p(\alpha + \beta\sigma)$ by

$$\nu_p(\alpha + \beta\sigma) = \min(\nu_p(\alpha), \nu_p(\beta))$$

where $\nu_p(\cdot)$ is the valuation of $\mathbb{Z}$ corresponding to p.

Lemma 3.4.2. *Let $p \in \mathbb{Z}$ be a rational prime with $p \neq 2$. Suppose $\sigma^n - 1 = p^t \cdot w \in \mathbb{Z}[\sigma]$ where $p \nmid w$. Then*

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{a_p}) \times \mathbb{Z}/(p^{b_p})$$

with $a_p = t$ and $b_p = t + \nu_p(w\bar{w})$ where $\bar{w}$ is the conjugate of w in $\mathbb{Z}[\sigma]$.

Proof. Suppose $\sigma^n - 1 = p^t \cdot w \in \mathbb{Z}[\sigma]$ where $p \nmid w$. Then Lemma 3.4.1 implies that $E[p^t] \subseteq E(\mathbb{F}_{2^n})$, but $E[p^{t+1}] \not\subseteq E(\mathbb{F}_{2^n})$. From Corollary 6.4.(b) in Silverman [1986], we know that

$$E[p^t] \cong \mathbb{Z}/(p^t) \times \mathbb{Z}/(p^t).$$

Note that $E(\mathbb{F}_{2^n}) = \ker(\sigma^n - 1)$ by definition. So

$$\begin{aligned}
\#E(\mathbb{F}_{2^n}) &= \#\ker(\sigma^n - 1) \text{ (by [Silverman, 1986, III.5.5. and III.4.10.c.])} \\
&= deg(\sigma^n - 1) \text{ (by [Silverman, 1986, III.6.1.])} \\
&= (\sigma^n - 1)(\overline{\sigma}^n - 1)
\end{aligned}$$

where $\overline{\sigma}$ is the dual isogeny of σ. Thus

$$\#E(\mathbb{F}_{2^n}) = (\sigma^n - 1)(\overline{\sigma}^n - 1) = (p^t \cdot w)(p^t \cdot \overline{w}) = p^{2t} \cdot w\overline{w}.$$

This implies that $\nu_p(\#E(\mathbb{F}_{2^n})) = 2t + \nu_p(w\overline{w})$. Since $E_p(\mathbb{F}_{2^n})$ contains $E[p^t]$ but not $E[p^{t+1}]$,

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{a_p}) \times \mathbb{Z}/(p^{b_p})$$

where $a_p = t$ and $b_p = t + \nu(w\overline{w})$. □

Thus, to determine a_p for each p, we need to know the factorization of $\sigma^n - 1$ in $\mathbb{Z}[\sigma]$.

Lemma 3.4.3. *Suppose $\mathfrak{p} \subseteq \mathbb{Z}[\sigma]$ is prime and n_0 is the smallest natural number such that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) = e$ with $e \geq 1$. Then $\nu_{\mathfrak{p}}(\sigma^n - 1) \geq e$ if and only if $n_0 | n$.*

Proof. Write n as $n = an_0 + r$ where $0 \leq r \leq n_0 - 1$. Since $\sigma^{n_0} \equiv 1 \pmod{\mathfrak{p}^e}$, we have

$$\sigma^n = \sigma^{an_0+r} = (\sigma^{n_0})^a \sigma^r \equiv \sigma^r \pmod{\mathfrak{p}^e}.$$

Thus $\sigma^n \equiv 1 \pmod{\mathfrak{p}}$ if and only if $\sigma^r \equiv 1 \pmod{\mathfrak{p}}$. Since n_0 is the smallest such that $\sigma^{n_0} \equiv 1 \pmod{\mathfrak{p}}$, $r = 0$. Hence, $n_0 | n$. □

For $e = 1$, we have the following useful corollary.

Corollary 3.4.4. *Suppose $\mathfrak{p} \subseteq \mathbb{Z}[\sigma]$ is prime and n_0 is the smallest natural number such that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) > 0$. Then $\nu_{\mathfrak{p}}(\sigma^n - 1) > 0$ if and only if $n_0 | n$.*

Note that the proof of Lemma 3.4.3 is still valid if $\mathfrak{p}$ is replaced by any ideal in $\mathbb{Z}[\sigma]$. Thus we have the following corollary too.

Corollary 3.4.5. *Suppose that $p \neq 2$ is a rational prime and n_0 is the smallest natural number such that $p | (\sigma^{n_0} - 1)$. Then $p | (\sigma^n - 1)$ if and only if $n_0 | n$.*

Lemma 3.4.6. *Suppose that $p \neq 2$ is a rational prime and n is the smallest natural number such that $\nu_p(\sigma^n - 1) = e$ where $n \geq 1$ and $e \geq 1$. Then the smallest $n' > n$ such that $\nu_p(\sigma^{n'} - 1) > e$ is pn. Moreover, $\nu_p(\sigma^{pn} - 1) = e + 1$.*

Proof. Since $\nu_p(\sigma^n - 1) = e$,

$$\sigma^n \equiv 1 + c \cdot p^e \pmod{p^{e+1}}$$

where $p \nmid c$. It is easy to see that

$$\sigma^{pn} \equiv 1 + c \cdot p^{e+1} \pmod{p^{e+2}},$$

i.e., $\nu_p(\sigma^{pn} - 1) = e + 1$. Suppose n' is the smallest such that $\nu_p(\sigma^{n'} - 1) > e$. From Lemma 3.4.3, $n' = kn$ with $1 \leq k \leq n$. Note

$$\sigma^{kn} \equiv 1 + ck \cdot p^e \pmod{p^{e+2}}.$$

So, $\nu_p(\sigma^{kn} - 1) > e$ if and only if $p | k$, i.e., $k = p$. Hence, $n' = pn$ and $\nu_p(\sigma^{pn} - 1) = e + 1$. □

Lemma 3.4.7. *Let p be an odd prime and n_0 is the smallest natural number such that $p|(\sigma^{n_0}-1)$. Suppose that $p|(\sigma^n-1)$ and $n = n_0 p^e n'$ where $p \nmid n'$. Then $\nu_p(\sigma^n-1) = e + \nu_p(\sigma^{n_0}-1)$.*

Proof. By applying Lemma 3.4.6, we know that $n_0 p^e$ is the smallest natural number such that $\nu_p(\sigma^{n_0 p^e}-1) = e + \nu_p(\sigma^{n_0}-1)$. Since $p \nmid n'$, from the proof of Lemma 3.4.6,

$$\nu_p(\sigma^n-1) = \nu_p(\sigma^{n_0 p^e}-1) = e + \nu_p(\sigma^{n_0}-1).$$

□

Lemma 3.4.8. *Suppose $\mathfrak{p} \subseteq \mathbb{Z}[\sigma]$ is prime above an odd rational prime p and n is the smallest such that $\nu_{\mathfrak{p}}(\sigma^n-1) = e$ with $e \geq 1$. Then the smallest natural number m such that $\nu_{\mathfrak{p}}(\sigma^m-1) > e$ is pn where $l \in \mathbb{Z}$ is a prime below $\mathfrak{p}$. Moreover, for any n with $\nu_{\mathfrak{p}}(\sigma^n-1) = e \geq 1$, if p does not ramify, then*

$$\nu_{\mathfrak{p}}(\sigma^{pn}-1) = e+1,$$

and if p ramifies and $\nu_{\mathfrak{p}}(\sigma^n-1) \geq 3$, then

$$\nu_{\mathfrak{p}}(\sigma^{pn}-1) = e+2.$$

Proof. From Corollary 3.4.4, we know that $n|m$. Let $m = kn$ where $k \geq 2$. Then

$$\sigma^m - 1 = \sigma^{kn} - 1 = (\sigma^n)^k - 1 = (\sigma^n - 1)(\sigma^{(k-1)n} + \cdots + \sigma^n + 1).$$

Since $\sigma^n \equiv 1 \pmod{\mathfrak{p}}$,

$$B = \sigma^{(k-1)n} + \cdots + \sigma^n + 1 \equiv k \pmod{\mathfrak{p}}. \tag{3.5}$$

Thus $\nu_{\mathfrak{p}}(B) > 0$ if and only if $\nu_{\mathfrak{p}}(k) > 0$, and the smallest such k is p.

Suppose p does not ramify. Then either $(p) = \mathfrak{p}$ or $(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}}$, then $\nu_{\mathfrak{p}}(p) = 1$ in either case. Suppose that $\nu_p(\sigma^n - 1) = 1$. Then $\sigma^n = 1 + c$ where $\nu_{\mathfrak{p}}(c) = 1$. Since p is odd,

$$\begin{aligned} \sigma^{pn} &= (1+c)^p \\ &\equiv 1 + c \cdot p \pmod{\mathfrak{p}^3}. \end{aligned}$$

Note that if p does not ramify, then $\nu_{\mathfrak{p}}(p) = 1$. So we know that

$$c \cdot p \in \mathfrak{p}^2 \text{ but } c \cdot p \notin \mathfrak{p}^3.$$

Thus $\nu_p(\sigma^{pn} - 1) = 2$.

Suppose $\nu_{\mathfrak{p}}(\sigma^n - 1) = e \geq 2$. In (3.5), for $k = p$,

$$\nu_{\mathfrak{p}}(B) = 1.$$

Then

$$\nu_{\mathfrak{p}}(\sigma^n - 1) = \nu_{\mathfrak{p}}(\sigma^n - 1) + \nu_{\mathfrak{p}}(B) = e + 1.$$

Now suppose p ramifies, i.e., $(p) = \mathfrak{p}^2$ in $\mathbb{Z}[\sigma]$ and $e \geq 3$. Then since $\nu_{\mathfrak{p}}(B) = 2$,

$$\nu_{\mathfrak{p}}(\sigma^n - 1) = \nu_{\mathfrak{p}}(\sigma^n - 1) + \nu_{\mathfrak{p}}(B) = e + 2.$$

This completes the proof. □

By Theorem 3.4.1. in [Milne, 2009], we know that, for a rational prime $p \neq 2$,

$$\begin{cases} (p) \text{ ramifies in } \mathbb{Z}[\sigma] & \text{if and only if } p = 7, \\ (p) \text{ splits in } \mathbb{Z}[\sigma] & \text{if and only if } \left(\frac{p}{7}\right) = 1, \\ (p) \text{ stays prime in } \mathbb{Z}[\sigma] & \text{if and only if } \left(\frac{p}{7}\right) = -1. \end{cases}$$

In the following, we study the subgroup structure according to each of the above cases.

3.4.1 Structure of $E_7(\mathbb{F}_{2^n})$

Note that (7) ramifies in $\mathbb{Z}[\sigma]$. In fact, $(7) = \mathfrak{p}^2$ where $\mathfrak{p} = (\sigma - 3, 7)$ is prime in $\mathbb{Z}[\sigma]$. Suppose that $\sigma^n - 1 = 7^x \cdot w$ where $x \geq 0$ and $w \in \mathbb{Z}[\sigma]$ and $7 \nmid w$. From now on, for a rational prime p, $\mathrm{Ord}_p(\alpha)$ denotes the multiplicative order of α modulo p where α can be an integer or integer matrix and, for an ideal I contained a ring R and an element $\alpha \in R$, $\mathrm{Ord}_{\mathfrak{p}}(\alpha)$ denotes the multiplicative order of α modulo I.

Lemma 3.4.9. *Let $\mathfrak{p} = (\sigma - 3, 7)$. Then the smallest natural number such that $\sigma^{n_0} \equiv 1 \pmod{\mathfrak{p}}$ is 6.*

Proof. Note $\sigma \equiv 3 \pmod{\mathfrak{p}}$ and $\mathrm{Ord}_{\mathfrak{p}}(3) = \mathrm{Ord}_7(3) = 6$. This completes the proof. □

Theorem 3.4.10. *Suppose that $\mathfrak{p} = (\sigma - 3, 7)$, the prime in $\mathbb{Z}[\sigma]$ above (7). Then $\#E(\mathbb{F}_{2^n})$ is divisible by 7 if and only if $6|n$. If $n = 6 \cdot 7^e \cdot m$ where $7 \nmid m$, then*

$$E_7(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(7^e) \times \mathbb{Z}/(7^{e+1}).$$

Proof. By Corollary 3.4.4 and Lemma 3.4.9, we know that $\nu_{\mathfrak{p}}(\sigma^n - 1) > 0$ if and only if $6|n$. Since $\#E(\mathbb{F}_{2^n})$ is divisible by 7 if and only $\nu_{\mathfrak{p}}(\sigma^n - 1) > 0$, $7|\#E(\mathbb{F}_{2^n})$ if and only $6|n$.

Now suppose $6|n$. Then

$$\sigma^n - 1 = 7^t \cdot w$$

where $t \geq 0$ and $w \in \mathbb{Z}[\sigma]$ with $7 \nmid w$. Since 6 is the smallest natural number such that $\sigma^n \equiv 1 \pmod{\mathfrak{p}}$, $\nu_{\mathfrak{p}}(\sigma^3 + 1) > 0$. From the minimum polynomial of σ, we know that $\sigma^3 + 1 = -\sigma + 3$, which is not divisible by 7. Thus $\nu_{\mathfrak{p}}(\sigma^6 - 1) = 1$.

By Lemma 3.4.8, the smallest n such that $\nu_{\mathfrak{p}}(\sigma^n - 1) > 1$ is $6 \cdot 7$. Since $\sigma^6 \equiv 1 \pmod{\mathfrak{p}}$ but $\sigma^6 \not\equiv 1 \pmod{7}$, there exist c_1 and c_2 in $\mathbb{Z}[\sigma]$ where $c_2 \notin \mathfrak{p}$ such that

$$\sigma^6 = 1 + c_1 7 + c_2(\sigma - 3).$$

Then

$$\begin{aligned}
\sigma^{6\cdot 7} &= (1 + c_1 7 + c_2(\sigma - 3))^7 \\
&\equiv (1 + c_2(\sigma - 3))^7 \pmod{7^2} \\
&\equiv 1 + \sum_{i=1}^{7} \binom{7}{i} c_2^i (\sigma - 3)^i \pmod{7^2} \\
&\equiv 1 \pmod{\mathfrak{p}^3}.
\end{aligned}$$

Since $c_2 \notin \mathfrak{p}$, $\sigma^{6\cdot 7} \not\equiv 1 \pmod{7^2}$, i.e., $\sigma^{6\cdot 7} \not\equiv 1 \pmod{\mathfrak{p}^4}$. Thus

$$\nu_{\mathfrak{p}}(\sigma^{6\cdot 7} - 1) = 3.$$

Lemma 3.4.8 tells us that $\nu_{\mathfrak{p}}(\sigma^n - 1)$ always increases by 2. Since $\nu_{\mathfrak{p}}(\sigma^6 - 1) = 1$ and $\nu_{\mathfrak{p}}(\sigma^{6\cdot 7} - 1) = 3$, $\nu_{\mathfrak{p}}(\sigma^n - 1)$ is odd for all n divisible by 6. So, for such n,

$$\sigma^n - 1 = w'\mathfrak{p}^{2e+1} = w'7^e\mathfrak{p}$$

where $w' \in \mathbb{Z}[\sigma]$ with $\nu_{\mathfrak{p}}(w) = 0$. Hence, for $n = 6 \cdot 7^e \cdot w$ where $7 \nmid w$,

$$E_7(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(7^e) \times \mathbb{Z}/(7^{e+1}).$$

□

3.4.2 Structure of $E_p(\mathbb{F}_{2^n})$ with $\left(\frac{p}{7}\right) = -1$

Suppose that $\left(\frac{p}{7}\right) = -1$ and $\sigma^n - 1 = p^e \cdot w$ in $\mathbb{Z}[\sigma]$ where $p \nmid w$ and $e \geq 1$. Since (p) stays prime in $\mathbb{Z}[\sigma]$, $p \nmid w$ implies that $p \nmid \bar{w}$. By Lemma 3.4.2, we have

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e).$$

3.4.3 Structure of $E_p(\mathbb{F}_{2^n})$ with $\left(\frac{p}{7}\right) = 1$

Suppose that $\left(\frac{p}{7}\right) = 1$. Then $p \equiv 1, 2$, or $4 \pmod 7$. Recall that $(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}}$ in $\mathbb{Z}[\sigma]$ where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are prime in $\mathbb{Z}[\sigma]$ with $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Then $\mathfrak{p} = (p, \sigma - \lambda)$ and $\overline{\mathfrak{p}} = (p, \sigma + \lambda - 1)$ where λ is a root of $X^2 - X + 2$ over $\mathbb{Z}/(p)$.

Lemma 3.4.11. *Suppose n_0 is the smallest natural number such that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) > 0$. Then $n_0 = Ord_p(\lambda)$, hence $n_0 | (p-1)$.*

Proof. Suppose $n_0 = \mathrm{Ord}_{\mathfrak{p}}(\lambda)$. Since $\sigma \equiv \lambda \pmod{\mathfrak{p}}$, $n_0 = \mathrm{Ord}_{\mathfrak{p}}(\sigma)$ as well. Since $\mathbb{Z}[\sigma]/\mathfrak{p} \cong \mathbb{Z}/(p)$ and $\sigma \in \mathbb{Z}$,

$$\mathrm{Ord}_p(\sigma) = \mathrm{Ord}_{\mathfrak{p}}(\lambda) = n_0.$$

Hence, $n_0|(p-1)$. □

Lemma 3.4.12. *Let n_0 and $\mathfrak{p}$ be as before. Then $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) = \nu_{\mathfrak{p}}(\sigma^{p-1} - 1)$.*

Proof. Suppose that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) = e$. Then

$$\sigma^{n_0} \equiv 1 \pmod{\mathfrak{p}^e} \text{ but } \sigma^{n_0} \not\equiv 1 \pmod{\mathfrak{p}^{e+1}},$$

i.e.,

$$\sigma^{n_0} = 1 + \alpha \cdot r \text{ where } r \in \mathfrak{p}^e \text{ but } r \notin \mathfrak{p}^{e+1}.$$

Let $p - 1 = kn_0$. Then

$$\sigma^{p-1} = (\sigma^{n_0})^k \equiv 1 + \alpha k \cdot r \pmod{\mathfrak{p}^{e+1}}.$$

Since $1 \leq k < p$, $\alpha k \cdot r \notin \mathfrak{p}^{e+1}$. Hence, $\nu_{\mathfrak{p}}(\sigma^{p-1} - 1) = e$. □

Theorem 3.4.13. *Suppose that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) = e_1$ and $\nu_p(\sigma^{n_0} - 1) = e_2$ with $e_1 \geq e_2$. Then, for $n = n_0 p^e n'$ with $p \nmid n'$,*

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{e+e_1}) \times \mathbb{Z}/(p^{e+e_2}).$$

Proof. By Lemma 3.4.8, $\nu_{\mathfrak{p}}(\sigma^n - 1) = e + e_1$ and by Lemma 3.4.7, $\nu_p(\sigma^n - 1) = e + e_2$. Suppose $\sigma^n - 1 = p^{e+e_2} \cdot w$ where $p \nmid w$. Then $\nu_{\mathfrak{p}}(w) = e_1 - e_2$. By Lemma 3.4.2, we have

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{e+e_1}) \times \mathbb{Z}/(p^{e+e_2}).$$

□

3.5 Tree Structure of g on $E(\mathbb{F}_{2^n})$

Recall that Proposition 3.3.1 and Proposition 3.3.2 imply that the tree structure of the dynamics of $g = \sigma + I$ on $E(\mathbb{F}_{2^n})$ solely depends on the dynamics of g on $E_2(\mathbb{F}_{2^n})$. In this section, we study the dynamics of g on $E_2(\mathbb{F}_{2^n})$. From Section 3.4, we know that $E(\mathbb{F}_{2^n})$ can be decomposed as

$$E(\mathbb{F}_{2^n}) = E_2(\mathbb{F}_{2^n}) + \bigoplus_{l \neq 2} E_p(\mathbb{F}_{2^n}) \tag{3.6}$$

where $E_2(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(2^{h_2})$ for some $h_2 = \nu_2(\#E(\mathbb{F}_{2^n}))$. Since g is $p - invariant$ and $g^{h_2}(P) = \mathcal{O}$ for any $P \in E_2(\mathbb{F}_{2^n})$ by Proposition 3.3.2, (3.6) is equivalent to

$$E(\mathbb{F}_{2^n}) = \ker g^{h_2} + \text{Im } g^{h_2}. \tag{3.7}$$

Then Proposition 3.3.2 tells us that the dynamics of g on $E_2(\mathbb{F}_{2^n})$ is a complete binary tree with height h_2. Thus we like to find out h_2.

Theorem 3.5.1. *Suppose that $K = \mathbb{F}_{2^m}$ where $m = 2^r \cdot m'$ with m' odd. Then $h_2 = r + 2$.*

To prove this theorem, we need the following lemma.

Lemma 3.5.2. *Define a sequence $\alpha_i's$ of elements in $\overline{\mathbb{F}}_2$ as follows:*

$$\alpha_1 = 0, \alpha_2 = 1, \text{ and } \alpha_i = \alpha_{i+1} + \alpha_{i+1}^{-1} \text{ for all } i \geq 2.$$

Then $\alpha_i \in \mathbb{F}_{2^{2^{i-2}}} \setminus \mathbb{F}_{2^{2^{i-3}}}$ for all $i \geq 3$.

To prove this lemma, we need the following theorem.

Theorem 3.5.3. *[Menezes et al., 1992, Theorem 3.10.] Let $q = 2^k$ and let $R(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ of degree n. Then $x^n R(x + x^{-1})$ is irreducible over $\mathbb{F}_q$ if and only if $Tr_{q|2}(c_1/c_0) \neq 0$.*

Proof of Lemma. We will prove it by induction. Note that $\alpha_1 = 0$ and $\alpha_2 = 1$. Let $R_i(x) = x + \alpha_i$ and $R_i^*(x) = xR_i(x + x^{-1}) = x^2 + \alpha_i x + 1$ for $i \geq 2$. Since $R_2(x) = x + \alpha_2 = x + 1$ is irreducible over $\mathbb{F}_2$ and $Tr_{2|2}(1) = 1 \neq 0$, so is $R_2^*(x) = x^2 + x + 1$ by Theorem 3.5.3. But, since $R_2^*(x)$ is a quadratic polynomial, $R_2^*(x)$ is reducible over $\mathbb{F}_{2^2}$, i.e., α_3, a root of $R_2^*(x)$, is in $\mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Thus the claim is true for $i = 3$. Assume that the claim is true for $3 \leq i \leq n$. Then

$$\begin{aligned} Tr_{2^{2^{n-2}}|2}(\alpha_n^{-1}) &= Tr_{2^{2^{n-3}}|2}\left(Tr_{2^{2^{n-2}}|2^{2^{n-3}}}(\alpha_n^{-1})\right) \\ &= Tr_{2^{2^{n-3}}|2}\left(Tr_{2^{2^{n-2}}|2^{2^{n-3}}}(\alpha_{n-1} + \alpha_n)\right) \\ &= Tr_{2^{2^{n-3}}|2}\left(Tr_{2^{2^{n-2}}|2^{2^{n-3}}}(\alpha_{n-1}) + Tr_{2^{2^{n-2}}|2^{2^{n-3}}}(\alpha_n)\right). \end{aligned}$$

By the induction hypothesis, $\alpha_{n-2} \in \mathbb{F}_{2^{2^{n-2}}}$, i.e., $Tr_{2^{2^{n-2}}|2^{2^{n-3}}}(\alpha_{n-1}) = 0$ and, by the definition of $R_n^*(x)$, $Tr_{2^{2^{n-2}}|2^{2^{n-3}}}(\alpha_n) = \alpha_{n-1}$. Thus, by the induction hypothesis,

$$Tr_{2^{2^{n-2}}|2}(\alpha_n^{-1}) = Tr_{2^{2^{n-3}}|2}(\alpha_{n-1}) \neq 0.$$

Hence, by Theorem 3.5.3, $R_n^*(x)$ is also irreducible over $\mathbb{F}_{2^{2^{n-2}}}$ and α_{n+1}, a root of R_n^* is in $\mathbb{F}_{2^{2^{n-1}}} \setminus \mathbb{F}_{2^{2^{n-2}}}$. This completes the proof. □

Proof of Theorem 3.5.1. Let $P_i = (\alpha_i, \beta_i) \in E(\overline{\mathbb{F}}_2)$ for $i \geq 0$ be any sequence of points such that

$$P_0 = \mathcal{O} \text{ and } g(P_{i+1}) = P_i \text{ for } i \geq 0.$$

We want to see in which field P_i lies for $i \geq 0$. It is easy to see that α_i is as described

in Lemma 3.5.2. Since $g(P_{i+1}) = P_i$, from (3.2), for all $i \geq 3$,

$$\beta_i = \frac{\alpha_i^2\beta_{i-1} + \alpha_i^4 + \alpha_i^2 + 1}{\alpha_i^2 + 1}. \tag{3.8}$$

Note that, for $i \geq 1$, β_i's roots of the polynomial $y^2 + \alpha_i y = \alpha_i^3 + 1$. Then one can check that $P_1 = (0, 1)$ and $P_2 = (1, 0)$ or $(1, 1)$, i.e., P_1 and P_2 are in $\mathbb{F}_2$. Note that for $i \geq 3$, that the largest subfield of $\mathbb{F}_{2^m}$ of the form $\mathbb{F}_{2^{2^{i-2}}}$ is $\mathbb{F}_{2^{2^r}}$. Then Lemma 3.5.2 says $\alpha_i \in \mathbb{F}_{2^m}$ for $1 \leq i \leq r+2$ and, for β_i, it is obvious that $\beta_i \in \mathbb{F}_{2^m}$ for $3 \leq i \leq r+1$. Since $\alpha_{r+2}, \beta_{r+1} \in \mathbb{F}_{2^m}$, from (3.8), $\beta_{r+2} \in \mathbb{F}_{2^m}$ too. Hence, the largest i such that $P_i \in E(K)$ is $r + 2$, which implies $h_2 = r + 2$.

□

Consider the tree structure of g on $E_2(\mathbb{F}_{2^n})$ where $n = 2^s \cdot n'$ with n' odd. Then, by Theorem 3.5.1,

$$E_2(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(2^{s+2}).$$

Hence, the dynamics of g on $E_2(\mathbb{F}_{2^n})$ is the complete binary tree of height $s + 1$ attached to $\mathcal{O}$ which is the only fixed point under g.

3.6 Cycle Structure of g on $E(\mathbb{F}_{2^n})$

Recall, from Section 3.3, that for $P \in E(\mathbb{F}_{2^n})$, the cycle length of P under g is the smallest natural number t such that

$$(M^t - I)\begin{pmatrix} P \\ g(P) \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}. \tag{3.9}$$

Suppose that h is such that $M^h - I \equiv 0 \pmod{|P|}$. Then $t = h$ satisfies (3.9). Depending on the structure of $< g > \cap < g(P) >$, the cycle length of P under g may be smaller than h. Thus the cycle length of P under g is determined by the behavior of M and the structure of $< P > \cap < g(P) >$. For the rest of the chapter, $\mathrm{Cl}_g(P)$ denotes the cycle length of P under g. Note that $E_p(\mathbb{F}_{2^n})$ is $g-invariant$ for $p|\#E(\mathbb{F}_{2^n})$. So, we consider the following three cases:

(a) $P \in E_7(\mathbb{F}_{2^n})$.

(b) $P \in E_p(\mathbb{F}_{2^n})$ with $\left(\frac{p}{7}\right) = -1$.

(c) $P \in E_p(\mathbb{F}_{2^n})$ with $\left(\frac{p}{7}\right) = 1$.

3.6.1 Cycle Length of $P \in E_7(\mathbb{F}_{2^n})$

From Section 3.4.1, we know that $E_7(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(7^e) \times \mathbb{Z}/(7^{e+1})$ for some $e \geq 0$. The cycle length of $P \in E_7(\mathbb{F}_{2^n})$ depends on the subgroup structure of $E_7(\mathbb{F}_{2^n})$ and the order of P. To study the cycle lengths, we need to know the properties of M modulo 7^e.

Lemma 3.6.1. *$Ord_{7^e}(M) = 7^{e-1} \cdot 21$ for all $e \geq 1$.*

Proof. We will prove it by induction. Note that $\mathrm{Ord}_7(M) = 21$ and

$$M^{21} \equiv \begin{pmatrix} 1+4\cdot 7 & 6\cdot 7 \\ 2\cdot 7 & 1+3\cdot 7 \end{pmatrix} \pmod{7^2}.$$

Suppose that $\mathrm{Ord}_{7^e}(M) = t$ with

$$M^t \equiv \begin{pmatrix} 1+a_{11}\cdot 7^e & a_{12}\cdot 7^e \\ a_{21}\cdot 7^e & 1+a_{22}\cdot 7^e \end{pmatrix} \pmod{7^{e+1}}$$

where a_{11}, a_{12}, a_{21}, and a_{22} are not simultaneously $0 \pmod 7$, i.e., $\mathrm{Ord}_{7^{e+1}}(M) > t$. Then

$$\begin{aligned} \left(M^t\right)^7 &\equiv \begin{pmatrix} (1+a_{11}\cdot 7^e)^7 & a_{12}\cdot 7^{e+1} \\ a_{21}\cdot 7^{e+1} & (1+a_{22}\cdot 7^e)^7 \end{pmatrix} \pmod{7^{e+2}} \\ &\equiv \begin{pmatrix} 1+a_{11}\cdot 7^{e+1} & a_{12}\cdot 7^{e+1} \\ a_{21}\cdot 7^{e+1} & 1+a_{22}\cdot 7^{e+1} \end{pmatrix} \pmod{7^{e+2}} \\ &\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{7^{e+1}}. \end{aligned}$$

We know that $\mathrm{Ord}_{7^{e+1}}(M) > t$ and $\mathrm{Ord}_{7^{e+1}}(M) | 7t$. Since 7 is a prime, $\mathrm{Ord}_{7^{e+1}}(M) = 7t$, which completes the proof. □

Corollary 3.6.2. *Let $e \geq 1$. Suppose that $Ord_{7^e}(M) = n$. Then*

$$M^n \equiv \begin{pmatrix} 1+4\cdot 7^e & 6\cdot 7^e \\ 2\cdot 7^e & 1+3\cdot 7^e \end{pmatrix} \pmod{7^{e+1}}.$$

Proof. It is trivial from the proof of Lemma 3.6.1. □

Lemma 3.6.3. *Suppose that* $E_7(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(7^e) \times \mathbb{Z}/(7^{e+1})$ *with* $e \geq 1$ *and* $P \in E_7$ *with* $|P| = 7^{e'}$ *where* $1 \leq e' \leq e$. *If* $< P > \cap < g(P) >$ *is not trivial, then*

$$| < P > \cap < g(P) > | = 7$$

Proof. Suppose $< P > \cap < g(P) >$ is nontrivial. If $| < P > | = 7$, then it is trivial that $| < P > \cap < g(P) > | = 7$. For the rest of the proof, we assume that $| < P > | > 7$, i.e., $e' \geq 2$. Since $< P > \cap < g(P) >$ is nontrivial and both $< P >$ and $< g(P) >$ are cyclic, there exist nonzero integers u and v such that

$$uP \ = \ vg(P)$$

where

$$< P > \cap < g(P) > = < uP > = < vg(P) > .$$

Then, from the minimum polynomial of g,

$$ug(P) \ = \ vg^2(P) \ = \ vg(P) - 2vP,$$

i.e.,

$$2vP \ = \ (v-u)g(P).$$

This implies that there exists $k \neq 0$ such that

$$ku \equiv 2v \pmod{7^{e'}},$$
$$kv \equiv v - u \pmod{7^{e'}}.$$

Eliminating u from the above equations, we get

$$v(k^2 - k + 2) \equiv 0 \pmod{7^{e'}}. \tag{3.10}$$

Since $k^2 - k + 2 = (k-4)^2 + 7(k-2)$, we see that $k^2 - k + 2$ is not divisible by 7^2 for any k. Since $e' \geq 2$ and $k^2 - k + 2 \not\equiv 0 \pmod{7^2}$, (3.10) implies that $7^{e'-1} | v$. Hence, $vg(P)$ has order at most 7. This implies that

$$| < P > \cap < g(P) > | = 7.$$

Note that for $vg(P)$ to have order 7, we must have

$$k^2 - k + 2 \equiv 0 \pmod{7},$$

i.e., $k \equiv 4 \pmod{7}$. If $e' = 1$, then $| < P > \cap < g(P) > | = 7$ implies that $< P >=< g(P) >$. Moreover, $4u = 2v$, i.e., $g(P) = 4P$. □

Note that in the above proof, for $vg(P)$ to have order 7, we must have

$$k^2 - k + 2 \equiv 0 \pmod{7},$$

i.e., $k \equiv 4 \pmod{7}$. Especially if $e' = 1$, then $| < P > \cap < g(P) > | = 7$ implies that $< P >=< g(P) >$ and $g(P) = 4P$.

Theorem 3.6.4. *Suppose that $P \in E_7(\mathbb{F}_{2^n})$ with $|P| = 7$. Then*

$$Cl_g(P) = \begin{cases} 21 \text{ if } | < P > \cap < g(P) > | = 1, \\ 3 \text{ if } | < P > \cap < g(P) > | = 7. \end{cases}$$

Proof. Suppose that $| < P > \cap < g(P) > | = 1$. Then, $\mathrm{Cl}_g(P) = \mathrm{Ord}_7(M) = 21$. Now suppose that $| < P > \cap < g(P) > | = 7$. This implies that $< P >=< g(P) >$ and from the proof of Lemma 3.6.3, we know $g(P) = 4 \cdot P$. Hence, $\mathrm{Cl}_g(P) = \mathrm{Ord}_7(4) = 3$. □

Theorem 3.6.5. *Suppose that* $E_7(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(7^e) \times \mathbb{Z}/(7^{e+1})$ *with* $e \geq 2$ *and* $P \in E_7(\mathbb{F}_{2^n})$ *with* $|P| = 7^{e'}$ *where* $e' \geq 2$. *Then*

$$Cl_g(P) = \begin{cases} Ord_{7^{e'}}(M) \text{ if } | < P > \cap < g(P) > | = 1, \\ Ord_{7^{e'-1}}(M) \text{ if } | < P > \cap < g(P) > | = 7. \end{cases}$$

Proof. Suppose $| < P > \cap < g(P) > | = 1$. Then, from (3.4),

$$\left(M^t - I\right) \begin{pmatrix} P \\ g(P) \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}$$

if and only if

$$M^t \equiv I \pmod{7^{e'}}.$$

Now suppose that $| < P > \cap < g(P) > | = 7$. Then, from the proof of Lemma 3.6.3,

$$g(7^{e'-1}P) = 4 \cdot 7^{e'-1}P.$$

Let t be the multiplicative order of M modulo $7^{e'-1}$. Then we know that, from the proof of Corollary 3.6.2,

$$(M^t - I) \equiv \begin{pmatrix} 4 \cdot 7^{e'-1} & 6 \cdot 7^{e'-1} \\ 2 \cdot 7^{e'-1} & 3 \cdot 7^{e'-1} \end{pmatrix} \pmod{7^{e'}}.$$

Thus

$$(M^t - I)\begin{pmatrix} P \\ g(P) \end{pmatrix} = \begin{pmatrix} 4 \cdot 7^{e'-1}P + 6 \cdot 7^{e'-1}g(P) \\ 2 \cdot 7^{e'-1}P + 3 \cdot 7^{e'-1}g(P) \end{pmatrix}$$
$$= \begin{pmatrix} 4 \cdot 7^{e'-1}P + 3 \cdot 7^{e'-1}P \\ 2 \cdot 7^{e'-1}P + 5 \cdot 7^{e'-1}P \end{pmatrix}$$
$$= \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}.$$

Since t is the smallest such that $M^t \equiv I \pmod{7^{e'-1}}$, $\mathrm{Cl}_g(P) = t$. □

Thus Theorem 3.6.4 and Theorem 3.6.5 explain the cycle length of P under g for $P \in E_7(\mathbb{F}_{2^n})$.

From Section 3.4.1, we know that $E_7(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(7^e) \times \mathbb{Z}/(7^{e+1})$ for some $e \geq 0$. Thus there exist P_1 and P_2 in $E_7(\mathbb{F}_{2^n})$ such that

$$E_7(\mathbb{F}_{2^n}) = < P_1, P_2 >$$

with $|P_1| = 7^e$ and $|P_2| = 7^{e+1}$. For the following cases, we can determine the structure of $< P > \cap < g(P) >$ explicitly.

Lemma 3.6.6. *Suppose $E_7(\mathbb{F}_{2^n})$ is as above and $P = \beta P_2$ with $|P| = 7^c$ where $1 \leq c \leq e+1$. Then*

$$| < P > \cap < g(P) > | = 7.$$

Proof. From the proof of Lemma 3.6.3, it suffices to show that $< 7^{c-1}P >=< 7^{c-1}g(P) >$. Since $|P| = 7^c$, $P = \beta_1 7^{e+1-c}P_2$ with $7 \nmid \beta_1$. Then

$$< 7^{c-1}P >=< 7^{c-1}\beta_1 7^{e+1-c}P_2 >=< 7^e P_2 > .$$

Suppose that

$$g(P_1) = a_{11}P_1 + a_{12}P_2,$$
$$g(P_2) = a_{21}P_1 + a_{22}P_2.$$

Since g is an isomorphism on $E_7(\mathbb{F}_{2^n})$, $7|a_{12}$ and $7 \nmid a_{22}$. Thus

$$< 7^{c-1}g(P) >=< g(7^{c-1}P) >=< g(7^e P_2) >=< a_{22}7^e P_2 >=< 7^e P_2 > .$$

Hence, $< 7^{c-1}P >=< 7^{c-1}g(P) >$, i.e., $| < P > \cap < g(P) > | = 7$. □

Lemma 3.6.7. *Suppose $E_7(\mathbb{F}_{2^n})$ is as above and $P = \alpha P_1 + \beta P_2$ with $\nu_7(\alpha) = \nu_7(\beta)$. Then*

$$| < P > \cap < g(P) > | = 7.$$

Proof. Suppose $|P| = 7^c$ with $1 \leq c \leq e$. Then

$$P = \alpha P_1 + \beta P_2 = \alpha_1 7^{e+1-c}P_1 + \beta_1 7^{e+1-c}P_2.$$

Similar to the proof of Lemma 3.6.6,

$$< 7^{c-1}P >=< 7^{c-1}(\alpha_1 7^{e+1-c}P_1 + \beta_1 7^{e+1-c}P_2) >=< \beta_1 7^e P_2 >=< 7^e P_2 >$$

and

$$< 7^{c-1}g(P) >=< g(\beta_1 7^e P_2) >=< 7^e P_2 > .$$

Hence, $< 7^{c-1}P >=< 7^{c-1}g(P) >$, i.e., $| < P > \cap < g(P) > | = 7$. □

For other cases, we have the following conjecture:

Conjecture 3.6.8. *Suppose $E_7(\mathbb{F}_{2^n})$ is as above and $P = \alpha P_1 + \beta P_2$ with $\alpha \not\equiv 0 \pmod{7^e}$ and $\nu_7(\alpha) \neq \nu_7(\beta)$. Then*

$$< P > \cap < g(P) >= \{\mathcal{O}\}.$$

3.6.2 Cycle Length of $P \in E_p(\mathbb{F}_{2^n})$ with $\left(\frac{p}{7}\right) = -1$

In Section 3.4.2, we have seen that $E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$ for a rational odd prime p such that $\left(\frac{p}{7}\right) = -1$. Since $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right) = -1$, $k^2 - k + 2$ is irreducible over $\mathbb{Z}/(p^e)$ for any $e \geq 1$. So, for any $P \in E_p(\mathbb{F}_{2^n})$,

$$< P > \cap < g(P) >= \{\mathcal{O}\}.$$

This tells us that the cycle length of $P \in E_p(\mathbb{F}_{2^n})$ with $|P| = p^e$ solely depends on $\mathrm{Ord}_{p^e}(M)$.

Theorem 3.6.9. *Suppose that p is a rational prime with $\left(\frac{p}{7}\right) = -1$ and $P \in E_p(\mathbb{F}_{2^n})$ with $|P| = p^e$ for some $e \geq 1$. Then $Cl_g(P) = Ord_{p^e}(M)$.*

Proof. Since $< P > \cap < g(P) >= \{\mathcal{O}\}$ and $|g(P)| = |P| = p^e$, we have

$$(M^n - I) \begin{pmatrix} P \\ g(P) \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}$$

if and only if $M^n - I \equiv 0 \pmod{p^e}$. $\square$

Lemma 3.6.10. *Suppose* $\left(\frac{p}{7}\right) = -1$. *Then*

$$Ord_p(M) = (p+1)\,Ord_p(2),$$

and for $e \geq 2$,

$$Ord_{p^e}(M) = p^{e'}\,Ord_p(M)$$

where $e' = \max(0, e - \nu_p(M^{Ord_p(M)} - I))$.

Proof. Suppose that λ_1 and λ_2 are roots of $m_g(T)$. Then, since ${\lambda_i}^{p+1} = 2$ for $i = 1, 2$,

$$M^{p+1} \equiv 2I \pmod{p}.$$

So $\mathrm{Ord}_p(M) = (p+1)\mathrm{Ord}_p(2)$.

Now suppose $\mathrm{Ord}_p(M) = c$ and

$$M^c \equiv I \pmod{p^{e'}} \text{ but } M^c \not\equiv I \pmod{p^{e'+1}}.$$

Then $\mathrm{Ord}_{p^{\bar{e}}}(M) = \mathrm{Ord}_p(M)$ for $1 \leq \bar{e} \leq e'$. Suppose that

$$M^c = I + p^{e'}A \text{ where } p \nmid A.$$

Then, for any $e > e'$,

$$\begin{aligned}(M^c)^{p^{e'-e}} &= (I + p^{e'}A)^{p^{e-e'}} \\ &\equiv I + p^e A \pmod{p^{e+1}} \\ &\equiv I \pmod{p^e}\end{aligned}$$

Moreover, since p is a prime and c is the order of M modulo p, $c \cdot p^{e-e'}$ is the order of M modulo p^e. □

Note that the cycle length of a point in $E_p(\mathbb{F}_{2^n})$ with $\left(\frac{p}{7}\right) = -1$ is determined by the multiplicative order of M modulo the order of the point. Thus we can determine the exact distribution of cycle lengths according to the orders of points in $E_p(\mathbb{F}_{2^n})$.

Theorem 3.6.11. *Suppose that $E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$ and $P \in E_p(\mathbb{F}_{2^n})$ with $|P| = p^c$ where $1 \leq c \leq e$. Then the number of cycles of length $Ord_{p^c}(M)$ is $p^{2c} = p^{2c-2}$.*

Proof. It suffices to show that the number of points in $E_p(\mathbb{F}_{2^n})$ of order p^c is $p^{2c} = p^{2c-2}$. Since $E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$, the number of points in $E_p(\mathbb{F}_{2^n})$ of order p^c is equal to that of points in $\mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$ of order p^c. Suppose that $(a, b) \in \mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$. Then (a, b) is of order p^c if and only if $(p^c \cdot a, p^c \cdot b) = (0, 0)$, but $(p^{c-1} \cdot a, p^{c-1} \cdot b) \neq (0, 0)$. Hence, there are $p^{2c} - p^{2(c-1)}$ points of order p^c. □

3.6.3 Cycle Length of $P \in E_p(\mathbb{F}_{2^n})$ with $\left(\frac{p}{7}\right) = 1$

3.6.3.1 When $E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{e_p})$ for some $e_p \geq 1$

Since $E_p(\mathbb{F}_{2^n})$ is cyclic, there exists $Q \in E_p(\mathbb{F}_{2^n})$ such that $E_p(\mathbb{F}_{2^n}) =< Q >$. Recall $E_p(\mathbb{F}_{2^n})$ is $g - invariant$. Thus there exists u such that

$$g(Q) = uQ.$$

Moreover, u satisfies $u^2 - u + 2 \equiv 0 \pmod{p^e}$. This implies that g is just a multiplicative map on $E_p(\mathbb{F}_{2^n})$. So the possible cycle lengths are $\mathrm{Ord}_{p^c}(u)$ where $1 \leq c \leq e$. Hence, for each c with $1 \leq c \leq e$, there are $\varphi(p^c) = (p-1)p^{c-1}$ points of cycle length $\mathrm{Ord}_{p^c}(u)$.

3.6.3.2 When $E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$ for some $e \geq 1$

Note that $E_p(\mathbb{F}_{2^n})$ is a $\mathbb{Z} - module$, so that there exists P_1 and P_2 in $E_p(\mathbb{F}_{2^n})$ such that $E_p =< P_1, P_2 >$ where$|P_1| = |P_2| = p^{e_p}$. Suppose that

$$g(P_1) = a_{11}P_1 + a_{12}P_2$$
$$g(P_2) = a_{21}P_1 + a_{22}P_2,$$

i.e.,

$$g \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix} = A \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}$$

where $A = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in (\mathbb{Z}/(p^2))^{2\times 2}$.

Since g is an isomorphism on $E_p(\mathbb{F}_{2^n})$, A is invertible modulo p^e. For any $P = aP_1 + bP_2 \in E_p(\mathbb{F}_{2^n})$,

$$g(P) = (a,b)g \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = (a,b)A \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}.$$

Thus, for all $n \geq 0$,

$$g^n(P) = (a,b)A^n \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}.$$

Lemma 3.6.12. *Suppose $A \neq \lambda I$ for any $\lambda \in \mathbb{Z}/(p^{e_p})$. Then, there exists a vector $(a,b) \in \mathbb{Z}/(p^{e_p}) \times \mathbb{Z}/(p^{e_p})$ such that V is invertible modulo p^{e_p} where*

$$V = \begin{pmatrix} (a,b) \\ (a,b)A \end{pmatrix},$$

i.e., $(a,b)A \neq \mu(a,b)$ for any μ in $\mathbb{Z}/(p^{e_p})$.

Proof. $(a,b)A = \mu(a,b)$ for some (a,b) and μ implies that μ is an eigenvalue and (a,b) is a corresponding eigenvector. Note that since $m_g(T)$ dose not have repeated roots modulo any prime $p \neq 7$, $A \neq \lambda I$. We start from $\mathbb{Z}/(p)$. Since the eigenvectors associated with distinct eigenvalues are linearly independent, the existence of such V modulo p is trivial. Then we can lift this to any power of p. This completes the proof. □

Corollary 3.6.13. *A is similar to M modulo p^e for any positive integer e. Moreover, there exists $Q \in E_p(\mathbb{F}_{2^n})$ such that $E_p(\mathbb{F}_{2^n}) =< Q, g(Q) >$.*

Proof. Directly from the relation between A and M. □

With such Q, any $P \in E_p(\mathbb{F}_{2^n})$ can be expressed as $a \cdot Q + b \cdot g(Q)$ for some $a, b \in \mathbb{Z}/(p^e)$ and

$$g(P) = (a,b)M \begin{pmatrix} Q \\ g(Q) \end{pmatrix}.$$

So the cycle length of $P \in E_p(\mathbb{F}_{2^n})$ depends on the order of P and the behavior of the matrix M modulo p^e. Note that M is diagonalizable modulo p^e, i.e.,

$$M \equiv U \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} U^{-1} \pmod{p^{e_p}} \equiv U \cdot D \cdot U^{-1} \pmod{p^{e_p}}$$

where U is invertible matrix modulo p^e. This implies that the dynamics of g over $E_p(\mathbb{F}_{2^n})$ is isomorphic to that of D over $\mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$. Thus it suffices to consider the dynamics of D over $\mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$.

Theorem 3.6.14. *Suppose that*

$$D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

and $P = (a, b) \in \mathbb{Z}/(p^e) \times \mathbb{Z}/(p^e)$. *Then*

$$Cl_D(P) = lcm(Ord_{p^{e-\nu_p(a)}}(\lambda_1), Ord_{p^{e-\nu_p(b)}}(\lambda_2)).$$

Proof. Note that $\mathrm{Cl}_D(P) = t$ if and only if t is the smallest such that

$$(a, b)\left(D^t - I\right) \equiv (0, 0) \pmod{p^e},$$

i.e.,

$$a \cdot (\lambda_1^t - 1) \equiv 0 \pmod{p^e} \text{ and } b \cdot (\lambda_2^t - 1) \equiv 0 \pmod{p^e}. \tag{3.11}$$

Suppose that $\nu_p(a) = e_a$ and $\nu_p(b) = e_b$. Then (3.11) is true if and only if

$$\lambda_1^t - 1 \equiv 0 \pmod{p^{e-e_a}} \text{ and } \lambda_2^t - 1 \equiv 0 \pmod{p^{e-e_b}}.$$

Thus t should be the multiple of the order of λ_1 modulo p^{e-e_a} and the order of λ_2 modulo p^{e-e_b}. Since t is the smallest such,

$$\mathrm{Cl}_D(P) = \mathrm{lcm}(\mathrm{Ord}_{p^{e-\nu_p(a)}}(\lambda_1), \mathrm{Ord}_{p^{e-\nu_p(b)}}(\lambda_2)).$$

□

3.6.3.3 When $E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{e_1}) \times \mathbb{Z}/(p^{e_2})$ with $e_1 < e_2$

In this case, for a point $P \in E_p(\mathbb{F}_{2^n})$, the structure of $< P > \cap < g(P) >$ can be arbitrary. We cannot obtain the exact $\mathrm{Cl}_g(P)$ without finding the exact structure of $< P > \cap < g(P) >$. But, from (3.9), we know $\mathrm{Cl}_g(P)$ should divide $\mathrm{Ord}_{p^{e_p}}(M)$. Hence, $\mathrm{Cl}_g(P)$ is bounded by $\mathrm{Ord}_{p^{e_p}}(M)$.

3.7 Dynamics of $x \mapsto x + x^{-1}$ on $\mathbb{F}_{2^n} \cup \{\infty\}$

So far we have studied the dynamics of g on $E(\mathbb{F}_{2^n})$. Using this information, we now study the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$ in this section. For each $x \in \mathbb{F}_{2^n}$, there are two points $(x, y) \in E(\mathbb{F}_{2^{2n}})$. The values of y are in $\mathbb{F}_{2^{2n}}$. Let the subset S of $E(\mathbb{F}_{2^{2n}})$ be

$$S = \{P = (x, y) \in E(\mathbb{F}_{2^{2n}}) : x \in \mathbb{F}_{2^n}\} \cup \{\mathcal{O}\}.$$

Suppose $|P| = 2^{c_2} p_1^{c_{p_1}} \cdots p_m^{c_{pm}}$ where p_i's are odd primes for $1 \leq i \leq m$. Then, P can be written as

$$P = P_2 + P_{p_1} + P_{p_2} + \ldots + P_{p_m}$$

where $P_2 \in E_2(\mathbb{F}_{2^{2n}})$ and $P_{p_i} \in E_{p_i}(\mathbb{F}_{2^{2n}})$ for $1 \leq i \leq m$. As we have seen in Section 3.6, we can determine $\mathrm{Cl}_g(P_{p_i})$ for $1 \leq i \leq m$. Then the tail length of P is c_2 and P is attached to a cycle whose cycle length is $\mathrm{lcm}(\mathrm{Cl}_g(P_{p_1}), \mathrm{Cl}_g(P_{p_2}), \ldots, \mathrm{Cl}_g(P_{p_m}))$. For the lengths of cycles in the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$, we have the following theorem:

Theorem 3.7.1. *Suppose $P = (x, y) \in S$ with $Cl_g(P) = m$. Then*

$$Cl_f(x) = \begin{cases} m \text{ if } m \text{ is odd,} \\ \frac{m}{2} \text{ if } m \text{ is even.} \end{cases}$$

Proof. Note that $\pi(P) = \pi(Q)$ for $P, Q \in E(\mathbb{F}_{2^{2n}})$ if and only of $Q = -P$. Thus $\mathrm{Cl}_f(x) < \mathrm{Cl}_g(P)$ if and only if P satisfies $g^{m'}(P) = -P$ for some $1 \leq m' < m$. Suppose that m is odd and there exists m' such that $g^{m'}(P) = -P$. Then, since g is

an endomorphism over $E(\mathbb{F}_{2^{2n}})$, $\mathrm{Cl}_g(-P) = m$. It implies that

$$g^{2m'}(P) = g^{m'}(-P) = -g^{m'}(P) = P,$$

which is contradiction to that m is odd. Thus, if m is odd, then $\mathrm{Cl}_g(P) = \mathrm{Cl}_f(x)$.

Suppose that m is even. Note that since for $P \in E(\mathbb{F}_{2^{2n}})$, $g^2(P) = P$ implies that $P \in E_2(\mathbb{F}_{2^{2n}})$, there is no cycle of length 2 in the dynamics of g on $E(\mathbb{F}_{2^{2n}})$. Thus $m \equiv 0 \pmod 4$. Note

$$(g^m - I)(P) = (g^{2m'} - I)(P) = (g^{m'} - I) \cdot (g^{m'} + I)(P) = \mathcal{O}.$$

Since $(g^{m'} - I)(P) \neq \mathcal{O}$, $(g^{m'} + I)(P) = \mathcal{O}$, i.e., $g^{m'}(P) = -P$. Hence,

$$\mathrm{Cl}_f(x) = m' = \frac{m}{2}.$$

□

Note that $\ker g^2 \setminus \ker g = \{(1,0),(1,1)\}$. Then the points in S have the following properties.

Lemma 3.7.2. *Suppose* $(x,y) \in S \setminus E(\mathbb{F}_{2^n})$ *and* $P = (1,0)+(x,y)$. *Then* $\pi(P) \notin \mathbb{F}_{2^n}$, *but* $\pi(g(P)) \in \mathbb{F}_{2^n}$.

Proof. From the addition formula,

$$\pi(P) = \left(\frac{y}{1+x}\right)^2 + \frac{y}{1+x} + 1 + x.$$

Since $P \in E$,

$$\begin{aligned}\pi(P) &= \frac{x^3+xy+1}{1+x^2} + \frac{y}{1+x} + 1 + x \\ &= \frac{x^3+y+1}{1+x^2} + 1 + x. \end{aligned} \tag{3.12}$$

Since $\pi(P) \in \mathbb{F}_{2^n}$ if an only if $(\pi(P))^{2^n} = \pi(P)$, . From (3.12), we can see that this is true if and only if

$$y^{2^{n+1}} + y^{2^n} = y^2 + y,$$

i.e.,

$$y^{2^n} = y.$$

Since $y \in \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$, this is not possible. Thus $\pi(P) \in \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$. Now apply g to P. Then

$$\begin{aligned} g(P) &= g((1,0)) + g((x,y)) \\ &= (0,1) + (x + x^{-1}, y') \end{aligned}$$

where $y' = x^2 + y + 1 + \frac{y+1}{x^2}$. So,

$$\begin{aligned}\pi(g(P)) &= \frac{(y'+1)^2}{(x+x^{-1})^2} + \frac{y'+1}{x+x^{-1}} + x + x^{-1} \\ &= \frac{1}{(x+x^{-1})^2}\left(y'^2 + 1 + (y'+1)(x+x^{-1}) + (x+x^{-1})^3\right) \\ &= \frac{1}{(x+x^{-1})^2}\left((x+x^{-1})^3 + (x+x^{-1})y' + (y'+1)(x+x^{-1}) + (x+x^{-1})^3\right) \\ &= \frac{1}{(x+x^{-1})^2}\left(x+x^{-1}\right) \\ &= \frac{1}{x+x^{-1}}. \end{aligned}$$

Hence $\pi(g(P)) \in \mathbb{F}_{2^n}$. □

Lemma 3.7.3. *Suppose* $(x, y) \in S \setminus E(\mathbb{F}_{2^n})$ *and* $P = (1, 1)+(x, y)$. *Then* $\pi(P) \notin \mathbb{F}_{2^n}$, *but* $\pi(g(P)) \in \mathbb{F}_{2^n}$.

Proof. The same argument with the previous lemma will work. □

Lemma 3.7.4. *For any* $P \in E(\mathbb{F}_{2^{2n}}) \setminus E_2(\mathbb{F}_{2^{2n}})$,

$$\pi((1, 0) + P) \neq \pi((1, 1) + P).$$

Proof. Let $P = (x, y)$. Then

$$\pi((1, 0) + (x, y)) = \frac{y^2}{1 + x^2} + \frac{y}{1 + x} + 1 + x \tag{3.13}$$

and

$$\pi((1, 1) + (x, y)) = \frac{1 + y^2}{1 + x^2} + \frac{1 + y}{1 + x} + 1 + x. \tag{3.14}$$

Thus (3.13) = (3.14) if and only if $x = 0$, i.e., $P = (0, 1) \in E_2(\mathbb{F}_{2^{2n}})$. This contradicts that $P \notin E_2(\mathbb{F}_{2^{2n}})$, which completes the proof. □

Lemma 3.7.5. *Suppose* $P \in S \setminus E(\mathbb{F}_{2^n})$ *and* P *is periodic with the cycle length bigger than* 1. *Then, for any* $n \geq 1$, $g^n(P) \in S \setminus E(\mathbb{F}_{2^n})$.

Proof. It suffices to show $g(P)$ has the same property with P. Let $P = (x, y)$ and $g(P) = (u, v)$. Then, $u = x + x^{-1}$. Since $x \in \mathbb{F}_{2^n}$, so is u. From Section 3.2,

$$v = x^2 + y + 1 + \frac{y + 1}{x^2}.$$

Since $v^{2^n} = x^2 + y^{2^n} + 1 + \frac{y^{2^n}+1}{x^2}$, $v \in \mathbb{F}_{2^n}$ if and only if

$$\left(y^{2^n} + y\right)\left(1 + \frac{1}{x^2}\right) = 0. \tag{3.15}$$

Since $y \in \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$, (3.15) is true if and only if $x = 1$, i.e., $g(P) = (1, 0) \in E_2(\mathbb{F}_{2^{2n}})$. This contradicts that P is periodic, which completes the proof. □

Lemma 3.7.5 implies that periodic points in the same cycle have the same described property. Let $n = 2^s \cdot n'$ with $2 \nmid n'$. Then, from Section 3.5, $E_2(\mathbb{F}_{2^{2n}}) \cong \mathbb{Z}/(2^{s+3})$ and any tree in the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ is identical to the tree attached to $\mathcal{O}$ which is a complete binary tree of height $s + 2$. For our purpose, we view a single point as a tree of height 0. To study the tree structure of the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$, we consider these cases separately:

1. Structure of the tree attached to ∞.

2. Structure of trees projected down from trees attached to periodic points which are in $E(\mathbb{F}_{2^n})$.

3. Structure of trees projected down from trees attached to periodic points which are in $S \setminus E(\mathbb{F}_{2^n})$.

Theorem 3.7.6. *Suppose that $n = 2^s \cdot n'$ where $2 \nmid n'$. Then the tree structure attached to ∞ is as follows: a complete binary tree of height s is attached to 0 and 0 is attached to ∞.*

Proof. By the definition of f, $\ker f = \{\infty, 0\}$ and 0 maps to ∞ which is the only fixed point of f. Then, by Theorem 3.5.1, $E_2(\mathbb{F}_{2^{2n}}) \cong \mathbb{Z}/(2^{s+3})$. Thus the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ is a complete binary tree of height $s + 2$, which is attached to $\mathcal{O}$. From the proof of Theorem 3.5.1, we know that for $P \in E_2(\mathbb{F}_{2^{2n}})$, $P \in S$ if and only if

$P \in \ker g^{s+2}$. Note that $(1,0),(1,1) \in \ker g^2 \setminus \ker g$ and $g((1,0)) = g((1,1)) = (0,1)$. Thus two complete binary trees of height s are attached to $(0,1)$. Since $\pi(1,0) = \pi(1,1) = 1$, those two trees of height s will be projected by π to one binary tree of height s which is attached to 0 in the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$. □

Lemma 3.7.7. *Suppose that n is defined as in Theorem 3.7.6. Then structure of a tree projected from a tree attached to a periodic point in $S \setminus E(\mathbb{F}_{2^n})$ is a tree of height 0.*

Proof. Suppose that $P \in S \setminus E(\mathbb{F}_{2^n})$ and P is periodic. Then, by Lemma 3.7.2 and Lemma 3.7.3,

$$\pi((1,0)+P), \pi((1,0)+P) \notin \mathbb{F}_{2^n},$$

but

$$\pi(g((1,0)+P)), \pi(g((1,0)+P)) \in \mathbb{F}_{2^n}.$$

This implies that for any point $Q \in E(\mathbb{F}_{2^{2n}})$ such that $g^m(Q) = (1,0)+P$ or $(1,1)+P$ for some $m \geq 1$, $Q \notin S$. Note that $g((1,0)+P) = g((1,1)+P) = (0,1)+g(P)$, whose tail length is 1. Hence, the projected tree is of height 0. □

Lemma 3.7.8. *Suppose that $P \in E(\mathbb{F}_{2^n})$ and $Q \in E_2(\mathbb{F}_{2^{2n}}) \setminus E_2(\mathbb{F}_{2^n})$. Then $P+Q \notin S$, i.e., x-coordinate of $P+Q$ is not in $\mathbb{F}_{2^n}$.*

Proof. Let $P+Q = (x,y)$ and $g(P)+g(Q) = (u,v)$. Suppose that $P+Q \in S$, i.e., $x \in \mathbb{F}_{2^n}$. Since $Q \in E_2(\mathbb{F}_{2^{2n}}) \setminus E_2(\mathbb{F}_{2^n})$, then $g(Q) \in E_2(\mathbb{F}_{2^n}) \subseteq E(\mathbb{F}_{2^n})$ by Lemma 3.5.2 and Theorem 3.5.1. Since P is $E(\mathbb{F}_{2^n})$, so is $g(P)$. Thus $g(P)+g(Q) \in E(\mathbb{F}_{2^n})$. From 3.2, y is in a field containing both x and v, i.e., $y \in \mathbb{F}_{2^n}$. This implies that $P+Q \in E(\mathbb{F}_{2^n})$, but since $Q \in E_2(\mathbb{F}_{2^{2n}}) \setminus E_2(\mathbb{F}_{2^n})$, $P+Q \notin E(\mathbb{F}_{2^n})$, which is a contradiction. This completes the proof. □

Lemma 3.7.9. *Suppose that n is defined as in Theorem 3.7.6. Then structure of a tree projected from a tree in the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ attached to a periodic point which is in $E(\mathbb{F}_{2^n})$ is a complete binary tree of height $s+1$.*

Proof. Suppose $P \in E(\mathbb{F}_{2^n})$ is a periodic point under g. From the decomposition of $E(\mathbb{F}_{2^{2n}})$ in 3.7, for any point Q in a tree in the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ attached to P, Q can be written as

$$Q = Q_2 + Q_c$$

where $Q_2 \in E_2(\mathbb{F}_{2^{2n}})$ and $Q_c \in E(\mathbb{F}_{2^n})$ is periodic with cycle length bigger than one. Then, by Lemma 3.7.8, $\pi(Q)\mathbb{F}_{2^n}$ if and only if $Q_2 \in \ker g^{s+2}$. This implies that the height of the projected tree by π to $\mathbb{F}_{2^n} \cup \{\infty\}$ is one less than that of the tree in $E(\mathbb{F}_{2^{2n}})$. Hence, the structure of a tree projected from a tree in the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ attached to a periodic point which is in $E(\mathbb{F}_{2^n})$ is a complete binary tree of $s+1$. □

Suppose that x is periodic of cycle length bigger than 1 in the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$. Since g is $2-$*cover* of f, the point above x is also periodic. Since $\mathcal{O}$ is the only fixed point of g and there is no cycle of length 2 in the dynamics of g on $\mathbb{F}_{2^{2n}}$, with Lemma 3.7.7 and Lemma 3.7.9, we have the following theorem which explains the structures of trees attached to cycles of length bigger than one.

Theorem 3.7.10. *In the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$, structures of trees attached to a cycle of length bigger than 1 are identical and they are complete trees of height either 0 or $s+1$.*

Suppose that we want to study the dynamics of f on $\mathbb{F}_{2^5} \cup \{\infty\}$. Then we study that of g on $E(\mathbb{F}_{2^{10}})$ and project it to $\mathbb{F}_{2^5} \cup \{\infty\}$. Figure 3.4 shows how we project the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ to that of f on $E(\mathbb{F}_{2^n})$. Notice that in the

dynamics of g on $E(\mathbb{F}_{2^{10}})$, points painted in blue are points whose $x-$coordinates are not in $\mathbb{F}_{2^5}$ and T represents a binary tree of height 2. Since $5 = 5 \cdot 2^0$, trees in the dynamics of g on $E(\mathbb{F}_{2^{10}})$ are of height 2. Thus trees in the dynamics of f on $\mathbb{F}_{2^5} \cup \{\infty\}$ are height of either 0 or 1. We also see that two components are projected to one component, cycles of length 5 are projected to a cycle of the same length, and a cycle of length 10 is projected to a cycle of length 5. These are consistent with our results.

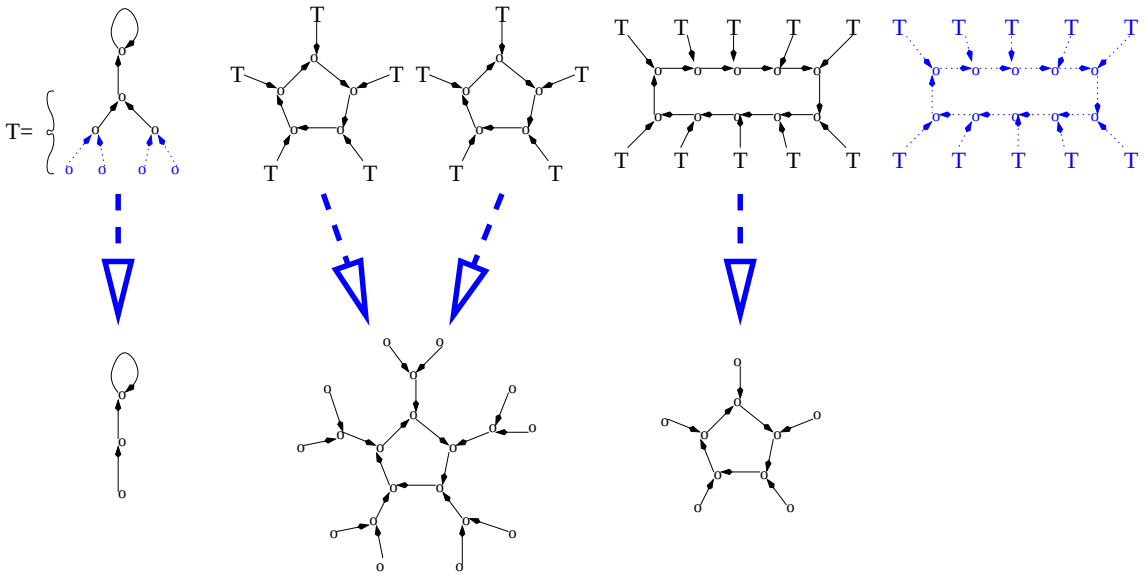


Figure 3.4: Dynamics of g on $E(\mathbb{F}_{2^{10}})$ and that of $f(x) = x + x^{-1}$ on $\mathbb{F}_{2^5} \cup \{\infty\}$.

Chapter 4

Permutation Maps over Finite Fields

4.1 Introduction

A map over a finite field is called a permutation map if it is bijective. Due to the fact that every map over a finite field can be expressed by a polynomial, it was natural to focus on maps defined by polynomials. Since Hermite [1863] investigated permutation polynomials over finite prime fields and Dickson [1897] studied them over general finite fields, numerous mathematicians and engineers have shown their interests in permutation polynomials due not only to their mathematical importance but also to their applications in diverse areas such as coding theory, combinatorics, and cryptography. For more background material on permutation polynomials, we refer the readers to Chapter 7 of [Lidl and Niederreiter, 1997] and, for a detailed survey and some open problems, to [Lidl and Mullen, 1988, 1993].

Two well-known classes of permutation polynomials are monomials x^k over $\mathbb{F}_q$ with $k \geq 1$ and $\gcd(k, q-1) = 1$ and Dickson's polynomials over $\mathbb{F}_q$ with degrees rela-

tively prime to q^2-1. Binomial polynomials of certain forms have been studied by several scholars; see [Akbary and Wang, 2006], [Masuda et al., 2006], [Masuda and Zieve, 2007, 2009], [Turnwald, 1998], and [Wang, 2002]. For permutation polynomials in more general forms, see [Akbary and Wang, 2005], [Park and Lee, 1998], and [Wan and Lidl, 1991].

In this chapter, we take a different approach. Applying finite covering, we construct a new family of permutation maps from known one. Here we introduce a new class of permutation maps over finite fields defined by rational functions that are not equivalent to any known classes of permutation polynomials.

Throughout the chapter $\mathbb{F}_q$ denotes a finite field with q elements, q is a power of an odd prime p, i denotes $\sqrt{-1}$ as an element of $\mathbb{F}_{q^2}$, and α is a nonzero element of $\mathbb{F}_q$. We introduce the following rational map over $\mathbb{F}_q$: for any $k \geq 1$,

$$c_k(x,\alpha) = \frac{a_k(x,\alpha)}{b_k(x,\alpha)}$$

where

$$a_k(x,\alpha) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} (-1)^j \alpha^{2j+1} x^{k-2j}, \qquad b_k(x,\alpha) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j+1} (-1)^j \alpha^{2j+1} x^{k-2j-1}.$$

Theorem 4.1.1. *The rational map $c_k(x,\alpha)$ is a permutation map on $\mathbb{F}_q$ if and only if*

$$\begin{cases} \gcd(k, q-1) = 1 \text{ for } q \equiv 1 \pmod 4, \\ \gcd(k, q+1) = 1 \text{ for } q \equiv 3 \pmod 4. \end{cases}$$

The proof of Theorem 4.1.1 is presented in the next section.

4.2 Proof

We need some simple properties before presenting the proof.

Lemma 4.2.1. *Suppose $\alpha \in \mathbb{F}_q$ with $\alpha \neq 0$. Then For any $x \in \mathbb{F}_q$ with $x \neq \alpha i$ and $y = \frac{x+\alpha i}{x-\alpha i}$, we have*

$$\begin{cases} y^{q-1} = 1 \text{ for } q \equiv 1 \pmod 4, \\ y^{q+1} = 1 \text{ for } q \equiv 3 \pmod 4. \end{cases}$$

Proof. Since $\alpha, x \in \mathbb{F}_q$,

$$y^q = \frac{(x+\alpha i)^q}{(x-\alpha i)^q} = \frac{x+\alpha i^q}{x-\alpha i^q}.$$

Note that $i^q = (-1)^{\frac{q-1}{2}} i$. Thus

$$y^q = \frac{x+\alpha i^q}{x-\alpha i^q} = \begin{cases} \frac{x+\alpha i}{x-\alpha i} = y \text{ for } q \equiv 1 \pmod 4, \\ \frac{x-\alpha i}{x+\alpha i} = 1/y \text{ for } q \equiv 3 \pmod 4. \end{cases}$$

Hence, the proposition follows. □

We rewrite the expressions for $a_k(x,\alpha)$ and $b_k(x,\alpha)$ as follows:

$$a_k(x,\alpha) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} (-1)^j \alpha^{2j+1} x^{k-2j} = \frac{\alpha}{2} \left((x+\alpha i)^k + (x-\alpha i)^k \right), \tag{4.1}$$

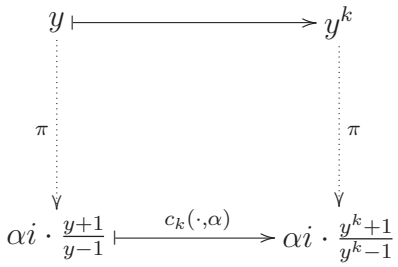
and

$$b_k(x,\alpha) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j+1} (-1)^j \alpha^{2j+1} x^{k-2j-1} = -\frac{i}{2} \left((x+\alpha i)^k - (x-\alpha i)^k \right). \tag{4.2}$$

For $x \neq \alpha i$, let $y = \frac{x+\alpha i}{x-\alpha i}$. Then $y \neq 1$ and, for any $k \geq 1$, we have

$$c_k(x,\alpha) = \begin{cases} \alpha i \cdot \frac{y^k+1}{y^k-1} & \text{for } x \neq \alpha i, \\ \alpha i & \text{for } x = \alpha i. \end{cases}$$

Thus we have the following commutative diagram:



Notice that since $c_k(x,\alpha)$ is a rational map, $c_k(x,\alpha)$ is not defined for $x \in \mathbb{F}_q$ such that $b_k(x,\alpha) = 0$. Thus, for $c_k(x,\alpha)$ to be a permutation map, we need the following lemmas.

Lemma 4.2.2. *Suppose* $q \equiv 1 \pmod 4$. *Then* $b_k(x,\alpha)$ *has no roots in* $\mathbb{F}_q$ *if and only if* $\gcd(k, q-1) = 1$.

Proof. In this case, $\alpha i \in \mathbb{F}_q$. From (4.2), it is easy to see that $\pm\alpha i$ is not the root of $b_k(x,\alpha)$ for any $k \geq 1$. It suffices to consider $\beta \in \mathbb{F}_q$ with $\beta \neq \pm\alpha i$. Notice that $b_k(\beta,\alpha) \neq 0$ if and only if $\left(\frac{\beta+\alpha i}{\beta-\alpha i}\right)^k \neq 1$.

Suppose $\gcd(k, q-1) = 1$. Then the only solution to $X^k = 1$ over $\mathbb{F}_q$ is 1. Since $y = \frac{\beta+\alpha i}{\beta-\alpha i} \neq 1$ and is in $\mathbb{F}_q$, we see that $\left(\frac{\beta+\alpha i}{\beta-\alpha i}\right)^k \neq 1$. Thus $b_k(x,\alpha)$ has no roots in $\mathbb{F}_q$.

Now suppose that $\gcd(k, q-1) = d > 1$. Then there is an element $\gamma \in \mathbb{F}_q$, $\gamma \neq 1$, such that $\gamma^k = 1$. Let $\beta = \alpha i \cdot \frac{\gamma+1}{\gamma-1} \in \mathbb{F}_q$. Then $\gamma = \frac{\beta+\alpha i}{\beta-\alpha i}$, so $\left(\frac{\beta+\alpha i}{\beta-\alpha i}\right)^k = \gamma^k = 1$, i.e., $b_k(\beta,\alpha) = 0$. This completes the proof. □

Lemma 4.2.3. *Suppose* $q \equiv 3 \pmod 4$. *Then* $b_k(x, \alpha)$ *has no roots in* $\mathbb{F}_q$ *if and only if* $\gcd(k, q+1) = 1$.

Proof. The proof will be similar to the proof of Lemma 4.2.2. Suppose that $\gcd(k, q+1) = 1$. For any $\beta \in \mathbb{F}_q$, let $\lambda_\beta = \frac{\beta+\alpha i}{\beta-\alpha i} \neq 1$. Then, since $i \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\lambda_\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then, by Proposition 4.2.1, $\lambda_\beta^{q+1} = 1$. Since $\gcd(k, q+1) = 1$, we have $\lambda_\beta^k \neq 1$. Hence, $b_k(x, \alpha)$ has no roots in $\mathbb{F}_q$.

Now suppose that $\gcd(k, q+1) = d > 1$. Then $X^{q+1} - 1$ has a root in $\mathbb{F}_{q^2}$ that is different from 1, say λ. Then one can check that $\beta = \alpha i \cdot \frac{\gamma+1}{\gamma-1} \in \mathbb{F}_q$ and is a root of $b_k(x, \alpha)$. This completes the proof. □

Lemma 4.2.2 and Lemma 4.2.3 give us the exact condition for the domain of $c_k(x, \alpha)$ to be entire $\mathbb{F}_q$ and notice that this condition is identical to the condition for Theorem 4.1.1. Now we prove the main theorem.

Proof of Theorem 4.1.1. For any $x \in \mathbb{F}_q$, let $y = \frac{x+\alpha i}{x-\alpha i}$ as above. Notice that $i \in \mathbb{F}_q$ only for $q \equiv 1 \pmod 4$, and $c_k(x, \alpha) = \alpha i$ if and only if $x = \alpha i$. We may assume that $x \neq \alpha i$. We have

$$c_k(x, \alpha) = \alpha i \cdot \frac{y^k + 1}{y^k - 1}.$$

Suppose $q \equiv 1 \pmod 4$. Then $i \in \mathbb{F}_q$ and so $y \in \mathbb{F}_q$. Note that the map $y = \frac{x+\alpha i}{x-\alpha i}$ defines a bijection from $\mathbb{F}_q \setminus \{i\}$ to $\mathbb{F}_q \setminus \{1\}$. Also, the map y^k defines a permutation on the subset $\mathbb{F}_q \setminus \{1\}$ if and only if $\gcd(k, q-1) = 1$. Hence, $c_k(x, \alpha)$ is a permutation on $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$.

Now suppose $q \equiv 3 \pmod 4$. Let G be the multiplicative subgroup of $\mathbb{F}_{q^2}$ of order $q+1$. By Lemma 4.2.1, $y \in G \setminus \{1\}$. In fact, the map $y = \frac{x+\alpha i}{x-\alpha i}$ defines a bijection from $\mathbb{F}_q$ to $G \setminus \{1\}$. Note that the map y^k defines a permutation on $G \setminus \{1\}$ if and only if $\gcd(k, q+1) = 1$. It follows that $c_k(x, \alpha)$ defines a permutation on $\mathbb{F}_q$

if and only if $\gcd(k, q+1) = 1$. This completes the proof. $\square$

Chapter 5

Conclusions

Chapter 2 has focused on monomial dynamics over finite fields. We have shown that counting the number of fixed points of boolean monomial dynamics is a $\#P-complete$ problem and investigating cycle structure can be reduced to studying fixed point structure. We also have examined monomial dynamics over general finite fields and seen that investigating it is equivalent to solving linear systems modulo prime power. For the monomial dynamics with more than one component, which have not been covered in this thesis, there is still difficulty in studying cycle structure of such dynamics.

In Chapter 3, we have presented a map $f(x) = x+x^{-1}$ over $\mathbb{F}_{2^n} \cup \{\infty\}$ which is not linear nor a finite-quotient of an affine map, but whose dynamics can be explained with finite covering. We have analyzed the dynamics of f over $\mathbb{F}_{2^n} \cup \{\infty\}$ by lifting to that of an isogeny $g = I + \sigma$ on a Koblitz curve $E : y^2 + xy = x^3 + 1$ over $\mathbb{F}_{2^{2n}}$ whose dynamics is much simpler to understand. We have shown that g satisfies a linear recurrence relation and the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ can be determined by the group decomposition of $E(\mathbb{F}_{2^{2n}})$ and the behavior of the linear recurrence relation over $E(\mathbb{F}_{2^{2n}})$.

In Chapter 4, using finite covering, we have constructed a new class $c_k(x, \alpha)$ of permutation maps over finite fields which has a weaker condition to be permutation than Dickson's polynomials. Notice that $c_k(x, \alpha)$ and the Dickson's polynomial of degree k are projected down from the same map over the quadratic extension with different projection maps.

As mentioned in the introduction, discrete dynamics over finite fields is a young area of mathematics. In this thesis, we have investigated some of interesting problems. But there are many interesting questions yet to be explored. It would be interesting to investigate the following questions:

- What is "simple" dynamics ? How do we measure simplicity of discrete dynamics ?
- When can a dynamics be covered by a simple dynamics ?
- How do we study dynamics defined by morphism in higher dimensional algebraic varieties ?
- How does the algebraic structure of the set affect the dynamics ?
- What other algebraic techniques can be used to study dynamics ?

We believe that answering these questions will contribute greatly to discrete dynamics. Since there are numerous applications of discrete dynamics such as reverse-engineering problems [Laubenbacher and Stigler, 2004], modeling of gene regulatory networks [Albert and Othmer, 2003; Celada and Seiden, 1992], and building secure cryptosystems [Habutsu et al., 1991], exploring the above questions will provide interesting and challenging research directions as well.

Bibliography

Akbary, A. and Wang, Q. (2005). On some permutation polynomials over finite fields. *International Journal of Mathematics and Mathematical Sciences*, 2005:2631–2640.

Akbary, A. and Wang, Q. (2006). A generalized lucas sequence and permutation binomials. *Proceedings of the American Mathematical Society*, 134:15–22.

Albert, R. and Othmer, H. (2003). The topology of the regulatory interactions predicts the expression patterns of the segment polarity genes in drosophila melanogaster. *Journal of Theoretical Biology*, 223:1–18.

Celada, F. and Seiden, P. (1992). A computer model of cellular interactions in the immune system. *Immunology today*, 13(2).

Colón-Reyes, O., JarrahR., A., Laubenbacher, R., and Sturmfels, B. (2006). Monomial dynamical systems over finite fields. *ArXiv Mathematics e-prints*.

Colón-Reyes, O., Laubenbacher, R., and Pareigis, B. (2004). Boolean monomial dynamical systems. *Annals of Combinatorics*, 8.

Devaney, R. (2003). *An Introduction to Chaotic Dynamical System*. Westview Press, second edition.

Dickson, L. (1896-1897). The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Annals of Mathematics*, 11(1/6).

Elspas, B. (1959). The theory of autonomous linear sequential networks. *IRE Transactions on Circuit Theory*, CT-6(1).

Gilbert, C., Kolesar, J., Reiter, C., and Stroey, J. (2001). Function digraphs of quadratic maps modulo p. *The Fibonacci Quarterly*, 39.

Habutsu, T., Nishio, Y., Sasase, I., and Mori, S. (1991). A secret key cryptosystem by iterating a chaotic map. *Eurocrypt*.

Hermite, C. (1863). Sur les fonctions de sept lettres. *Comptes Rendus des Sèances de l'Académie des Sciences*, 57.

Hernandez-Toledo, R. (2005). Linear finite dynamical systems. *Communications in Algebra*, 33.

Hjorth, P. and Petersen, C. (2006). *Dynamics on the Riemann Sphere: A Bodil Branner Festschrift*. European Mathematical Society.

Jarrah, A., Laubenbacher, R., and Veliz-Cuba, A. (2008). The dynamics of conjunctive and disjunctive boolean networks. arXiv:0805.0275v1.

Jarrah, A., Laubenbacher, R., and Vera-Licona, P. (2006). An efficient algorithm for finding the phase space structure of liner finite dynamical systems.

Knuth, D. and Ruskey, F. (2003). Efficient coroutine generation of constrained gray sequences. *Lecture Notes in Computer Science*, 2635.

Koblitz, N. (1991). Cm-curves with good cryptographic properties. In Feigenbaum, J., editor, *Advances in Cryptology - Proceedings of CRYPTO 1991, LNCS*, volume 576, pages 279–287, London, UK. Springer-Verlag.

Laubenbacher, R. and Stigler, B. (2004). A computational algebra approach to the reverse-engineering of gene regulatory networks. *Journal of Theoretical Biology*, 229.

Lidl, R. and Mullen, G. (1988). When does a polynomial over a finite field permute the elements of the field? *American Mathematical Monthly*, 95.

Lidl, R. and Mullen, G. (1993). When does a polynomial over a finite field permute the elements of the field? ii. *American Mathematical Monthly*, 100.

Lidl, R. and Niederreiter, H. (1997). *Finite Fields*. Cambridge University Press, New York.

Masuda, A., Panario, D., and Wang, Q. (2006). The number of permutation binomials over $\tilde{f}_{4p+1}$ where p and $4p+1$ are primes. *Electronic Journal of Combinatorics*, 13.

Masuda, A. and Zieve, M. (2007). Nonexistence of permutation binomials of certain shapes. *Electronic Journal of Combinatorics*, 14.

Masuda, A. and Zieve, M. (2009). Permutation binomials over finite fields. *TRANSACTIONS OF THE AMERICAN MATHEMATICAL SOCIETY*, 361(8).

Menezes, A., Blake, I., Gao, S., Mullin, R., Vanstone, S., and Yaghoobiann, T. (1992). *Applications of Finite Fields*. Kluwer Academic Publishers.

Milne, J. (2009). Algebraic number theory (v3.01). Available at www.jmilne.org/math/.

Park, J. (2003). Algebraic properties of the digraph generated by the iteration of quadratic mapping $x \mapsto x^2 - 2 \pmod{p}$. manuscript.

Park, Y. and Lee, J. (1998). Permutation polynomials with exponents in an arithmetic progression. *Bulletin of the Australian Mathematical Society*, 57.

Provan, J. and Ball, M. (1983). Complexity of counting cuts. *Siam Journal of Computing*, 12.

Robinson, C. (1998). *Dynamical Systems - Stability, Symbolic Dynamics, and Chaos*. CRC.

Rogers, T. (1996). The graph of the square mapping on the prime fields. *Discrete Mathematics*, 148.

Rück, H. (1987). A note on elliptic curve over finite fields. *Mathematics of Computation*, 179.

Silverman, J. (1986). *The Arithmetic of Elliptic Curves*. Springer.

Turnwald, G. (1998). Permutation polynomials of binomial type. *Contributions to General Algebra*, 6.

Valiant, L. (1979). The complexity of computing the permanent. *Theoretical Computer Science*, 8.

Vasiga, T. and Shallit, J. (2004). On the itereation of certain quadratic maps over $gf(p)$. *Discrete Mathematics*, 277.

Wan, D. and Lidl, R. (1991). Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. *Monatshefte für Mathematik*, 112.

Wang, L. (2002). On permutation polynomials. *Finite Fields and Their Applications*, 8.

Weil, A. (1948). *Courbes algébriques et variètès abéliennes. Sur les courbes algébriques et les varietés qui s'en deduisent*. Hermann.

Xua, G. and Zoub, Y. (2009). Linear dynamical systems over finite rings. *Journal of Algebra*, 321(8).

Zieve, M. (1996). *Cycles of Polynomial Mappings*. PhD thesis, University of California at Berkeley.