Dynamics of $f(x) = x + x^{-1}$ via Elliptic Curves

Jang-Woo Park

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA

Shuhong Gao

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA

Abstract

Understanding the dynamics of nonlinear maps is an important but difficult problem, and there are not many methods available. In this paper, we study the dynamics of a simple function, $f(x) = x + x^{-1}$, on fields of characteristic two and provide explicit information about structure of it. The main idea is to lift it to the dynamics of an isogeny on an elliptic curve and study the dynamics of the isogeny.

Keywords: dynamics over finite fields, elliptic curves, function iteration
2000 Mathematics Subject Classification: 37P05, 11G20, 11T99

1. Introduction

A dynamical system consists of a set V and a map $f : V \to V$. For any point $v \in V$, we can iterate f by defining $f^0(v) = v$ and $f^i(v) = f(f^{i-1}(v))$ for $i \geq 1$. 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 $f^m(v) = v$, and such a minimum m is called the **cycle length** of v under f. A point v is called **preperiodic** if the orbit of v is finite. In this case, the orbit of v contains a cycle, and the tail length of v is the smallest n such that $f^n(v)$ is cyclic.

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 and 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. In a classical dynamical system, it is important to understand the limiting behaviors of orbits and to characterize the Julia set. For more on classical dynamical system, we recommend [6] and [21].

Email addresses: `jpark@clemson.edu` (Jang-Woo Park), `sgao@math.clemson.edu` (Shuhong Gao)

Understanding dynamical systems 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 a discrete dynamical system 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 $f(v) = w$. Then the graph consists of a collection of cycles with each node on the cycles having a tree. We are interested in understanding the distribution of the cycle lengths and the tree structures.

Although one 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. For dynamical systems over finite fields, there are only a few cases that have been studied so far. For linear dynamical systems, Elspas [7] 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 [12] 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. [13] presented an algorithms which describes the phase spaces. Xua and Zoub [27] 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. Barta and Morton [2, 3] studied the dynamics of certain types of polynomials over algebraic closure of finite fields. Zieve [28] investigated the cycle lengths of polynomial maps over various rings. Even dynamics of quadratic 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 [22] and the dynamics of $f(x) = x^2 - 2$ over prime fields was analyzed in [9], [20], and [26]. For monomial dynamics, Jarrah et al. [14] provided an analysis of boolean monomial dynamical systems and Colón-Reyes et al. [5] showed that the structure of fixed points of monomial dynamics over general finite fields can be reduced to boolean monomial dynamics.

In this paper, we are interested in the dynamics of a simple map $f(x) = x + x^{-1}$, $x \in \mathbb{F}$, where $\mathbb{F}$ is any field. We make the convention that $f(0) = \infty$ and $f(\infty) = \infty$. So f can be viewed as a function on the projection space, $\mathbb{F} \cup \{\infty\}$. We are interested in the case when $\mathbb{F}$ is a finite field. We did extensive computer experiments on the dynamical systems of f over finite fields. It showed that the dynamics of f over finite fields of odd characteristics look quite random, but very regular over fields of characteristic two. For example, each connected component of the graph is a cycle with binary tree of the same height attached to each node. Figure 1 shows the dynamics of f on $\mathbb{F}_{2^5} \cup \{\infty\}$. We want to understand the mathematical reasons behind this phenomenon.

In the next Section, we present the concept of finite covering as a general framework for understanding dynamical systems. In particular, we show that the dynamics of $f(x) = x + x^{-1}$ on a field of characteristic two can be lifted to a dynamical system on an elliptic curve on $\overline{\mathbb{F}}_2$, i.e. so-called the Koblitz

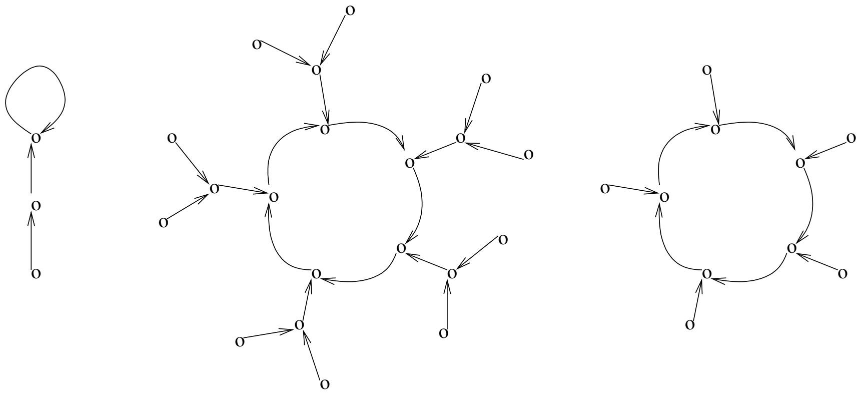

Figure 1: Dynamics of $f(x) = x + x^{-1}$ on $\mathbb{F}_{2^5} \cup \{\infty\}$.

curve E, with corresponding dynamics defined by an isogeny g(i.e. g is a group homomorphism of the elliptic curve group). In Section 3, we describe the recurrence relation of g using the minimum polynomial of g. In Section 4, we examine the group structure of $E(\mathbb{F}_{2^n})$ and its relation to the structure of the endomorphism ring $End(E)$ of the elliptic curve E. In Section 5, we analyze the cycle structure of g and show that the cycle lengths can be determined by the group structure of $E(\mathbb{F}_{2^n})$ and the linear recurrence relation of g. In Section 6, we prove that all trees attached to the cycle of g are complete binary trees of the same height and show how to determine the exact height of trees. In Section 7, we project the dynamics of g on $E(\mathbb{F}_{2^{2n}})$ to that of f on $\mathbb{F}_{2^n} \cup \{\infty\}$. In Section 8, we conclude with a few interesting questions.

2. Understanding Dynamics via Finite Covering

Let V be an algebraic variety and $f : V \to V$ be any morphism. We want to understand the dynamics of f on V. We say that f is covered by a morphism $g : W \to W$ where W is an algebraic variety if there is a finite dominant morphism $\pi : W \to V$ so that the following diagram is commutative:

$$\begin{tikzcd}
W \arrow[r, "g"] \arrow[d, "\pi"'] & W \arrow[d, "\pi"] \\
V \arrow[r, dotted, "f"] & V
\end{tikzcd}$$

The commutativity of the diagram implies that each orbit of g on W is projected by π to an orbit of f on V. Hence each cycle of g yields a cycle of f, though of possibly smaller length. Since π is dominant, then almost all cycles of f can be obtained this way from g. If the dynamics of g is easier to analyze, then we may understand the dynamics of f via that of g. The question is, for a given morphism f on V, how to decide if f is covered by a simpler dynamics of g on some algebraic variety W. We illustrate this idea by the following example. Let k be a field and $f(x) = x^2 - 2$ which defines a dynamics on $V = k$. The dynamics of f is nontrivial to see and is in fact the subject of some recent papers [9], [20], and [26]. Now let $W = \{(u, v) \in K^2 : uv = 1\}$ where K is an extension of k that contains all the square roots of elements in k, and let $g : W \to W$ be defined by $g(u, v) = (u^2, v^2)$. Then we have the following diagram:

$$\begin{tikzcd}
(u,v) \arrow[r, mapsto, "g"] \arrow[d, dotted, "\pi"'] & (u^2,v^2) \arrow[d, dotted, "\pi"] \\
x \arrow[r, mapsto, "f"] & x^2-2
\end{tikzcd}$$

where $\pi : W \to V$ is defined by $\pi(u, v) = u + v$. Since $\pi(u^2, v^2) = \pi(u, v)^2 - 2$, the above diagram is commutative. As π is a 2-cover, any odd cycle of g projects (via π) to a cycle of f of the same length, and any even cycle of g projects to a cycle of half length. So we can explain the dynamics of f by studying the dynamics of g which is the squaring map. Especially if $k = \mathbb{F}_q$, then $K = \mathbb{F}_{q^2}$ and the cycle lengths of g are the orders 2 modulo m where $m|q^2 - 1$. f has a special name which is the Dickson's polynomial $D_2(x, 1)$. In fact, using the same method, we can analyze the complete structure of the dynamics of the is the Dickson's polynomials $D_n(x, 1)$ for any n.

Especially the rational maps covered by elliptic curve endomorphisms are called Lattès maps. Since the dynamics of endomorphisms on elliptic curves are simpler due to the structure of elliptic curve groups, the dynamics of Lattès maps show more regularities than that of arbitrary rational maps. They have been studied for years primarily over the complex numbers. [18] provides excellent introduction to Lattès maps over $\mathbb{C}$. They also have been studied over other fields such as algebraically closed fields and local fields. For more on Lattès maps over these fields, we recommend Chapter 6 of [25]. In [8], [19], and [10], Lattès maps over finite fields plays very important roles to solve the Schur problem for polynomials and rational functions. Now we consider a covering of the map $f(x) = x + x^{-1}$ over fields of characteristic 2. Let E be the elliptic curve group over the algebraic closure $\overline{\mathbb{F}}_2$ defined by

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

This curve is sometimes called Koblitz curve, due to its use in cryptosystems [15].

Then, with the point $\mathcal{O}$ at infinity, E forms an abelian group with respect to the addition of points. 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 $P = (x, y) \notin \{\mathcal{O}, (0, 1)\}$,

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

where

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

and

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

Thus we have the following commutative diagram[1]:

$$\begin{tikzcd}
E \arrow[r, "g"] \arrow[d, "\pi"'] & E \arrow[d, "\pi"] \\
\overline{\mathbb{F}}_2 \cup \{\infty\} \arrow[r, dotted, "f"] & \overline{\mathbb{F}}_2 \cup \{\infty\}
\end{tikzcd}$$

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 $\mathbb{F}_{2^{2n}}$ 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 $\mathbb{F}_{2^n} \cup \{\infty\}$, i.e. f is a Lattès map over fields of characteristic 2. We shall see below that this will enable us to have a good understanding of the dynamics of g on $E(\mathbb{F}_{2^{2n}})$, hence of f on $\mathbb{F}_{2^n} \cup \{\infty\}$.

Throughout this paper, E will denote the elliptic curve as defined in (1), $End(E)$ denotes the ring of endomorphisms of E, $E[m]$ indicates m-torsion group of E over algebraic closure, and, for a field k, $E(k)[m]$ represents $E[m] \cap E(k)$. For a 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. Recurrence Relation of g on E and $g-$invariant subgroups of E

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

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

[1] Observed by H.W. Lenstra, Jr.

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

$$g^2 - g + 2 = 0 \tag{3}$$

as a group homomorphism on E. Then we have the following recurrence relation: for any $t \geq 1$,

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

Let

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

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

$$\begin{pmatrix} g^t(P) \\ g^{t+1}(P) \end{pmatrix} = M^t \begin{pmatrix} P \\ g(P) \end{pmatrix}. \tag{5}$$

Thus, for $t \geq 0$, $g^t(P) = P$ if and only if

$$M^t \begin{pmatrix} P \\ g(P) \end{pmatrix} = \begin{pmatrix} P \\ g(P) \end{pmatrix}. \tag{6}$$

So, for a point $P \neq \mathcal{O}$, P is cyclic if and only if there is a positive integer t satisfying (6), and the smallest such t gives the cycle length of P under g.

Let $\ker g$ deonte the set of points P in E such that $g(P) = \mathcal{O}$. Then one can check that $\ker g = \{\mathcal{O}, (0, 1)\}$. Moreover, $(0, 1)$ is the only point in E of order 2. For any point P in E, the order of P,denoted by $|P|$, is the smallest positive integer such that $mP = \mathcal{O}$.

Proposition 3.1. *Suppose $P \in E$ and $|P| = m$. Then*

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

Proof. Note that since g is an endomorphism on E, for any $P \in E$,

$$n \cdot g(P) = \mathcal{O} \Leftrightarrow g(nP) = \mathcal{O} \Leftrightarrow nP \in \ker g \Leftrightarrow 2nP = \mathcal{O}.$$

This completes the proof. □

Note that $E(\mathbb{F}_{2^n})$ is a finite abelian group. Thus it is decomposed as

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

As an immediate consequence of Proposition 3.1, we have the following corollary:

Corollary 3.2. *For each prime p, $E_p(\mathbb{F}_{2^n})$ is g-invariant. Furthermore, g is a 2-to-1 map on $E_2(\mathbb{F}_{2^n})$ and g is an automorphism on $E_p(\mathbb{F}_{2^n})$ for odd p.*

Hence we may focus on the dynamics of g on the p-subgroups of E for each prime p dividing $\#E(\mathbb{F}_{2^n})$. Before proceeding further, we need to understand the group structure of $E_p(\mathbb{F}_{2^n})$.

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

Note that $E(\mathbb{F}_{2^n}) = \ker(\sigma^n - 1)$. Define the sequence a_n by $a_0 = 2$, $a_1 = 1$, and $a_{n+1} = a_n - 2a_{n-1}$ for all $n \geq 1$. Then, by [15],

$$\#E(\mathbb{F}_{2^n}) = 2^n + 1 - a_n$$

By Theorem 3 in [23],

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

i.e., $E_2(\mathbb{F}_{2^n})$ is a cyclic group of order 2^{h_2} for some integer h_2. We will give more details of the size of $E_2(\mathbb{F}_{2^n})$ in depth in Section 6. Now we focus on $E_p(\mathbb{F}_{2^n})$ for an odd prime p dividing $\#E(\mathbb{F}_{2^n})$. Theorem 3 in [23] also says

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

where $0 \leq e_p \leq h_p$. The following lemma provides a basic tool to study the group structure of $E(\mathbb{F}_{2^n})$.

Lemma 4.1 ([23])**.** *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 $w \in End(E)$.*

Let $End(E)$ be the endomorphism ring of E. We know that from [24] that $End(E) = \mathbb{Z}[\sigma]$. As $\sigma^2 + \sigma + 2 = 0$, we may identify σ with $\frac{-1+\sqrt{-7}}{2}$, so $\overline{\sigma} = \frac{-1-\sqrt{-7}}{2}$. The factorization of a prime p in $\mathbb{Z}[\sigma]$ depends on $\left(\frac{-7}{p}\right)$. By the quadratic reciprocity,

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

For our purpose, we denote $\nu_{\mathfrak{p}}(\cdot)$ the valuation corresponding to a prime $\mathfrak{p}$ in $\mathbb{Z}[\sigma]$. For a 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 4.2. *Let $p \in \mathbb{Z}$ be a prime with $p \neq 2$. Suppose $\sigma^n - 1 = p^t \cdot w \in \mathbb{Z}[\sigma]$ where $p \nmid w$. Then*

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^t) \times \mathbb{Z}/(p^{t+\nu})$$

with $\nu = \nu_p(w\bar{w})$ 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 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 [24], we know that

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

and

$$\#E(\mathbb{F}_{2^n}) = (\sigma^n - 1)(\overline{\sigma}^n - 1). \tag{7}$$

Thus

$$\#E(\mathbb{F}_{2^n}) = (\sigma^n - 1)(\overline{\sigma}^n - 1) = (p^t \cdot w)(p^t \cdot \overline{w}) = p^{2t} \cdot w\overline{w}. \tag{8}$$

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 $E[p^{t+1}]$,

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^t) \times \mathbb{Z}/(p^{t+\nu})$$

where $\nu = \nu(w\overline{w})$. □

Lemma 4.3. *Suppose $e \geq 1$ and $\mathfrak{p} \subseteq \mathbb{Z}[\sigma]$ is a prime ideal and n_0 is the smallest natural number such that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) = e$. 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, $n_0 | n$. □

Corollary 4.4. *Suppose $\mathfrak{p} \subseteq \mathbb{Z}[\sigma]$ is a prime ideal above an odd prime p and n_0 is the smallest natural number such that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) > 0$. Then n_0 is the multiplicative order of σ modulo $\mathfrak{p}$ and also the smallest natural number such that $p | \#E(\mathbb{F}_{2^{n_0}})$.*

Proof. For p which ramifies or stays prime in $\mathbb{Z}[\sigma]$, it is obvious. So suppose $(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}} \in \mathbb{Z}[\sigma]$ and n_0 is the smallest natural number such that $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) > 0$. Then, by the definition, n_0 the multiplicative order of σ modulo $\mathfrak{p}$. It is also true that n_0 is also the smallest natural number such that $\nu_{\overline{\mathfrak{p}}}(\overline{\sigma}^{n_0} - 1) > 0$. Hence, from the equation (7), $p | \#E(\mathbb{F}_{2^{n_0}})$ and n_0 is the smallest. □

Lemma 4.5. *Suppose that $m \geq 1$, p is an odd prime, and n_0 is the smallest natural number such that $\nu_p(\sigma^{n_0} - 1) = m$. Then the smallest $n > n_0$ such that $\nu_p(\sigma^n - 1) > m$ is pn_0. Moreover, $\nu_p(\sigma^{pn} - 1) = m + 1$.*

Proof. Since $\nu_p(\sigma^{n_0} - 1) = m$,

$$\sigma^{n_0} = 1 + cp^m + c_1 p^{m+1}$$

where $c, c_1 \in \mathbb{Z}[\sigma]$ with $p \nmid c$. Then

$$\sigma^{pn_0} \equiv 1 + cp^{m+1} + c\binom{p}{2}p^{2m} \pmod{p^{m+2}}. \tag{9}$$

When $m = 1$, since p is odd,

$$p \nmid \left(1 + \frac{p(p+1)}{2}\right),$$

so $\nu_p(\sigma^{pn_0}-1)=2$. When $m>1$, from the equation (9),

$$\sigma^{pn_0} \equiv 1+cp^{m+1} \pmod{p^{m+2}},$$

so $\nu_p(\sigma^{pn_0}-1)=m+1$. Suppose n is the smallest such that $\nu_p(\sigma^n-1)>m$. From Lemma 4.3, $n=kn_0$ with $1\leq k\leq n_0$. Note

$$\sigma^{kn_0} \equiv 1+ck\cdot p^m \pmod{p^{m+2}}.$$

So $\nu_p(\sigma^{kn_0}-1)>m$ if and only if $p|k$, i.e., $k=p$. Hence, $n=pn_0$ and $\nu_p(\sigma^{pn_0}-1)=m+1$. □

Lemma 4.5 gives us the following useful corollary.

Corollary 4.6. *Let p be an odd prime and n_0 is the smallest natural number such that $p|(\sigma^{n_0}-1)$. Suppose $n=n_0p^en'$ where $p\nmid n'$. Then $\nu_p(\sigma^n-1)=e+\nu_p(\sigma^{n_0}-1)$.*

Lemma 4.7. *Suppose $\mathfrak{p}\subseteq\mathbb{Z}[\sigma]$ is a prime ideal above an odd 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 $m=p\cdot n$ where $p\in\mathbb{Z}$ 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 Lemma 4.3, 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 $\sigma^n\equiv 1 \pmod{\mathfrak{p}}$,

$$B=\sigma^{(k-1)n}+\cdots+\sigma^n+1\equiv k \pmod{\mathfrak{p}}. \qquad (10)$$

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

Now let $k=p$ and $B\equiv p \pmod{\mathfrak{p}}$. Suppose p does not ramify. Then either $(p)=\mathfrak{p}$ or $(p)=\mathfrak{p}\cdot\overline{\mathfrak{p}}$, thus $\nu_{\mathfrak{p}}(p)=1$ in either case. If $\nu_p(\sigma^n-1)=1$, then $\sigma^n=1+c$ where $\nu_{\mathfrak{p}}(c)=1$ and

$$\sigma^{pn}=(1+c)^p\equiv 1+c\cdot p+c^2\binom{p}{2} \pmod{\mathfrak{p}^3}.$$

As p is odd, $\binom{p}{2}$ is divisible by p, so $c^2\binom{p}{2}\equiv 0 \pmod{\mathfrak{p}^3}$. Hence

$$\sigma^{pn}\equiv 1+c\cdot p \pmod{\mathfrak{p}^3}.$$

Since $\nu_{\mathfrak{p}}(p)=1$,

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

Thus $\nu_p(\sigma^{pn} - 1) = 2$. If $\nu_{\mathfrak{p}}(\sigma^n - 1) = e \geq 2$, then, in the equation (10), for $k = p$,

$$B \equiv p \pmod{\mathfrak{p}^2},$$

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

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

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

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

This completes the proof. □

For a prime p, let $\mathrm{Ord}_p(\alpha)$ denote the multiplicative order of α modulo p where α can be an integer or integer matrix and, for an ideal I contained in a ring R and an element $\alpha \in R$, $\mathrm{Ord}_I(\alpha)$ indicates the multiplicative order of α modulo I.

Theorem 4.8. *For any odd prime p, let $\mathfrak{p}$ be a prime ideal above p in $\mathbb{Z}[\sigma]$ and $n_0 = Ord_{\mathfrak{p}}(\sigma)$. Then $p | \# E(\mathbb{F}_{2^n})$ if and only if $n_0 | n$. Moreover, suppose $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) = u$ and $n = n_0 p^v n'$ with $p \neq n'$. Then*

(a) for p with $\left(\frac{p}{7}\right) = -1$,

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{u+v}) \times \mathbb{Z}/(p^{u+v})$$

(b) for p with $\left(\frac{p}{7}\right) = 1$,

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{e_0+v}) \times \mathbb{Z}/(p^{u+v})$$

where $e_0 = \nu_p(\sigma^{n_0} - 1)$,

(c) for $p = 7$, $n_0 = 6$ with $u = 1$ and

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

Proof. Suppose p is an odd prime. Let $\mathfrak{p} \in \mathbb{Z}[\sigma]$ be a prime ideal above p and $n_0 = \mathrm{Ord}_{\mathfrak{p}}(\sigma)$. Then. by Lemma 4.3 and Corollary 4.4, $p | \# E(\mathbb{F}_{2^n})$ if and only if $n_0 | n$. Let $\nu_{\mathfrak{p}}(\sigma^{n_0} - 1) = u$ and $n = n_0 p^v n'$ with $p \neq n'$. Suppose $\left(\frac{p}{7}\right) = -1$. Then, since p stays prime in $\mathbb{Z}[\sigma]$, $\nu_p(w\overline{w}) = 0$ in (8). Thus, by Lemma 4.2 and Corollary 4.6,

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{u+v}) \times \mathbb{Z}/(p^{u+v})$$

Suppose p is an odd prime with $\left(\frac{p}{7}\right) = 1$. Let $e_0 = \nu_p(\sigma^{n_0} - 1)$. Then

$$\sigma^{n_0} - 1 = p^{e_0} \cdot w$$

where $w \in \mathbb{Z}[\sigma]$ with $\nu_{\mathfrak{p}}(w) = u - e_0$. Then, by Corollary 4.6,

$$\nu_p(\sigma^n - 1) = e_0 + v$$

and, by Lemma 4.7,

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

Thus, by Lemma 4.2,

$$E_p(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(p^{e_0+v}) \times \mathbb{Z}/(p^{u+v})$$

Suppose $p = 7$. Let $\mathfrak{p} = (\sigma - 3, 7)$, the prime ideal above (7) in $\mathbb{Z}[\sigma]$. Since $\sigma \equiv 3 \pmod{\mathfrak{p}}$ and $\mathrm{Ord}_{\mathfrak{p}}(3) = \mathrm{Ord}_7(3) = 6$, $n_0 = 6$. Note that $\sigma^6 - 1 = (\sigma^3 - 1)(\sigma^3 + 1)$. Thus $\nu_{\mathfrak{p}}(\sigma^6 - 1) = \nu_{\mathfrak{p}}(\sigma^3 + 1)$. From the minimum polynomial of σ, we know that $\sigma^3 + 1 = -\sigma + 3$, which is not divisible by 7. Thus $u = \nu_{\mathfrak{p}}(\sigma^6 - 1) = 1$. Now suppose $6|n$. Then

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

By Lemma 4.7, the smallest n such that $\nu_{\mathfrak{p}}(\sigma^n - 1) > 1$ is $6 \cdot 7$. We need to determine $\nu_{\mathfrak{p}}(\sigma^{6\cdot 7} - 1)$. 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

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

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 4.7 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 $n = 6 \cdot 7^v \cdot n'$ where $7 \nmid n'$,

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

□

5. Cycle Structures of the dynamics of g on $E(\mathbb{F}_{2^n})$

Let p be an odd prime and $P \in E_p(\overline{\mathbb{F}}_2)$. To determine the integer t in (4), we need to know the intersection of the subgroup generated by P and $g(P)$, respectively. From now on, for any point $P \in E(\overline{\mathbb{F}}_2)$, $\mathrm{Cl}_g(P)$ denotes the cycle length of P under g.

Theorem 5.1. *Let $P \in E_p(\mathbb{F}_{2^n})$ with $|P| = p^{e_1} > 1$. Suppose $\langle P \rangle \cap \langle g(P) \rangle = \{\mathcal{O}\}$. Then $Cl_g(P) = Ord_{p^{e_1}}(M)$ where M is as in (4) and $Ord_{|P|}(M)$ denotes the multiplicative order of M modulo p^{e_1}.*

Proof. Since $\langle P \rangle \cap \langle g(P) \rangle = \{\mathcal{O}\}$,

$$M^t \begin{pmatrix} P \\ g(P) \end{pmatrix} = \begin{pmatrix} P \\ g(P) \end{pmatrix}$$

if and only if $M^t \equiv I \pmod{p^{e_1}}$. Hence $\mathrm{Cl}_g(P) = \mathrm{Ord}_{p^{e_1}}(M)$. □

Next we need to know when the intersection is nontrivial.

Lemma 5.2. *Let p be an odd prime. Suppose there is a point $P \in E_p(\overline{\mathbb{F}}_2)$ such that $|P| = p^{e_1} > 1$ and $|\langle P \rangle \cap \langle g(P) \rangle| = p^{e_2} > 1$. Then there is an integer λ such that*

$$g(p^{e_1-e_2}P) = \lambda p^{e_1-e_2}P \quad \textit{and} \quad \lambda^2 - \lambda + 2 \equiv 0 \pmod{p^{e_2}}.$$

Hence $X^2 - X + 2$ is reducible modulo p.

Proof. There are integers u and v such that

$$uP = vg(P) \text{ and } \langle P \rangle \cap \langle g(P) \rangle = \langle uP \rangle = \langle vg(P) \rangle. \tag{11}$$

Since P and $g(P)$ have the same order p^{e_1}, we have

$$\nu_p(u) = p^{e_1-e_2} \text{ and } \nu_p(v) = p^{e_1-e_2}.$$

Let $u = u_1 p^{e_1-e_2}$ and $v = v_1 p^{e_1-e_2}$ where $p \nmid u_1$ and $p \nmid v_1$, and let

$$\lambda \equiv u_1/v_1 \pmod{p^{e_2}}.$$

Then the equation (11) implies that

$$p^{e_1-e_2}\lambda P = p^{e_1-e_2}g(P).$$

Let $Q = p^{e_1-e_2}P$. Then Q has the order p^{e_2} and $g(Q) = \lambda Q$. Since $g^2 - g + 2 = 0$, we have

$$g(g(Q)) - g(Q) - 2Q = \mathcal{O},$$

hence

$$(\lambda^2 - \lambda + 2)Q = \mathcal{O}.$$

Therefore $\lambda^2 - \lambda + 2 \equiv 0 \pmod{p^{e_2}}$. □

5.1. Dynamics of g on $E_7(\mathbb{F}_{2^n})$

Lemma 5.3. *For any $P \in E_7(\mathbb{F}_{2^n})$,*

$$|\langle P\rangle \cap \langle g(P)\rangle| = 1 \text{ or } 7.$$

Proof. If $|P| = 7$, then it is obvious. Thus, for the rest of the proof, we assume that $|P| = 7^{e_1}$ with $e_1 \geq 2$ and $|\langle P\rangle \cap \langle g(P)\rangle| = 7^{e_2} > 1$. By the proof of Lemma 5.2, there exists an integer λ such that $g(7^{e_1-e_2}P) = \lambda 7^{e_1-e_2}P$ and $\lambda^2 - \lambda + 2 \pmod{7^{e_2}}$. Note that $X^2 - X + 2 = (X-4)^2 + 7(X-2)$. Then we see that $X^2 - X + 2 \equiv (X-4)^2 \pmod 7$, but $X^2 - X + 2$ is not reducible modulo 7^e for $e \geq 2$. This forces $e_2 = 1$ and $\lambda \equiv 4 \pmod 7$. □

Theorem 5.4. *Suppose $P \in E_7(\mathbb{F}_{2^n})$ with $|P| = 7^c$ and $P \neq \mathcal{O}$. Then*

$$Cl_g(P) = \begin{cases} Ord_{7^c}(M) & \text{if } |\langle P\rangle \cap \langle g(P)\rangle| = 1, \\ Ord_7(4) & \text{if } c = 1 \text{ and } |\langle P\rangle \cap \langle g(P)\rangle| = 7, \\ Ord_{7^{c-1}}(M) & \text{if } c > 1 \text{ and } |\langle P\rangle \cap \langle g(P)\rangle| = 7. \end{cases}$$

Proof. By Theorem 5.1, if $|\langle P\rangle \cap \langle g(P)\rangle| = 1$, then $\mathrm{Cl}_g(P) = \mathrm{Ord}_{7^c}(M)$. Thus we suppose that $|\langle P\rangle \cap \langle g(P)\rangle| = 7$. If $c = 1$, then $\langle P\rangle = \langle g(P)\rangle$ and, from the proof of Lemma 5.3, we know $g(P) = 4 \cdot P$. Thus $\mathrm{Cl}_g(P) = \mathrm{Ord}_7(4) = 3$. Now suppose $c > 1$. Then, from the proof of Lemma 5.3,

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

Let $t = \mathrm{Ord}_{7^{c-1}}(M)$ for $c \geq 2$. Using the induction, one can show that

$$(M^t - I) \equiv \begin{pmatrix} 4 \cdot 7^{c-1} & 6 \cdot 7^{c-1} \\ 2 \cdot 7^{c-1} & 3 \cdot 7^{c-1} \end{pmatrix} \pmod{7^c}.$$

Thus

$$\begin{aligned} (M^t - I)\begin{pmatrix} P \\ g(P) \end{pmatrix} &= \begin{pmatrix} 4 \cdot 7^{c-1}P + 6 \cdot 7^{c-1}g(P) \\ 2 \cdot 7^{c-1}P + 3 \cdot 7^{c-1}g(P) \end{pmatrix} \\ &= \begin{pmatrix} 4 \cdot 7^{c-1}P + 3 \cdot 7^{c-1}P \\ 2 \cdot 7^{c-1}P + 5 \cdot 7^{c-1}P \end{pmatrix} \\ &= \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}. \end{aligned}$$

Since t is the smallest such that $M^t \equiv I \pmod{7^{c-1}}$, we have $\mathrm{Cl}_g(P) = \mathrm{Ord}_{7^{c-1}}(M)$.

□

5.2. Dynamics of g on $E_p(\mathbb{F}_{2^n})$ with $p \neq 2, 7$

Let $p \neq 7$ be an odd prime and $P \in E_p(\overline{\mathbb{F}}_2)$. If $\langle P\rangle \cap \langle g(P)\rangle = \{\mathcal{O}\}$, the the cycle length of P is determined by Theorem 5.1. So we only need to deal with the case when $\langle P\rangle \cap \langle g(P)\rangle \neq \{\mathcal{O}\}$.

Theorem 5.5. *Let $P \in E_p(\mathbb{F}_{2^n})$ with $|P| = p^{e_1} > 1$. Suppose $|\langle P\rangle \cap \langle g(P)\rangle| = p^{e_2}$ where $1 \leq e_2 \leq e_1$. Then there exists an integer λ such that*

$$g(p^{e_1-e_2}P) = \lambda p^{e_1-e_2}P$$

where λ is a root of $X^2 - X + 2 \bmod p^{e_2}$ and λ can be lifted to any power of p. Moreover, suppose that λ_1 is a roof of $X^2 - X + 2 \mod p^{e_1}$ with $\lambda_1 \equiv \lambda \pmod{p^{e_2}}$. Then

$$Cl_g(P) = lcm(Ord_{p^{e_1-e_2}}(M), Ord_{p^{e_1}}(\lambda_1)).$$

Proof. For this theorem, we define $\mathrm{Ord}_{p^0}(M) = 1$. By the proof of Lemma 5.2, $Q = p^{e_1-e_2}P$ has order p^{e_2} and there exists an integer λ such that $g(Q) = \lambda Q$ and λ is also a root of $X^2 - X + 2 \bmod p^{e_2}$. Notice the other root of $m_g(X) \bmod p^{e_2}$ is $1 - \lambda$. Since $X^2 - X + 2$ has two distinct nonzero roots modulo p, i.e. $\lambda \not\equiv \frac{1}{2} \pmod{p}$, and λ and $1 - \lambda$ can be uniquely lifted to roots of $X^2 - X + 2$ modulo any power of p. Let λ_1 be the root of $X^2 - X + 2 \bmod p^{e_1}$ with $\lambda_1 \equiv \lambda \pmod{p}$. Notice the characteristic polynomial of M is $X^2 - X + 2$, thus M is diagonalizable modulo p^{e_1} and can be written as

$$M \equiv U^{-1} \cdot D \cdot U \pmod{p^{e_1}}$$

where $D = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & 1-\lambda_1 \end{smallmatrix}\right)$ and U is invertible modulo p^{e_1}. Let $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then, from the diagonalizaion of M,

$$U \cdot M \equiv D \cdot U \pmod{p^{e_1}},$$

i.e.,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix} \equiv \begin{pmatrix} \lambda_1 & 0 \\ 0 & 1-\lambda_1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{p^{e_1}}.$$

We have

$$\begin{pmatrix} -2b & a+b \\ -2d & c+d \end{pmatrix} \equiv \begin{pmatrix} \lambda_1 a & \lambda_1 b \\ (1-\lambda_1)c & (1-\lambda_1)d \end{pmatrix} \pmod{p^{e_1}}.$$

In particular

$$\begin{aligned} \lambda_1 b &\equiv a + b \pmod{p^{e_1}}, \\ (1-\lambda_1)d &\equiv c + d \pmod{p^{e_1}}. \end{aligned}$$

Hence

$$\begin{aligned} a &\equiv (\lambda_1 - 1)b \pmod{p^{e_1}}, \\ c &\equiv -\lambda_1 d \pmod{p^{e_1}}. \end{aligned}$$

Note that, since U is invertible modulo p^{e_1} and $\lambda_1 \not\equiv 0, \frac{1}{2} \pmod{p^{e_1}}$, we see that a, b, c, and d are not all equal to zero modulo p. Let

$$t = \mathrm{lcm}(\mathrm{Ord}_{p^{e_1-e_2}}(M), \mathrm{Ord}_{p^{e_1}}(\lambda_1)).$$

Then

$$\begin{aligned}(M^t - I)\begin{pmatrix} P \\ g(P)\end{pmatrix} &= U^{-1}(D^t - I)U\begin{pmatrix} P \\ g(P)\end{pmatrix} \\ &= U^{-1}(D^t - I)\begin{pmatrix} aP + bg(P) \\ cP + dg(P)\end{pmatrix}. \qquad (12)\end{aligned}$$

Since t is divisible by $\mathrm{Ord}_{p^{e_1-e_2}}(M) = \mathrm{Ord}_{p^{e_1-e_2}}(D)$, there are integers α and β such that

$$(D^t - I) = \begin{pmatrix} \alpha p^{e_1-e_2} & 0 \\ 0 & \beta p^{e_1-e_2}\end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta\end{pmatrix} p^{e_1-e_2}.$$

Thus, by (12),

$$\begin{aligned}(M^t - I)\begin{pmatrix} P \\ g(P)\end{pmatrix} &= U^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \beta\end{pmatrix}\begin{pmatrix} ap^{e_1-e_2}P + bg(p^{e_1-e_2}P) \\ cp^{e_1-e_2}P + dg(p^{e_1-e_2}P)\end{pmatrix} \\ &= U^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \beta\end{pmatrix}\begin{pmatrix} aQ + bg(Q) \\ cQ + dg(Q)\end{pmatrix} \\ &= U^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \beta\end{pmatrix}\begin{pmatrix} aQ + b\lambda_1 Q \\ cQ + d\lambda_1 Q)\end{pmatrix} \\ &= U^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \beta\end{pmatrix}\begin{pmatrix} b(2\lambda_1 - 1)Q \\ \mathcal{O}\end{pmatrix} \qquad (13)\end{aligned}$$

As $\mathrm{Ord}_{p^{e_1}}(\lambda_1)|t$, $\lambda_1^t \equiv 1 \pmod{p^{e_1}}$, so $\alpha \equiv 0 \pmod{p^{e_2}}$. Hence, in (13),

$$\alpha b(2\lambda_1 - 1)Q = \mathcal{O}, \qquad (14)$$

therefore, $\mathrm{Cl}_g(P)|t$.

Now we want to show $t = \mathrm{Cl}_g(P)$. Let $t_0 = \mathrm{Cl}_g(P)$. Then

$$(M^{t_0} - I)\begin{pmatrix} P \\ g(P)\end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O}\end{pmatrix}.$$

Let

$$(M^{t_0} - I) = \begin{pmatrix} a_1 + a_2 p^{e_1-e_2} & b_1 + b_2 p^{e_1-e_2} \\ c_1 + c_2 p^{e_1-e_2} & d_1 + d_2 p^{e_1-e_2}\end{pmatrix}$$

Then we have

$$\begin{aligned} a_1P + b_1g(P) + a_2Q + b_2g(Q) &= \mathcal{O}, \\ c_1P + d_1g(P) + c_2Q + d_2g(Q) &= \mathcal{O}.\end{aligned}$$

Since $Q, g(Q)$ are in $\langle P\rangle \cap \langle g(P)\rangle$, we have

$$a_1P = -b_1g(P) - a_2Q - b_2g(Q) \in \langle P\rangle \cap \langle g(P)\rangle.$$

Hence $a_1P = u_1Q = u_1p^{e_1-e_2}P$ for some integer u_1. So $a_1 \equiv 0 \pmod{p^{e_1-e_2}}$. Similarly, $b_1, c_1, d_1 \equiv 0 \pmod{p^{e_1-e_2}}$. Hence

$$(M^{t_0} - I) \equiv 0 \pmod{p^{e_1-e_2}}.$$

Thus t_0 is divisible by $\mathrm{Ord}_{p^{e_1-e_2}}(M)$. This implies that

$$D^{t_0} - I = \begin{pmatrix} \alpha_0 & 0 \\ 0 & \beta_0 \end{pmatrix} p^{e_1-e_2}$$

for some integers α_0 and β_0. Then, by (12),

$$(M^{t_0} - I) \begin{pmatrix} P \\ g(P) \end{pmatrix} = U^{-1} \begin{pmatrix} \alpha_0 b(2\lambda_1 - 1)Q \\ \mathcal{O} \end{pmatrix}.$$

Since $t_0 = \mathrm{Cl}_g(P)$,

$$\alpha_0 b(2\lambda_1 - 1)Q = \mathcal{O},$$

i.e.

$$\alpha_0 b(2\lambda_1 - 1) \equiv 0 \pmod{p^{e_2}}.$$

Recall that $\lambda_1 \not\equiv \frac{1}{2} \pmod{p^{e_1}}$ and $b \not\equiv 0 \pmod{p}$. Thus $\alpha_0 \equiv 0 \pmod{p^{e_2}}$. This imiplies that

$$\lambda^{t_0} = 1 + \alpha_0 p^{e_1-e_2} \equiv 1 \pmod{p^{e_1}}.$$

Thus t_0 is divisible by $\mathrm{Ord}_{p^{e_1}}(\lambda_1)$. Since t_0 is the smallest such integer,

$$t_0 = \mathrm{lcm}(\mathrm{Ord}_{p^{e_1-e_2}(M)}, \mathrm{Ord}_{p^{e_1}}(\lambda_1)) = t.$$

This completes the proof. □

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

From Section 3, we know that the tree structure of the dynamics of g on $E(\mathbb{F}_{2^n})$ solely depends on the dynamics of g on $E_2(\mathbb{F}_{2^n})$. Recall that $E(\mathbb{F}_{2^n})$ can be decomposed as

$$E(\mathbb{F}_{2^n}) = E_2(\mathbb{F}_{2^n}) + \bigoplus_{p \neq 2} E_p(\mathbb{F}_{2^n}) \tag{15}$$

where $E_2(\mathbb{F}_{2^n}) \cong \mathbb{Z}/(2^{h_2})$. Since g is p-invariant and $g^{h_2}(P) = \mathcal{O}$ for any $P \in E_2(\mathbb{F}_{2^n})$ by Proposition 3.1, the equation(15) is equivalent to

$$E(\mathbb{F}_{2^n}) = \ker g^{h_2} + \mathrm{Im} g^{h_2}. \tag{16}$$

Then Proposition 3.1 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 need to determine h_2.

Theorem 6.1. *Suppose $n = 2^r \cdot n'$ with n' odd. Then $\#E_2(\mathbb{F}_{2^n}) = 2^{r+2}$.*

To prove this theorem, we need the following lemma.

Lemma 6.2. *Suppose a sequence $\alpha_i \in \overline{\mathbb{F}}_2, i \geq 1$, satisfies the following:*

$$\alpha_1 = 0, \alpha_2 = 1, \text{ and } \alpha_i = \alpha_{i+1} + \alpha_{i+1}^{-1} \text{ for all } i \geq 2. \tag{17}$$

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

Proof. 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 3.10 in [17]. 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 3.10 in [17], $R_n^*(x)$ 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 6.1. 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 satisfies the equation (17) in Lemma 6.2. Since $g(P_i) = P_{i-1}$, from the equqation (2), for all $i \geq 3$,

$$\begin{aligned} \beta_{i-1} &= \alpha_i^2 + 1 + \frac{1}{\alpha_i^2} + \beta_i\left(1 + \frac{1}{\alpha_i^2}\right), \\ \beta_i &= \frac{\alpha_i^2\beta_{i-1} + \alpha_i^4 + \alpha_i^2 + 1}{\alpha_i^2 + 1}. \end{aligned} \tag{18}$$

Hence β_i lies in the same subfield that contains α_i and β_{i-1}. So we just need to know whether α_i is contained in $\mathbb{F}_{2^n}$. 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 $\mathbb{F}_{2^n}$ of the form $\mathbb{F}_{2^{2^{i-2}}}$ is $\mathbb{F}_{2^{2^r}}$. Then Lemma 6.2 says $\alpha_i \in \mathbb{F}_{2^n}$ for $1 \leq i \leq r + 2$. Hence, the largest i such that $P_i \in E(\mathbb{F}_{2^n})$ is $r + 2$, which implies $\#E_2(\mathbb{F}_{2^n}) = 2^{r+2}$. □

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

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

In this section, we study the dynamics of f on $\mathbb{F}_{2^n} \cup \{\infty\}$ using the information from that of g on $E(\mathbb{F}_{2^{2n}})$. For each $x \in \mathbb{F}_{2^n}$, there are two points $(x, y) \in E(\mathbb{F}_{2^{2n}})$ and 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 $|P| = 2^c p_1^{c_1} \cdots p_m^{c_m}$ where p_i's are odd primes for $1 \le i \le m$. Then P can be written as

$$P = P_0 + P_1 + P_2 + \ldots + P_m \tag{19}$$

where $P_0 \in E_2(\mathbb{F}_{2^{2n}})$ and $P_i \in E_{p_i}(\mathbb{F}_{2^{2n}})$ for $1 \le i \le m$.

Cycles - In the equation (19), we compute the orbit length of each P_i for $1 \le i \le m$. The tail length of P is c and P is attached to a cycle whose cycle length is $\mathrm{lcm}(\mathrm{Cl}_g(P_1), \ldots, \mathrm{Cl}_g(P_m))$.

Theorem 7.1. *Suppose $P = (x, y) \in S$ with $Cl_g(P) = m > 1$. 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 if $P = \pm Q$. Thus $\mathrm{Cl}_f(x) < \mathrm{Cl}_g(P)$ if and only if P satisfies $g^{m'}(P) = -P$ for some $1 \le m' < m$. Suppose that m is odd and there exists m' such that $g^{m'}(P) = -P$. Then

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

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

Suppose that $m = 2m'$ for some m'. Then

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

Since $(g^{m'} - I)(P) \neq \mathcal{O}$, $g^{m'}(P) = -P$. Hence, $\mathrm{Cl}_f(x) = m' = m/2$. □

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

Lemma 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. Note that, for $P = (1, 0) + (x, y) \in E$,

$$\pi(P) = \frac{x^3 + xy + 1}{1 + x^2} + \frac{y}{1 + x} + 1 + x = \frac{x^3 + y + 1}{1 + x^2} + 1 + x. \tag{20}$$

Note that since $y \in \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$ and $x\mathbb{F}_{2^n}$, we have $(\pi(P))^{2^n} \neq \pi(P)$. Thus $\pi(P) \in \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$. Now apply g to P. Then

$$g(P) = g((1, 0)) + g((x, y)) = (0, 1) + (x + x^{-1}, y')$$

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

$$\pi(g(P)) = \frac{(y'+1)^2}{(x+x^{-1})^2} + \frac{y'+1}{x+x^{-1}} + x + x^{-1} = \frac{1}{x+x^{-1}}.$$

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

Lemma 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 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

$$\pi((1,0) + (x,y)) = \frac{y^2}{1+x^2} + \frac{y}{1+x} + 1 + x \tag{21}$$

and

$$\pi((1,1) + (x,y)) = \frac{1+y^2}{1+x^2} + \frac{1+y}{1+x} + 1 + x. \tag{22}$$

Thus the equation (21) is equal to the equation (22) 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 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 the equation (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

$$\left(y^{2^n} + y\right)\left(1 + \frac{1}{x^2}\right) = 0. \tag{23}$$

Since $y \in \mathbb{F}_{2^{2n}} \setminus \mathbb{F}_{2^n}$, the equation (23) 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 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 6, $E_2(\mathbb{F}_{2^{2n}}) \cong \mathbb{Z}/(2^{s+3})$ 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 $s + 2$ due to the group decomposition of $E(\mathbb{F}_{2^{2n}})$. 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:

(a) Structure of the tree attached to ∞.

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

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

Theorem 7.6. *Suppose that $n = 2^s \cdot n'$ where $2 \nmid n'$. Then the tree attached to* 0 *is a complete binary tree of height s.*

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 6.1, $E_2(\mathbb{F}_{2^{2n}}) \cong \mathbb{Z}/(2^{s+3})$. 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 6.1, 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 7.7. *Suppose that n is defined as in Theorem 7.6 and $P = (x, y) \in E(\overline{\mathbb{F}}_2)$ where $x \in \mathbb{F}_{2^n}$, but $y \notin \mathbb{F}_{2^n}$. Then the tree attached to x 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 7.2 and Lemma 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 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 6.2 and Theorem 6.1. Since P is $E(\mathbb{F}_{2^n})$, so is $g(P)$. Thus $g(P)+g(Q) \in E(\mathbb{F}_{2^n})$. From 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 7.9. *Suppose that n is defined as in Theorem 7.6 and $P = (x, y) \in E(\mathbb{F}_{2^{2n}})$. Then the tree attached to x 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 16, 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 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 7.7 and Lemma 7.9, we have the following theorem which explains the structures of trees attached to cycles of length bigger than one.

Theorem 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 2 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 with dotted edges are the 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.

8. Conclusion

In this paper, we have analyzed the dynamics of $f(x) = x + x^{-1}$ over $\mathbb{F}_{2^n} \cup \{\infty\}$ by lifting to that of an isogeny $g = I + \sigma$ on Koblitz curve $E : y^2 + xy = x^3 + 1$ over $\mathbb{F}_2$ whose dynamics is much simpler to understand. Although finite coverings provide us a great tool to study dynamics of maps, it is generally difficult to decide the existence of a suitable finite covering for a general map. It is interesting to investigate which maps can be studied with this methodology and what would be the exact conditions for a map to have a finite covering. Since there are numerous applications of discrete dynamics such as reverse-engineering problems [16], modeling of gene regulatory networks [1, 4], and building secure cryptosystems [11], studying discrete dynamics over finite fields is both interesting and challenging.

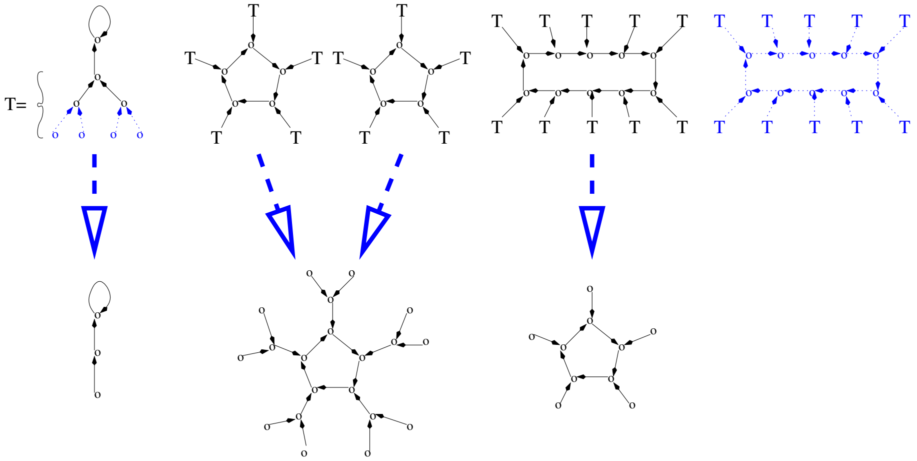

Figure 2: Dynamics of g on $E(\mathbb{F}_{2^{10}})$ and that of $f(x) = x + x^{-1}$ on $\mathbb{F}_{2^5} \cup \{\infty\}$.

[1] R. Albert and H.G. Othmer. 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, 2003.

[2] A. Barta and P. Morton. Algebraic dynamics of polynomial maps on the algebraic closure of a finite field,I. *Rocky Mountain Journal of Mathematics*, 24:(2) 453–481, 1994.

[3] A. Barta and P. Morton. Algebraic dynamics of polynomial maps on the algebraic closure of a finite field,II. *Rocky Mountain Journal of Mathematics*, 24:(3) 905–932, 1994.

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

[5] O. Colón-Reyes, A.S. JarrahR., R. Laubenbacher, and B. Sturmfels. Monomial dynamical systems over finite fields. *Complex Systems*, 16, 2006.

[6] R.L. Devaney. *An Introduction to Chaotic Dynamical System*. Westview Press, second edition, 2003.

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

[8] M. Fried. Galois groups and complex multiplication. *Transactions of the American Mathematical Society*, 235, 1978.

[9] C.L. Gilbert, J.D. Kolesar, C.A. Reiter, and J.D. Stroey. Function digraphs of quadratic maps modulo p. *The Fibonacci Quarterly*, 39, 2001.

[10] R.M. Guralnick, P. Müller, and J. Saxl. The rational function analogue of a question of Schur and exceptionality of permutation representations. 1999.

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

[12] R.A. Hernandez-Toledo. Linear finite dynamical systems. *Communications in Algebra*, 33, 2005.

[13] A.S. Jarrah, R. Laubenbacher, and P. Vera-Licona. An efficient algorithm for finding the phase space structure of linear finite dynamical systems, 2006. preprints.

[14] A.S. Jarrah, R. Laubenbacher, and A. Veliz-Cuba. The dynamics of conjunctive and disjunctive boolean networks. *Bulletin of Mathematical Biology*, 72(6), 2010.

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

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

[17] A.J. Menezes, I.F. Blake, S. Gao, R.C. Mullin, S.A. Vanstone, and T. Yaghoobiann. *Applications of Finite Fields.* Kluwer Academic Publishers, 1992.

[18] J. Milnor. On Lattès maps. *ArXiv:math.DS/0402147.* Stony Brook IMS Preprint #2004/01.

[19] P. Müller. Arithmetically exceptional functions and elliptic curves. *London Mathematical Society Lecture Note Series*, 256, 1998.

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

[21] C. Robinson. *Dynamical Systems - Stability, Symbolic Dynamics, and Chaos.* CRC, 1998.

[22] T.D. Rogers. The graph of the square mapping on the prime fields. *Discrete Mathematics*, 148, 1996.

[23] H.G. Rück. A note on elliptic curve over finite fields. *Mathematics of Computation*, 179, 1987.

[24] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[25] J.H. Silverman. *The Arithmetic of Dynamical Systems.* Springer, 2007.

[26] T. Vasiga and J. Shallit. On the iteration of certain quadratic maps over $GF(p)$. *Discrete Mathematics*, 277, 2004.

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

[28] M.E. Zieve. *Cycles of polynomial mappings.* PhD thesis, University of California at Berkeley, 1996.