POTENTIAL GOOD REDUCTION OF DEGREE 2 RATIONAL MAPS

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF THE UNIVERSITY OF HAWAIʻI AT MĀNOA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

DECEMBER 2012

By

Diane Yap

Dissertation Committee:

Michelle Manes, Chairperson

Kim Binsted
Ralph Freese
Pavel Guerzhoy
James B. Nation
Acknowledgments

These words cannot begin to describe the depths of my gratitude for the patience, generosity, brilliance and grace shown to me by my advisor, Michelle Manes. She is truly the most wonderful advisor any student could hope for. I thank Jamie Sethian and Tobin Fricke for first sparking my interest in mathematics. I would also like to thank David Lukas and the UH Astronomy cluster for their help in making my computational work possible.
Abstract

We give a complete characterization of degree two rational maps with potential good reduction over local fields. We show this happens exactly when the map corresponds to an integral point in the moduli space $M_2$. The proof includes an algorithm by which to conjugate any degree two rational map corresponding to an integral point in $M_2$ into a map with unit resultant. The local fields result is used to solve the same problem for fields over a principal ideal domain. Some additional results are given for degree 2 rational maps over $\mathbb{Q}$. We also give a full description of post-critically finite maps in $M_2(\mathbb{Q})$, including the algorithm used to find them.
# Table of Contents

Acknowledgments .................................................. ii

Abstract ........................................................... iii

List of Tables ....................................................... vi

List of Figures ...................................................... vii

1 Introduction ......................................................... 1

1.1 Rational Maps ..................................................... 1

1.2 Motivation: Elliptic Curves ....................................... 3

1.3 Good Reduction ................................................... 6

2 Background ........................................................ 8

2.1 Multipliers ........................................................ 8

2.2 Normal forms ...................................................... 11

2.3 Heights and PCF maps ........................................... 14

3 Main Result ......................................................... 16

4 Number Field Results ............................................. 22

4.1 Quadratic Polynomials .......................................... 22

4.2 Quadratic Rational Maps ....................................... 25

4.3 Results From Others ............................................ 27

5 Post-Critically Finite Maps ...................................... 30
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Algorithm</td>
<td>32</td>
</tr>
<tr>
<td>5.2 List of Degree 2 Rational Maps with Potential Good Reduction</td>
<td>35</td>
</tr>
<tr>
<td>5.3 Preperiodic Structures for Quadratic PCF Maps with Symmetries</td>
<td>35</td>
</tr>
<tr>
<td>A Sage Code</td>
<td>39</td>
</tr>
<tr>
<td>Bibliography</td>
<td>43</td>
</tr>
</tbody>
</table>
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 PCF maps with nontrivial automorphisms (from [4])</td>
<td>32</td>
</tr>
<tr>
<td>5.2 PCF maps with no nontrivial automorphisms</td>
<td>36</td>
</tr>
<tr>
<td>5.3 Rational preperiodic points portrait</td>
<td>37</td>
</tr>
</tbody>
</table>
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Addition law on elliptic curves ([12])</td>
<td>5</td>
</tr>
<tr>
<td>5.1</td>
<td>All possible rational preperiodic graphs for $\phi_b(z) = \frac{z}{2} + \frac{b}{z}$</td>
<td>38</td>
</tr>
<tr>
<td>5.2</td>
<td>All possible rational preperiodic graphs for $\theta_t(z) = t/z^2$</td>
<td>38</td>
</tr>
<tr>
<td>5.3</td>
<td>More possibilities and their related maps</td>
<td>38</td>
</tr>
<tr>
<td>5.4</td>
<td>$\phi(z) = \frac{2z-1}{z^2-1}$ has rational points on a three-cycle.</td>
<td>38</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Rational Maps

We review a few definitions from [12].

For convenience let $K$ be a field and given a $(d + 1)$-tuple $\mathbf{a} = (a_0, \ldots, a_d)$ let

$$F_a(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d$$

be the associated homogeneous polynomial. Also, for $(d + 1)$-tuples $\mathbf{a}$ and $\mathbf{b}$ we let $[\mathbf{a}, \mathbf{b}] \in \mathbb{P}^{2d+1}$ be the point in projective space with homogenous coordinates $[a_0, \ldots, a_d, b_0, \ldots, b_d]$.

**Definition** The set of rational functions $\phi = [F_a, F_b] : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $d$ is denoted by $\text{Rat}_d$.

It’s useful to note that there is a natural identification of $\text{Rat}_d$ with an open subset of $\mathbb{P}^{2d+1}$ via the map

$$\{ [\mathbf{a}, \mathbf{b}] \in \mathbb{P}^{2d+1} : \text{Res}(F_a, F_b) \neq 0 \} \rightarrow \text{Rat}_d,$$

$$[\mathbf{a}, \mathbf{b}] \mapsto [F_a, F_b].$$

Here $\text{Res}(F_a, F_b)$ refers to the resultant of $\phi$, which is the determinant of the Sylvester matrix of $F_a$ and $F_b$. The significance of a non-zero resultant is that the two polynomials share a common root in $\overline{K}$ if and only if $\text{Res}(F_a, F_b) = 0$ [14].
**Definition** The process of composing a map, \( \phi : K \rightarrow K \), with itself is known as *iteration* and the following notation will be used throughout:

\[
\phi^n = \underbrace{\phi \circ \phi \circ \ldots \circ \phi}_{\text{n times}} = \text{n}^{\text{th}} \text{ iterate of } \phi.
\]

In our discourse, we consider rational maps up to conjugation by an element of \( \text{PGL}_2 \), as this change of coordinates does not affect the geometric properties of the map. To see this conjugation will not change the dynamics of a map \( \phi(z) \in K(z) \), observe that for \( f \in \text{PGL}_2(\bar{K}) \),

\[
(\phi^f)^n = f^{-1} \circ \phi^n \circ f = (\phi^n)^f
\]

The objects we are concerned with are equivalence classes of rational maps which comprise the following quotient space.

**Definition** The *moduli space* of rational maps of degree \( d \) on \( \mathbb{P}^1 \) is the quotient space

\[
M_d = \text{Rat}_d / \text{PGL}_2
\]

where \( \text{PGL}_2 \) acts on \( \text{Rat}_d \) via conjugation, \( \phi^f = f^{-1} \circ \phi \circ f \).

This space exists as an affine integral scheme over \( \mathbb{Z} \) [12, Remark 4.51].

**Definition** Let \( \phi(z) \in \bar{K}(z) \) be a rational map. The *automorphism group of \( \phi \)* is the group

\[
\text{Aut}(\phi) = \{ f \in \text{PGL}_2(\bar{K}) : \phi^f(z) = \phi(z) \}.
\]

Most rational maps do not admit non-trivial automorphisms, but an example of one which does is \( \phi(z) = 2z + 5/z \), which has non-trivial automorphism \( f(z) = -z \).

**Definition** The *symmetry locus* \( S_d \subseteq M_d \) is the set consisting of all conjugacy classes of polynomial maps admitting non-trivial automorphisms.
**Definition** For a point $\alpha \in K$, the *forward orbit of $\alpha$* is the set

$$\mathcal{O}_\phi(\alpha) = \mathcal{O}(\alpha) = \{\phi^n(\alpha) : n \geq 0\}. $$

The point $\alpha$ is *periodic* if $\phi^n(\alpha) = \alpha$ for some $n \geq 1$, and the smallest such $n$ is known as the *exact period of $\alpha$*. The point $\alpha$ is *preperiodic* if some iterate $\phi^m(\alpha)$ is periodic. A point of exact period 1 is called a *fixed point*. The sets of periodic, preperiodic and fixed points of $\phi$ in $\mathbb{P}^1_K$ are denoted as follows:

- $\text{Per}(\phi, \mathbb{P}^1_K) = \{\alpha \in \mathbb{P}^1_K : \phi^n(\alpha) = \alpha \text{ for some } n \geq 1\}$,
- $\text{PrePer}(\phi, \mathbb{P}^1_K) = \{\alpha \in \mathbb{P}^1_K : \phi^{m+n}(\alpha) = \phi^m(\alpha) \text{ for some } n \geq 1\}
  = \{\alpha \in \mathbb{P}^1_K : \mathcal{O}_\phi(\alpha) \text{ is finite}\}$,
- $\text{Fix}(\phi, \mathbb{P}^1_K) = \{\alpha \in \mathbb{P}^1_K : \phi(\alpha) = \alpha\}$.

When $K$ is a fixed field, we write $\text{Per}(\phi)$, $\text{PrePer}(\phi)$ and $\text{Fix}(\phi)$. A fundamental goal of dynamics to classify points $\alpha$ according to their forward orbits, $\mathcal{O}_\phi(\alpha)$.

### 1.2 Motivation: Elliptic Curves

Many questions in arithmetic dynamics arise from exploiting parallels between diophantine geometry and dynamical systems.

<table>
<thead>
<tr>
<th>Diophantine Equations</th>
<th>Dynamical Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>rational and integral points on elliptic curves</td>
<td>rational and integral points in orbits</td>
</tr>
<tr>
<td>torsion points on elliptic curves</td>
<td>periodic and preperiodic points of rational maps</td>
</tr>
</tbody>
</table>

Motivation for this work comes from classical results from elliptic curves. In particular, we focus on finding a criterion in rational maps which gives us potential good reduction, the way that complex multiplication implies potential good reduction in elliptic curves.
We remind the reader of a few concepts from elliptic curves, all of which are found in [11].

**Definition** An **elliptic curve** $E$ over a field $K$ (of characteristic not equal to 2 or 3) is the set of solutions $(x, y)$ of the equation $y^2 = x^3 + ax + b$ with $a, b \in K$ along with a point $O$. We also require that the **discriminant**, $\Delta = 4a^3 + 27b^2 \neq 0$, meaning that the above cubic has distinct roots and $E$ is nonsingular.

**Definition** The **$j$-invariant** $j(E)$ of an elliptic curve is defined as $j(E) = \frac{1728}{4a^3 + 27b^2}$ and it uniquely determines the isomorphism class to which $E$ belongs. In fact, the moduli space of elliptic curves is known as the **$j$-line**.

**Example** Let $E/K : y^2 = x^3 + x$ be an elliptic curve, and $K$ a field of characteristic not equal to 2 or 3. We can calculate its $j$-invariant, $j(E) = 1728$. Substitute by the change of variables $x = x' + 2$ and $y = y' + 3x' + 5$ to get $E'/K : y'^2 + 6x'y' + 10y' = x'^3 - 3x'^2 - 17x' - 15$.

We can put $E'$ back into normal form as $E' : y'^2 = x'^3 - 48x$ and compute the $j$-invariant $j(E') = 1728$, as expected.

**Definition** Elliptic curves can also be thought of as groups with an **addition law** defined as follows: Let $P, Q \in E$, $L$ be the line connecting $P$ and $Q$ ($L$ is the tangent line at $P$ if $P = Q$), $R$ the third point of intersection of $L$ with $E$ and $L'$ the line connecting $R$ with the point $O$ at infinity. Then $P + Q$ is the third point at which $L'$ intersects $E$.

Figure 1.1 (from [12]) illustrates elliptic curve addition of distinct points $P$ and $Q$, and of the point $P$ to itself.

**Definition** Let $K$ be a local field, $E/K$ an elliptic curve and let $\tilde{E}$ be the reduced curve for a minimal Weierstrass equation. Then $E$ has **good reduction** over $K$ if $\tilde{E}$ is non-singular. $E$ has **potential good reduction** over $K$ if there is a finite extension $K'/K$ such that $E$ has good reduction over $K'$.

Over a number field, bad reduction at a prime ideal $p$ is equivalent to $p$ dividing the discriminant.
Definition The *endomorphism ring of E*, denoted \( \text{End}(E) \) is the set of isogenies from \( E \) to itself with the following addition and multiplication rules

\[
(\psi_1 + \psi_2)(P) = \psi_1(P) + \psi_2(P), \quad (\psi_1 \psi_2)(P) = \psi_1(\psi_2(P)).
\]

An elliptic curve \( E \) has *complex multiplication* if \( \text{End}(E) \) is strictly larger than \( \mathbb{Z} \). Note that by the addition law above, based on adding \( P \) to itself, it’s clear that \( \mathbb{Z} \subseteq \text{End}(E) \).

There is are well-known results for elliptic curves which state the following:

**Theorem 1.2.1.** Let \( K \) be a local field with a discrete valuation, and let \( E/K \) be an elliptic curve. Then \( E \) has potential good reduction if and only if its \( j \)-invariant is integral [11].

**Theorem 1.2.2.** Let \( E/\mathbb{C} \) be an elliptic curve with complex multiplication. Then \( j(E) \) is an algebraic integer [9].

*Sketch of proof.* First, one shows that an elliptic curve \( E/K \) with complex multiplication, over a number field \( K \) has potential good reduction at every prime \( p \) of \( K \). Hence, the \( j \)-invariant is \( K \)-rational and \( v \)-integral for every place \( v \). Together with 1.2.1, this shows that the \( j \)-invariant is an algebraic integer.
1.3 Good Reduction

**Definition** Let $\phi(z)$ be a rational map over a local field $K$. There are several equivalent conditions by which good reduction is defined, but we will primarily use that $\phi$ has **good reduction** if $\deg(\phi) = \deg(\tilde{\phi})$, where $\tilde{\phi}$ is the reduction of $\phi$ modulo $p$. A useful equivalent condition is that $\text{Res}(\phi)$ is a unit modulo $p$. Over a number field $K$, $\phi$ has **good reduction** if it has good reduction at $p$ for all prime ideals $p$. We say that $\phi$ has **potential good reduction** if there exists an $f \in \text{PGL}_2(\bar{K})$ such that the conjugation $\phi^f$ has good reduction over a finite extension of $K$.

**Example** Let $\phi(z) = 3z^2 + 2z - 1$. $\tilde{\phi}(z) = 2z - 1 \pmod{3}$, so $\phi(z)$ has bad reduction at $p = 3$. $\deg(\phi) = \deg(\tilde{\phi})$ for all other primes, so $\phi(z)$ has good reduction at primes other than 3.

Those elliptic curves with good reduction are represented by integral points on the $j$-line. It seems hopeful, then, to conjecture that integral points in the moduli space for rational maps would also indicate potential good reduction.

**Definition** To shorten our discourse we define a map $\phi$ as having **genuinely bad reduction** when it does not have potential good reduction. That is, regardless of which $f \in \text{PGL}_2$ we conjugate by, $\phi^f$ has bad reduction.

One of the goals of this paper is to formulate results analogous to 1.2.1 and 1.2.2 for rational maps and prove them for degree 2. We propose:

**Conjecture 1.3.1.** Let $K$ be a local field with discrete valuation. Then a rational map $\phi(z) \in K[z]$ of degree $d$ has potential good reduction if and only if $[\tilde{\phi}]$ is an integral point in the moduli space of degree $d$ rational maps, $M_d$.

**Definition** The *multiplier* of $\phi$ at a finite fixed point $\alpha$ is the derivative $\lambda_\alpha(\phi) = \phi'(\alpha)$. For a more precise definition, see Section 2.1.

We address the case $d = 2$, as it is known that $M_2 \cong \mathbb{A}^2$ with natural coordinates $(\sigma_1, \sigma_2)$. That is, given a rational map $\phi$, its corresponding coordinates in moduli space, $\sigma_1$ and $\sigma_2$ are the first and second symmetric functions on the multipliers of the fixed points of $\phi$, respectively [13]. (See Section 2.1 for definitions and further details.)
For larger $d$, it is not known what the moduli space $M_d$ looks like, so it is currently unclear what an integral point would be in higher dimensions.

**Definition** The rational map $\phi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ has a critical point at $\alpha$ if $\phi'(\alpha) = 0$. This definition applies to finite $\alpha$. For a more complete treatment, see Section 2.1.

**Definition** A map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is postcritically finite, or PCF if the forward orbit of each of its critical points is finite.

Silverman proposes in [10] that post-critically finite maps may be the correct dynamical analogue to elliptic curves with complex multiplication. This is based on the correspondence between elliptic curves and dynamical systems and the idea that the “special” points in the moduli space of elliptic curves (those representing elliptic curves with complex multiplication) would be analogous to “special” points in $M_d$, the PCF maps. We thus propose the following, in analogy to 1.2.1:

**Conjecture 1.3.2.** If $[\phi] \in M_d$ is post-critically finite, then $[\phi]$ corresponds to an integral point in $M_d$. 
Chapter 2

Background

2.1 Multipliers

Recall that the *multiplier* of \( \phi \) at a finite fixed point \( \alpha \) is the derivative \( \lambda_\alpha(\phi) = \phi'(\alpha) \).

**Definition** A fixed point \( \alpha \) is called

- *attracting* if \(|\lambda_\alpha(\phi)| < 1\),
- *neutral* if \(|\lambda_\alpha(\phi)| = 1\),
- *repelling* if \(|\lambda_\alpha(\phi)| > 1\).

Multipliers are conjugation invariant in \( \text{PGL}_2 \) by the following proposition:

**Proposition 2.1.1.** *(Proposition 1.9 in [12])* Let \( \phi \in \mathbb{C}(z) \) be a rational map and let \( \alpha \neq \infty \) be a fixed point of \( \phi \). Let \( f \in \text{PGL}_2(\mathbb{C}) \) be a change of coordinates and set \( \beta = f^{-1}(\alpha) \) with \( \beta \neq \infty \), so \( \beta \) is a fixed point of the conjugate map \( \phi^f = f^{-1} \circ \phi \circ f \). Then

\[
\lambda_\alpha(\phi) = \lambda_\beta(\phi^f).
\]
Proof. By a chain rule calculation, we prove the equivalent statement, \( \phi'(\alpha) = (\phi^f)'(\beta) \).

\[
(\phi^f)'(\beta) = (f^{-1})'(\phi(f(\beta))) \cdot \phi'(\beta) \cdot f'(\beta) \\
= (f^{-1})'(\phi(\alpha)) \cdot \phi'(\alpha) \cdot f'(\beta) \\
= (f^{-1} \circ f)'(\beta) \cdot \phi'(\alpha) \\
= \phi'(\alpha). \qed
\]

**Theorem 2.1.2.** *(Theorem 1.14, in [12]) Let \( K \) be an algebraically closed field and let \( \phi(z) \in K(z) \) be a rational function of degree \( d \geq 2 \). Assume that

\[ \lambda_P \neq 1 \text{ for all } P \in \text{Fix}(\phi). \]

Then

\[
\sum_{P \in \text{Fix}(\phi)} \frac{1}{1 - \lambda_P(\phi)} = 1.
\]

Note: the above theorem only holds when \( \phi \) has \( d + 1 \) distinct fixed points, since the condition \( \lambda_P(\phi) \neq 1 \) is equivalent to the condition that the fixed point \( P \) has multiplicity 1.

When \( d = 2 \), we can derive from Theorem 2.1.2 that the symmetric functions \( \sigma_1, \sigma_3 \) on the multipliers fulfill the following relation:

\[
\sigma_1 = \sigma_3 + 2. \quad (2.1.1)
\]

Though Theorem 2.1.2 does not hold when one or more of the multipliers is 1, (2.1.1) still does. To see this, suppose one of the multipliers equals 1. Then one of the fixed points has multiplicity greater than one, so at least two multipliers are 1. It is easy to see that (1) holds when two or three of the multipliers are 1.

Note that \( (\sigma_1, \sigma_2) \in M_2 \) is integral if and only if all three multipliers, \( \lambda_1, \lambda_2, \lambda_3 \) are algebraic integers. One direction is clear. For the other direction, suppose that \( \sigma_1 \) and \( \sigma_2 \) are integral. Since \( \sigma_1, \sigma_2, \sigma_3 \) are the symmetric functions on \( \lambda_1, \lambda_2, \lambda_3 \), the latter are the roots of the monic polynomial \( f(z) = z^3 - \sigma_1 z^2 + \sigma_2 z - \sigma_3 \). We can conclude that the multipliers are algebraic integers. Since the definition of potential good reduction allows us to go to an extension field, we can then assert that an integral point in \( M_2 \) is equivalent to integral multipliers.
The notion of multiplier can be extended to a cycles of length $n$. Suppose that $\alpha$ is a critical point of the map $\phi(z)$, and that $\alpha$ has exact period $n$. The following simple chain rule calculation shows how multiplier is derived.

$$\lambda_\alpha(\phi) = (\phi^n)'(\alpha) = \phi'(\alpha) \cdot \phi'(\phi \alpha) \cdot \phi'(\phi^2 \alpha) \cdots \phi'(\phi^{n-1} \alpha).$$

The categorizations of fixed points based on their multipliers (attracting, repelling, neutral) also apply in a similar manner to periodic points.

**Lemma 2.1.3.** When $\alpha = \infty$, we may take

$$\lambda_\infty(\phi) = \lim_{z \to 0} \frac{z^{-2} \phi'(z^{-1})}{\phi(z^{-1})^2}.$$ 

*Proof.* When $\alpha = \infty$, we conjugate by $f(z) = 1/z$. To be in keeping with the above proposition, it must hold that $\lambda_\infty(\phi) = (\phi^f)'(f^{-1}(\infty))$. By a chain rule calculation, we get the desired equation,

$$\lambda_\infty(\phi) = \lim_{z \to 0} \frac{z^{-2} \phi'(z^{-1})}{\phi(z^{-1})^2}. \quad \Box$$

With Lemma 2.1.3, we can make sense of having $\infty$ as a critical point. For example, we can use it to determine that the multiplier at $\infty$ of the map $\phi(z) = z^2 + 1$ is indeed 0.

$$\lambda_\infty(\phi) = \lim_{z \to 0} \frac{z^{-2} 2(z^{-1})}{(z^{-2} + 1)^2} = \lim_{z \to 0} \frac{2z^{-3}}{z^{-4} + 2z^{-2} + 1} = \lim_{z \to 0} \frac{2z}{1 + 2z^2 + z^4} = 0.$$ 

We will make frequent use of the following lemma:

**Lemma 2.1.4.** (Corollary 5.3 in [8]) Let $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$ with good reduction at the prime $p$. Let $P \in \mathbb{P}^1(\bar{K})$ be a periodic point for $\phi$. Then $P$ is $p$-adically non-repelling.

*Remark.* In our discourse, we will be working over a local field and using the contrapositive to Lemma 2.1.4 – that if $\phi$ has a $p$-adically repelling periodic point then it has genuinely bad reduction.
2.2 Normal forms

Throughout this work, proofs rely on normal forms which describe degree 2 rational maps up to conjugation over $\text{PGL}_2$. This assures that the results are applicable to the entire space, as the normal forms give a complete representation of the desired maps. The use of normal forms also spares us the more complicated task of attempting to use a fully general map such as

$$\phi(z) = \frac{az^2 + bz + c}{dz^2 + ez + f}.$$ 

The first normal form, given in Lemma 2.2.1 will be used to prove the main result, which gives a complete characterization of degree 2 rational maps with potential good reduction. However, note that a map $\phi$ does not have a unique normal form via Lemma 2.2.1: most maps have 3 distinct multipliers, so each map can have up to 6 representations in this normal form. Thus, since we only wish to evaluate each map once, we use a different normal form (Theorem 2.2.3) in the algorithm for finding PCF maps.

Lemma 2.2.1. (4.59, Normal Forms Lemma in [12]) Let $\phi \in \text{Rat}_2(\mathbb{C})$ be a rational map of degree 2 and let $\lambda_1, \lambda_2, \lambda_3$ be the multipliers of its fixed points.

(a) If $\lambda_1 \lambda_2 \neq 1$, then there is an $f \in \text{PGL}_2(\mathbb{C})$ such that

$$\phi^f(z) = \frac{z^2 + \lambda_1 z}{\lambda_2 z + 1}.$$ 

Further, $\text{Res}(z^2 + \lambda_1 z, \lambda_2 z + 1) = 1 - \lambda_1 \lambda_2$.

(b) If $\lambda_1 \lambda_2 = 1$, then $\lambda_1 = \lambda_2 = 1$ and there is an $f \in \text{PGL}_2(\mathbb{C})$ such that

$$\phi^f(z) = z + \sqrt{1 - \lambda_3 + \frac{1}{z}}.$$

Proof. (a) Let $\phi(z)$ be a rational map of the following form:

$$\phi(z) = \frac{a_0 z^2 + a_1 z + a_2}{b_0 z^2 + b_1 z + b_2}.$$ 

The assumption that $\lambda_1 \lambda_2 \neq 1$ gives us that $\lambda_1 \neq 1$ and $\lambda_2 \neq 1$, meaning that the fixed points corresponding to $\lambda_1$ and $\lambda_2$ are distinct. We can find an element of $\text{PGL}_2(\mathbb{C})$ that moves the fixed points to 0 and $\infty$, respectively. After the change of variables we have

$$\phi(z) = \frac{a_0 z^2 + a_1 z}{b_1 z + b_2} \quad \text{with} \quad a_0 b_2 \neq 0.$$
Since $a_0 \neq 0$, we can dehomogenize to get

$$\phi(z) = \frac{z^2 + b_2 \lambda_1 z}{\lambda_2 z + b_2} \quad \text{with} \quad b_2 \neq 0.$$  

Finally, we can replace $\phi(z)$ with $b_2^{-1} \phi(b_2 z)$ to get the desired form.

(b) In this case, we begin by moving the fixed point associated with $\lambda_1$ to $\infty$ to get

$$\phi(z) = \frac{a_0 z^2 + a_1 z + a_2}{b_1 z + b_2} \quad \text{with} \quad a_0 \neq 0 \quad \text{and} \quad \lambda_1 = \lambda_\infty(\phi) = \frac{b_1}{a_0}.$$  

In fact, since $\lambda_1 \lambda_2 = 1$, $\lambda_1 = \lambda_2 = 1$, so $a_0 = b_2$. Dehomogenizing $a_0 = 1$ then replacing $\phi(z)$ with $\phi(z - b_2) + b_2$ gives us

$$\phi(z) = \frac{z^2 + a_1 z + a_2}{z} \quad \text{with} \quad a_2 \neq 0.$$  

Finally, we can replace $\phi(z)$ with $\phi(\sqrt{a_2} z)/\sqrt{a_2}$ to get the desired form

$$\phi(z) = \frac{z^2 + a_1 z + 1}{z} = z + a_1 + \frac{1}{z}.$$  

To compute the value of $a_1$, note that $\phi(z)$ has a double fixed point at $\infty$ and its other fixed point is at $-a_1^{-1}$. We can calculate the third multiplier $\lambda_3 = \phi'(a_1^{-1}) = 1 - a_1^2$, so $a_1 = \sqrt{1 - \lambda_3}$, as desired.

\[\therefore\]

**Lemma 2.2.2.** *(Statement 4.12 in [12])* For $K$ of characteristic not equal to 2, every quadratic polynomial $f(z) = Az^2 + Bz + C \in K[z]$ is linearly conjugate over $K$ to a unique polynomial of the form $\phi(z) = z^2 + c$.

**Proof.** Let $g(z) = (2z - B)/2A$, then conjugate:

$$\phi(z) = f^9(z) = g^{-1} \circ f \circ g(z) = z^2 + \left(AC - \frac{1}{4}B^2 + \frac{1}{2}B\right) = z^2 + c. \quad \square \quad (2.2.1)$$

It is known in the case of polynomial maps and maps of even degree, that a $K$-rational point in $M_2$ corresponds to a conjugacy class of quadratic rational maps $[\psi]$ and there must be some map $\phi \in [\psi]$ with coefficients in $K$ ([12]). Each family $[\psi]$ describes a conjugacy class of maps, but only within
an algebraically closed field \( \overline{K} \). It is possible to have a map \( \phi \) defined over \( K \) but have the conjugate map given by the normal form of Lemma 2.2.1 defined over a quadratic or cubic extension of \( K \).

Later, we will be using the symmetric functions \( \sigma_1 \) and \( \sigma_2 \) of the multipliers to iterate through equivalence classes of quadratic rational maps. However, having the symmetric functions defined over \( K \) does not guarantee that the multipliers are also defined there. In particular, they may be defined over a cubic extension of \( K \). In fact, we can use Equation 2.1.1 to find that the field extension required will be given by \( f(z) = z^3 - \sigma_1 z^2 + \sigma_2 z - (\sigma_1 - 2) \), which consists of either 3 linear factors, a linear and an irreducible quadratic, or an irreducible cubic. We require a different normal form to deal with the possibility of multipliers not in the original field. The following normal form of Manes and Yasufuku facilitates our goal to list all rational degree 2 PCF maps.

**Theorem 2.2.3.** (Theorem 1 in [6]) Let \( K \) be a field with characteristic different from 2 and 3. Let \( \psi(z) \in K(z) \) have degree 2, and let \( \lambda_1, \lambda_2, \lambda_3 \in \overline{K} \) be the multipliers of the fixed points of \( \psi \) (counted with multiplicity).

(a) If the multipliers are distinct or if exactly two multipliers are 1, then \( \psi(z) \) is conjugate over \( K \) to the map

\[
\phi(z) = \frac{2z^2 + (2 - \sigma_1)z + (2 - \sigma_1)}{-z^2 + (2 + \sigma_1)z + 2 - \sigma_1 - \sigma_2} \in K(z),
\]

where \( \sigma_1 \) and \( \sigma_2 \) are the first two symmetric functions of the multipliers. Furthermore, no two distinct maps of this form are conjugate to each other over \( K \).

(b) If \( \lambda_1 = \lambda_2 \neq 1 \) and \( \lambda_3 \neq \lambda_1 \) or if \( \lambda_1 = \lambda_2 = \lambda_3 = 1 \), then \( \psi \) is conjugate over \( K \) to a map of the form

\[
\phi_{k,b}(z) = kz + \frac{b}{z}
\]

with \( k \in K \setminus \{0, -1/2\} \) (in fact, \( k = \frac{\lambda_1 + 1}{2} \)), and \( b \in K^* \). Furthermore, two such maps \( \phi_{k,b} \) and \( \phi_{k',b'} \) are conjugate over \( \overline{K} \) if and only if \( k = k' \); they are conjugate over \( K \) if in addition \( b/b' \in (K^*)^2 \).

(c) If \( \lambda_1 = \lambda_2 = \lambda_3 = -2 \), then \( \psi \) is conjugate over \( K \) to a map of the form

\[
\theta_{d,k}(z) = \frac{kz^2 - 2dz + dk}{z^2 - 2kz + d}, \quad \text{with} \quad k \in K, d \in K^*, \quad \text{and} \quad k^2 \neq d.
\]

All such maps are conjugate over \( \overline{K} \). Furthermore, \( \theta_{d,k}(z) \) and \( \theta_{d',k'}(z) \) are conjugate over \( K \) if and only if

\[
d' = b^2 d, \quad \text{and} \quad k' \in \left\{ \frac{bd}{k}, b \left( d^2 \gamma^3 + 3dk\gamma^2 + 3d\gamma + k \right) \right\}
\]

\[
\frac{1}{k} \cdot \left( d^2 \gamma^3 + 3dk\gamma^2 + 3d\gamma + 1 \right)
\]
for some $\gamma \in K$ and $b \in K^*$.

Each quadratic rational map $\phi(z) \in K(z)$ must fall into exactly one of the cases above, so this gives a complete description of the $K$-conjugacy classes of such maps.

### 2.3 Heights and PCF maps

Height is a notion of size and arithmetic complexity. We introduce height in order to have a measure of arithmetic size of points in projective space similar to how the size of a rational number is measured by taking the larger of its numerator and denominator. For a number field $K/\mathbb{Q}$ and a point $P \in \mathbb{P}^n(K)$, the height that we define takes into account the size of each of the coordinates with respect to each absolute value over $K$.

To begin, we introduce some notation from [12]. For a point $P = [x_0, \ldots, x_N]$ with coordinates in $K$,

$$|P|_v = \max\{|x_0|_v, \ldots, |x_N|_v\}.$$  

The multiplicative height of $P$ is then denoted

$$H(P) = \left(\prod_{v \in M_K} |P|^v_{n_v}\right)^{1/[K:\mathbb{Q}]}.$$  

Here, $n_v = [K_v : \mathbb{Q}_v]$ is the local degree of $v$.

It is easy to prove that if $K/\mathbb{Q}$ is a number this height has the property that for any constant $B$, the following set is finite

$$\{P \in \mathbb{P}^n(K) : H(P) \leq B\}.$$  

In particular, a height function should have the property that only finitely many points have bounded size.

For further detail and proof, see Theorem 3.7 in [12]. The result which makes it feasible to enumerate all PCF maps is derived from Corollary 4.12 in a paper of Ingram, Jones and Levy [3]:

**Lemma 2.3.1.** Let $\phi(z) \in \overline{\mathbb{Q}}(z)$ have degree 2, suppose that $\phi$ is PCF, and let $\lambda$ be the multiplier of any fixed point of $\phi$. Then $H(\lambda) \leq 4$. 

---

14
This height bound for rational PCF maps, coupled with the normal form of Theorem 2.2.3 allows us to determine a range for the possible coordinates \((\sigma_1, \sigma_2)\) of a PCF function in \(M_2\). That is, we are able to derive bounds for \(\sigma_1\) and \(\sigma_2\), then test a quadratic rational map from each equivalence class to obtain the full list of rational PCF maps of degree 2. This new height bound is derived later in Proposition 5.0.3.
Chapter 3

Main Result

We will be working with maps of the form $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, and the following notation (from [12]) will be used:

- $K$: a field with normalized discrete valuation $v : K^* \to \mathbb{Z}$.
- $| \cdot |_v = c^{-v(x)}$ for some $c > 1$, an absolute value associated to $v$.
- $\mathcal{O}_K = \{ \alpha \in K : v(\alpha) \geq 0 \}$, the ring of integers of $K$.
- $p = \{ \alpha \in K : v(\alpha) \geq 1 \}$, the maximal ideal of $R$.
- $\mathcal{O}_K^* = \{ \alpha \in K : v(\alpha) = 0 \}$, the group of units of $R$.
- $k = R/p$, the residue field of $R$.
- $\sim$ reduction modulo $p$, i.e., $R \to k$, $a \mapsto \bar{a}$.
- $\pi$ uniformizer of $p$.

In this section, we prove the main result, Theorem 3.0.3, which characterizes degree two rational maps with potential good reduction over local fields $K$. The proof relies on the Lemma 2.2.1 and a part of the proof requires the assumption that all three multipliers $\lambda_1, \lambda_2, \lambda_3$ of a rational map are in $\mathcal{O}_K$, the ring of integers of $K$, so we begin with a lemma detailing when this does not happen. The main theorem itself is proved via two propositions, one for each normal form in Lemma 2.2.1.

**Lemma 3.0.2.** Let $\lambda_1 = a_1 \pi^{e_1}$ and $\lambda_2 = a_2 \pi^{e_2}$. If $\lambda_1 \lambda_2 \neq 1$ and $\lambda_1 \lambda_2 \equiv 1 \pmod{\pi}$, then $\lambda_3 \notin \mathcal{O}_K$ if and only if the following conditions all hold:

\begin{align*}
  e_1 &= e_2 = e \\
  a_1 + a_2 &= a \pi^e, \quad a \in \mathcal{O}_K^* \\
  a + a_1 a_2 &\equiv 0 \pmod{\pi}.
\end{align*}
Proof. Suppose $\lambda_1 \lambda_2 \neq 1$ and $\lambda_1 \lambda_2 \equiv 1 \pmod{\pi}$. By (2.1.2), we can represent $\lambda_3$ in terms of the other two multipliers:

$$\lambda_3 = \frac{2 - \lambda_1 - \lambda_2}{1 - \lambda_1 \lambda_2} = \frac{a_1 \pi^{e_1} + a_2 \pi^{e_2}}{a_1 \pi^{e_1} + a_2 \pi^{e_2} + a_1 a_2 \pi^{e_1 + e_2}}.$$

Without loss of generality, suppose that $e_1 \leq e_2$, and simplify to obtain

$$\lambda_3 = \frac{a_1 + a_2 \pi^{e_2 - e_1}}{a_1 + a_2 \pi^{e_2 - e_1} + a_1 a_2 \pi^{e_2}}.$$

The condition $\lambda_3 \notin O_K$ occurs precisely when a higher power of $\pi$ divides the denominator than the numerator, which happens only when $a_1 + a_2 \pi^{e_2 - e_1}$ and $a_1 a_2 \pi^{e_2}$ have the same $\pi$-adic valuation.

Since $\pi \nmid a_1$ and $\pi \nmid a_2$, we can simplify the statement to

$$|a_1 + a_2 \pi^{e_2 - e_1}|_\pi = |\pi^{e_2}|_\pi.$$

However, since $\pi \nmid a_1$, we can conclude that $e_1 = e_2$ and represent $a_1 + a_2 = a \pi^e$ with $a \neq 0$ and $\pi \nmid a$. It follows that $e_2 = e$. Rewriting with our new information, we get

$$\lambda_3 = \frac{a \pi^e}{\pi^e(a + a_2)}.$$

For the denominator to be divisible by a higher $\pi$ power than the numerator gives us the final condition, that $a + a_1 a_2 \equiv 0 \pmod{\pi}$. \qed

**Theorem 3.0.3.** A degree 2 rational map $\phi(z)$ over a local field $K$ has potential good reduction if and only if $[\phi] \in M_2(O_K)$.

Suppose $[\phi] \notin M_2(O_K)$. We remind the reader that an integral point in the moduli space is equivalent to integral multipliers if we allow for a field extension. If $[\phi]$ does not correspond to an integral point in the moduli space, it must have a non-integral multiplier, $\lambda$. Equivalently, $|\lambda|_v > 1$ so $\phi(z)$ has a repelling fixed point. By Lemma 2.1.4, $\phi(z)$ has genuinely bad reduction.

The other direction will be proved using two propositions — one for each of the two forms in (2.2.1). Suppose that the multipliers $\lambda_1, \lambda_2, \lambda_3$ of $\phi(z)$ are all algebraic integers.

**Proposition 3.0.4.** Let

$$\phi(z) = z + \sqrt{1 - \lambda_3} + \frac{1}{z}$$

with $\lambda_1 \lambda_2 = 1$. Then $\phi(z)$ has good reduction.
Proof. Given $\lambda_3 \in \mathcal{O}_K$, it follows trivially that $1 - \lambda_3 \in \mathcal{O}_K$, so $\sqrt{1 - \lambda_3}$ is also integral as it’s the root of the monic polynomial $z^2 + \lambda_3 - 1$. Since the coefficients of $\phi(z)$ are all integral, we can calculate the resultant $\text{Res}(\phi(z)) = \text{Res}(z^2 + \sqrt{1 - \lambda_3}z + 1, z) = 1$. We can therefore conclude that in this case $\phi(z)$ has good reduction. \qed

**Proposition 3.0.5.** Let

$$\phi(z) = \frac{z^2 + \lambda_1 z}{\lambda_2 z + 1}.$$ 

If $\lambda_1 \lambda_2 \neq 1$ and $\lambda_3 \in \mathcal{O}_K$, then $\phi(z)$ has potential good reduction.

**Proof.** Recall that by Lemma 2.2.1,

$$\text{Res}(z^2 + \lambda_1 z, \lambda_2 z + 1, z) = 1 - \lambda_1 \lambda_2.$$ 

If $\lambda_1 \lambda_2 \neq 1 \pmod{\pi}$, then $\text{Res}(\phi(z)) \neq 0 \pmod{\pi}$, so $\phi(z)$ has good reduction.

Now suppose $\lambda_1 \lambda_2 \equiv 1 \pmod{\pi}$.

Here, we can show by equation (2.1.1) that $\lambda_1 \equiv 1 \pmod{\pi}$ and $\lambda_2 \equiv 1 \pmod{\pi}$:

$$\sigma_1 = \sigma_3 + 2$$
$$\lambda_1 + \lambda_2 + \lambda_3 = \lambda_1 \lambda_2 \lambda_3 + 2$$
$$\lambda_1 + \lambda_2 \equiv 2 \pmod{\pi}.$$ 

Now, we may substitute and use our assumption here that $\lambda_1 \lambda_2 \equiv 1 \pmod{\pi}$ to get the following:

$$\lambda_1(2 - \lambda_1) \equiv 1 \pmod{\pi}$$
$$\lambda_1^2 - 1 \equiv 0 \pmod{\pi}$$
$$\lambda_1 \equiv 1 \pmod{\pi}.$$ 

It follows that $\lambda_2 \equiv 1 \pmod{\pi}$ must hold too. We can represent $\lambda_1$ and $\lambda_2$ as follows, with $a_1, a_2, e_1, e_2 \in \mathcal{O}_K$, $e_1, e_2 > 0$, $\pi \nmid a_1$, and $\pi \nmid a_2$:

$$\lambda_1 = 1 + a_1 \pi^{e_1}$$
$$\lambda_2 = 1 + a_2 \pi^{e_2}.$$
For $\lambda_3 \in \mathcal{O}_K$ to hold, at least one of the conditions in Lemma 3.0.2 must fail.

**Case 1**

Suppose $e_1 \neq e_2$. Then, without loss of generality, we may assume $e_1 < e_2$.

$$\text{Res}(\phi) = 1 - \lambda_1 \lambda_2$$

$$= -(a_1 \pi^{e_1} + a_2 \pi^{e_2} + a_1 a_2 \pi^{e_1+e_2})$$

$$= -\pi^{e_1} (a_1 + a_2 \pi^{e_2-e_1} + a_1 a_2 \pi^{e_2}).$$

By assumption $\pi \nmid a_1$, so the order of $\pi$ in $\text{Res}(\phi)$ is $e_1$. To see that $\phi(z)$ has potential good reduction, first conjugate by $f(z) = z - 1$ to obtain

$$\phi^f(z) = \frac{z^2 + (\lambda_1 + \lambda_2 - 2)z + 2 - \lambda_1 - \lambda_2}{\lambda_2 z - \lambda_2 + 1}.$$ 

Now conjugate again by $g(z) = cz$ (with $c = \sqrt{\pi^{e_1}}$) to get

$$(\phi^f)^g(z) = \frac{c^2 z^2 + (\lambda_1 + \lambda_2 - 2)cz + 2 - \lambda_1 - \lambda_2}{c^2 \lambda_2 z + c(1 - \lambda_2)}. \quad (3.0.1)$$

Since $\lambda_1 + \lambda_2 - 2 = a_1 \pi^{e_1} + a_2 \pi^{e_2} = \pi^{e_1}(a_1 + a_2 \pi^{e_2-e_1})$, with $\pi \nmid a_1$, we can write $c^2 m = \lambda_1 + \lambda_2 - 2$ with $\pi \nmid m$. Similarly, we can let $c^2 n = 1 - \lambda_2$. With those substitutions, (3) may be rewritten as

$$(\phi^f)^g(z) = \frac{z^2 + cmz - m}{\lambda_2 z + cn}.$$ 

with all coefficients in $\mathcal{O}_L$, where $L = K(c)$, a finite extension of $L$. We can calculate the resultant

$$\text{Res}((\phi^f)^g(z)) = -\lambda_2^2 m - \lambda_2 c^2 mn + c^2 n^2$$

$$= c^2 n^2 + c^2 mn - m.$$ 

Since the resultant is in $\mathcal{O}_K$, it’s enough to verify that $\pi \nmid \text{Res}((\phi^f)^g(z))$. Recall that $\pi \nmid m$, so we know that $\text{Res}((\phi^f)^g(z)) \not\equiv 0 \pmod{\pi}$, so $\phi(z)$ has potential good reduction.
Using the above defined substitutions, \( \lambda_1 = c^2(m + n) + 1 \) and \( \lambda_2 = 1 - c^2n \). In particular,

\[
\text{Res}(\phi) = 1 - \lambda_1 \lambda_2 = c^2(c^2n^2 + c^2mn - m).
\]

Note that

\[
\text{Res}(\phi) = c^2 \text{Res}((\phi f)g(z)). \tag{3.0.2}
\]

**Case 2**

Suppose that \( e_1 = e_2 = e \), but \( a_1 + a_2 \neq a\pi^e \) for any \( a \in \mathcal{O}_K \). We may write \( a_1 + a_2 = a\pi^d \) with \( d < e \) and \( \pi \nmid a \).

\[
\text{Res}(\phi) = 1 - \lambda_1 \lambda_2 = -\pi^e(a_1 + a_2 + a_1a_2\pi^e)
\]

\[
= -\pi^{e+d}(a + a_1a_2\pi^{e-d}).
\]

Now let \( f(z) = z - 1 \) and \( g(z) = cz \) with \( c = \sqrt{\pi^{e+d}} \). Conjugating by \( f \) then \( g \) gives us equation (3). Now write \( \lambda_1 + \lambda_2 - 2 = \pi^e(a_1 + a_2) = a\pi^{e+d} = ac^2 \) and \( 1 - \lambda_2 = a\pi^e = cn \), then substitute to get

\[
(\phi f)^g(z) = \frac{z^2 + acz - a}{\lambda_2 z + n}.
\]

The resultant is

\[
\text{Res}((\phi f)^g) = -\lambda_2^2 - a\lambda_2cn + n^2
\]

\[
= -a + acn + n^2.
\]

Since \( \pi \) divides both the 2nd and 3rd terms, but not \( a \), \( \text{Res}((\phi f)^g) \not\equiv 0 \pmod{\pi} \). Thus \( \phi(z) \) has potential good reduction.

Using the above defined substitutions, \( \lambda_1 = ac^2 + 1 + cn \) and \( \lambda_2 = 1 - cn \). In particular,

\[
\text{Res}(\phi) = 1 - \lambda_1 \lambda_2 = k^2(-a + acn + n^2).
\]
Note that again, \( \text{Res}(\phi) = c^2 \text{Res}((\phi^f)^g(z)) \).

**Case 3**

Suppose \( e_1 = e_2 = e \) and \( a_1 + a_2 = a\pi^e \) but \( a + a_1a_2 \not\equiv 0 \pmod{\pi} \).

\[
\text{Res}(\phi) = 1 - \lambda_1\lambda_2 \\
= -(a_1\pi^{e_1} + a_2\pi^{e_2} + a_1a_2\pi^{e_1+e_2}) \\
= -\pi^e(a_1 + a_2 + a_1a_2\pi^{2e}) \\
= -\pi^{2e}(a + a_1a_2).
\]

By our assumption that \( a + a_1a_2 \not\equiv 0 \pmod{\pi} \), we have that \( \pi \) has order \( 2c \) in \( \text{Res}(\phi) \). As before, conjugate \( \phi(z) \) first by \( f(z) = z - 1 \) then by \( g(z) = cz \), this time with \( c = \pi^e \) to get an equation identical to (3). Now note that \( \lambda_1 + \lambda_2 - 2 = (a_1 + a_2)\pi^e = a\pi^{2e} = ac^2 \), and let \( 1 - \lambda_2 = -a_2\pi^e = -a_2c \). With these substitutions, we have

\[
(\phi^f)^g(z) = \frac{z^2 + acz - a}{\lambda_2z - a_2}, \quad (3.0.3)
\]

Here the resultant is \( \text{Res}((\phi^f)^g) = a_2^2 + aa_2\lambda_2c - a\lambda_2^2 \).

\[
\text{Res}((\phi^f)^g) \equiv 0 \pmod{\pi} \iff a_2^2 - a\lambda_2^2 + aa_2\lambda_2c \equiv 0 \pmod{\pi} \\
\iff a_2^2 - a\lambda_2^2 \equiv 0 \pmod{\pi} \\
\iff a_2(a\pi^e - a) - a(1 + 2a_2\pi^e + a^2\pi^{2e}) \equiv 0 \pmod{\pi} \\
\iff a_1a_2 + a \equiv 0 \pmod{\pi}.
\]

Since we assumed \( a_1a_2 + a \not\equiv 0 \pmod{\pi} \), it follows that \( \text{Res}((\phi^f)^g) \not\equiv 0 \pmod{\pi} \), so \( \phi(z) \) has potential good reduction.

Using the above defined substitutions, \( \lambda_1 = ac^2 + 1 - a_2c \) and \( \lambda_2 = 1 - a_2c \). In particular we may rewrite

\[
\text{Res}((\phi^f)^g) = a_2^2 + -a - aa_2c \\
\text{Res}(\phi) = 1 - \lambda_1\lambda_2 = c^2(a_2^2 - a - aa_2c).
\]

Note that once again, \( \text{Res}(\phi) = c^2 \text{Res}((\phi^f)^g(z)) \). This concludes the proof of Theorem 3.0.3. \( \square \)
Chapter 4

Number Field Results

The shift from local fields to global fields requires us to show that a degree 2 rational map which corresponds to an integral point in the moduli space but has bad reduction at more than one prime \( p \) still has potential good reduction. The main result above only proved this for a single prime, so it is now necessary to show that similar techniques can be applied to piece together the local results into a global one.

We begin this section by proving stronger results for quadratic polynomials, since this family is of great interest in research.

4.1 Quadratic Polynomials

**Theorem 4.1.1.** Let \( \phi(z) \in K[z] \) be a quadratic polynomial over a number field. Then \( \phi \) has potential good reduction if and only if \( [\phi] \) is an integral point in the moduli space \( M_2 \).

**Proof.** By Lemma 2.2.2, we may assume \( \phi(z) = z^2 + c \).

The function \( \phi(z) \) has fixed points at \( q_{\pm} = \frac{1 \pm \sqrt{1 - 4c}}{2} \), with corresponding multipliers \( \lambda_{q_{\pm}} = 1 \pm \sqrt{1 - 4c} \).

Suppose that \( \phi(z) \) has potential good reduction. Then by Theorem 3.0.3, all multipliers are \( p \)-adically integral for every prime \( p \). We can calculate:
\[ |\lambda_{q_+}|_p \leq 1 \iff |1 - 4c|_p^{1/2} \leq 1 \]
\[ \iff |1 - 4c|_p \leq 1 \]
\[ \iff |4c|_p \leq 1. \]

So potential good reduction means \(|4c|_p \leq 1\). Or, in other words, that \(4c\) is a \(p\)-adic integer for that \(p\). The symmetric functions on the multipliers of the fixed points of \(\phi(z)\) are \(\sigma_1 = 2\) and \(\sigma_2 = 4c\), so \(\phi(z)\) corresponds to the point \((2, 4c)\), which is integral the moduli space.

Now suppose that \([\phi(z)] = [z^2 + c]\) is integral in the moduli space. In particular, it corresponds to the point \((2, 4c)\) which is integral when \(|4c|_p \leq 1\). The following steps show how to find an \(f(z) \in \text{PGL}_2\) to conjugate by to obtain a rational map with good reduction. First, we find the fixed points of \(\phi(z)\), which are \(z = 1 \pm \sqrt{1 - c^2}\). Then let \(f(z) = z + \frac{1 + \sqrt{1 - c}}{2}\). Conjugating gives \(\phi^f(z) = z^2 + (1 + \sqrt{1 - c})z\), which has good reduction over the quadratic extension field \(K[\sqrt{1 - c}]\). Therefore \(\phi(z)\) has potential good reduction.

We have some additional results when \(K = \mathbb{Q}\):

**Lemma 4.1.2.** Let \(\phi(z) = z^2 + \frac{k}{4}\) with \(k \in \mathbb{Z}\). Then if \(k \equiv 0, 1 \pmod{4}\), there exist \(B, C \in \mathbb{Z}\) such that \(\phi(z)\) is conjugate to \(z^2 + Bz + C\), which has good reduction.

**Proof.** Let \(f(z) = z + \frac{B}{2}\), (where \(B\) is as yet to be determined). Then conjugation gives

\[
f^{-1} \circ \phi \circ f(z) = z^2 + Bz + \left(\frac{B^2}{4} - \frac{B}{2} + \frac{k}{4}\right).
\]

For whatever \(B \in \mathbb{Z}\) we choose, it must hold that \(C = \frac{B^2 - 2B + k}{4} \in \mathbb{Z}\). That is, for some \(x \in \mathbb{Z}\), \(B^2 - 2B + k = 4x\). Solving for \(B\) yields

\[ B = 1 \pm \sqrt{1 - k - 4x} \in \mathbb{Z}. \]

So there is some \(y \in \mathbb{Z}\) for which \(\sqrt{1 - k - 4x} = y\). Squaring both sides and rearranging, we get that \(y^2 \equiv 1 - k \pmod{4}\). The only quadratic residues in \(\mathbb{Z}/4\mathbb{Z}\) are 0 and 1, so it must hold that \(k \equiv 0, 1 \pmod{4}\).

The case \(k \equiv 0 \pmod{4}\) is exactly the case where \(\phi(z) = z^2 + C\) with \(C = \frac{k}{4} \in \mathbb{Z}\), so no \(B\) needs to be chosen, as \(\phi(z)\) already has good reduction. In the other case, \(k \equiv 1 \pmod{4}\), we set \(B = 1\), and \(C = \frac{k - 1}{4}\). \(\square\)
Proposition 4.1.3. Let $\phi(z) = z^2 + \frac{k}{4}$ with $k \in \mathbb{Z}$. Then $\phi(z)$ is linearly conjugate to a morphism $\psi(z) \in \mathbb{Q}(z)$ with good reduction over $\mathbb{Q}$ if only if $k \equiv 0, 1 \pmod{4}$.

Proof. The forward direction is a result of the previous lemma. For the other direction, suppose $\phi(z) = z^2 + \frac{k}{4}$ and $f(z) = \frac{ax + b}{cz + d} \in \text{PGL}_2$. Then the full conjugation, $\psi(z) = \phi^f(z)$ looks like:

$$
\frac{(4a^2d + c^2dk - 4bcz^2)z^2 + (8abcd + 2cd^2k - 8bcd)z + 4b^2d + d^3k - 4bd^2}{(4ac^2 - 4a^2c - c^3k)z^2 + (8acd - 8abc - 2c^2dk)z + 4ad^2 - 4b^2c - cd^2k}.
$$

First, note that $c$ and $d$ cannot both be 0, since $f(z) \in \text{PGL}_2$. Now consider the case $c = 0$. Substituting and reducing in the above equation gives

$$
\psi(z) = \frac{4a^2z^2 + 8abz + 4b^2 + d^2k - 4bd}{4ad}.
$$

For $\psi(z)$ to have good reduction, it must hold that $d|a$, $d|2b$ and $2|d$. So we can change notation and replace $a$ with $ad$ and $2b$ with $bd$. Then we can rewrite $\psi(z)$ as

$$
\psi(z) = \frac{4a^2z^2 + 4abz + b^2 - 2b + k}{4a}.
$$

Now we need $\frac{b^2 - 2b + k}{4a} = x$ for some $x \in \mathbb{Z}$. Solving for $b$, we get

$$
b = 1 \pm \sqrt{1 - k + 4ax}.
$$

So there is some $y \in \mathbb{Z}$ such that $y^2 = 1 - k + 4ax$. In other words, $y^2 \equiv 1 - k \pmod{4}$. Since the only quadratic residues in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1, we have that $k \equiv 0, 1 \pmod{4}$ when $c = 0$.

Next, consider the case $d = 0$. Then we have

$$
\psi(z) = \frac{4bcz^2}{(4a^2 - 4ac + c^2k)z^2 + 8abz + 4b^2}.
$$

For $\psi(z)$ to have good reduction the coefficient $-4bc$ in the numerator must cancel. So we have these divisibility properties: $c|2a$ and $c|b$. As before, replace $2a$ with $ac$ and $b$ with $bc$. Then we can rewrite $\psi(z)$ as

$$
\psi(z) = \frac{4bz^2}{(a^2 - 2a + k)z^2 + 4abz + 4b^2}.
$$

Now, we just need to ensure that $\frac{a^2 - 2a + k}{4b} = x$ for some $x \in \mathbb{Z}$. Solving for $a$, we get
\[ a = 1 \pm \sqrt{1-k+4bx}. \]

There must be some \( y \in \mathbb{Z} \) such that \( y^2 = 1 - k - 4bx \), i.e. \( y^2 \equiv 1 - k \pmod{4} \). Thus we have that \( k \equiv 0, 1 \pmod{4} \).

Now consider the case where both \( c \) and \( d \) are nonzero. Without cancellation, \( g(z) \) reduces to the constant \(-\frac{d}{c}\) in \( \mathbb{Z}/2\mathbb{Z} \), indicating bad reduction. The only possibility for good reduction requires that each monomial be divisible by 2, requiring that \( c \) and \( d \) both be even.

Knowing that \( c \) and \( d \) are both even, we may rewrite \( f(z) \) as \( f(z) = \frac{az+b}{2cz+2d} \). Then \( \psi(z) \) once again reduces to \(-\frac{d}{c}\) in \( \mathbb{Z}/2\mathbb{Z} \) unless there is cancellation. Suppose that \( 2^n | c \) and \( 2^n | d \). Then we can repeat the process, continuing to rewrite \( f(z) \) as above and recalculating \( \psi(z) \), indicating that \( \psi(z) \) reduces to \(-\frac{d}{c}\) for arbitrarily large \( n \). Since there are no \( c \) and \( d \) in \( \mathbb{Z} \) which would permit cancellation, \( \phi(z) = z^2 + \frac{k}{4} \) cannot be conjugate to a function with good reduction over \( \mathbb{Q} \) unless \( k \equiv 0, 1 \pmod{4} \), as in the above cases.

\[ \square \]

### 4.2 Quadratic Rational Maps

Our result over number fields is a corollary to Theorem 3.0.3 and the proof follows an identical format, so we will be brief.

**Corollary 4.2.1.** If degree 2 rational map \( \phi(z) \) over a \( \mathbb{Q} \) has potential good reduction, then \( [\phi] \in M_2(\mathbb{Z}) \). Conversely, if \( [\phi] \in M_2(\mathbb{Z}) \) and \( \phi \) has at least one multiplier in \( \mathbb{Z} \), then \( \phi(z) \) has potential good reduction.

**Proof.** Recall from the proof of the local fields case that the change of variables we employed gave us a resultant which was no longer divisible by the prime \( \pi \) of bad reduction, or more precisely, (3.0.2). Note that Proposition 3.0.4 holds as a global result.

To extend Proposition 3.0.5 to \( \mathbb{Q} \), recall our assumptions that \( [\phi] \in M_2(\mathbb{Z}) \) and \( \phi \) has at least one multiplier, \( \lambda_3 \), which is in \( \mathbb{Z} \). Then by Lemma 2.2.1, we may write our map as

\[
\phi(z) = \frac{z^2 + \lambda_1 z}{\lambda_2 z + 1}
\]

with \( \text{Res}(\phi) = 1 - \lambda_1 \lambda_2 \). The multiplier polynomial in this case will factor over \( \mathbb{Z} \) into \( z - \lambda_3 \) and at worse an irreducible quadratic \( z^2 - (\lambda_1 + \lambda_2)z + \lambda_1 \lambda_2 \). Since \( \lambda_1 \lambda_2 \in \mathbb{Z} \), \( \text{Res}(\phi) \in \mathbb{Z} \) as well.
Then we can write \( \text{Res}(\phi) = \prod_{i=1}^{n} \pi_i^{e_i} \). For each of the \( \pi_i \), there are two cases: either \( \pi_i \) has the property that \( \lambda_1 \lambda_2 \equiv 1 \pmod{\pi_i} \) or it doesn’t. In the case that it does not, the proof of Proposition 3.0.5 shows that \( \phi(z) \) has good reduction for that \( \pi_i \), so we need only be concerned with \( \pi_i \) for which \( \lambda_1 \lambda_2 \equiv 1 \pmod{\pi_i} \).

To that end, let \( \pi_i \) for \( i = 1, 2, \ldots, m \) be the complete list of primes such that \( \lambda_1 \lambda_2 \equiv 1 \pmod{\pi_i} \) and \( \text{Res}(\phi) \equiv 0 \pmod{\pi_i} \). Following the proof of Proposition 3.0.5, simply let \( e_i \) be the order of \( \pi_i \) in \( \text{Res}(\phi) \), and set

\[
k = \sqrt{\prod_{i=1}^{m} \pi_i^{e_i}}.
\]

By (3.0.2),

\[\text{Res}(\phi(z)) = \text{Res}(\phi^f(z)) \prod_{i=1}^{m} \pi_i^{e_i} \cdot \]

In particular, the resultant of the conjugated map is no longer divisible by any prime \( \pi \) with the property \( \lambda_1 \lambda_2 \equiv 1 \pmod{\pi} \). Since the \( \text{Res}(\phi^f(z)) \) is not equivalent to zero \( \pmod{\pi} \) for any \( \pi \), we may conclude that \( \phi(z) \) has potential good reduction over \( \mathbb{Q} \).

**Example** Let \( \phi(z) = z^2 - 2z - 2z + 1 \). \( \text{Res}(\phi) = -3 \), and we verify that \( \lambda_1 \lambda_2 = (-2)(-2) \equiv 1 \pmod{3} \).

Now, conjugate first by \( f(z) = z - 1 \), then by \( g(z) = \sqrt{3}z \) to get

\[
(\phi^f)^g = \frac{z^2 - 2\sqrt{3}z + 2}{-2z + \sqrt{3}}
\]
which has resultant 1.

**Example** Let \( \phi(z) = z^2 - \frac{-3z}{-3z+1} \). \( \text{Res}(\phi) = -8 \), and we verify that \( \lambda_1 \lambda_2 = (-3)(-3) \equiv 1 \pmod{2} \).

Now, conjugate first by \( f(z) = z - 1 \), then by \( g(z) = 2\sqrt{2}z \) to get

\[
(\phi^f)^g = \frac{z^2 - 2\sqrt{2}z + 1}{-3z + \sqrt{2}}
\]
which has resultant 1.

**Example** Let \( \phi(z) = z^2 - \frac{-3z}{-3z+1} \). \( \text{Res}(\phi) = -2 \), and we verify that \( \lambda_1 \lambda_2 = (-3)(-1) \equiv 1 \pmod{2} \).

Now, conjugate first by \( f(z) = z - 1 \), then by \( g(z) = \sqrt{2}z \) to get

\[
(\phi^f)^g = \frac{z^2 - 3\sqrt{2}z + 3}{-z + \sqrt{2}}
\]
which has resultant 1.

**Example** Now for an example with bad reduction at two primes, let \( \phi(z) = \frac{z^2 + 13z}{z+1} \). \( \text{Res}(\phi) = -12 \), and we verify that \( \lambda_1 \lambda_2 = (1)(13) \equiv 1 \pmod{2} \) and also \( \lambda_1 \lambda_2 \equiv 1 \pmod{3} \). Now, conjugate first by \( f(z) = z - 1 \), then by \( g(z) = \sqrt{12}z \) to get

\[
(\phi^f)^g = \frac{z^2 + 2\sqrt{3}z - 1}{z}
\]

which has resultant \(-1\).

### 4.3 Results From Others

Bruin and Molnar [1] describe an algorithm for finding a minimal model for rational maps of arbitrary degree \( d > 1 \). Their ultimate goal is to find maps with many integral points in an orbit. When a rational map defined over \( K \) has a model with good reduction also defined over a local field \( K \), their algorithm can be used to find this model. Unlike their algorithm, the present work allows for moving to a finite extension of \( K \) when necessary. See below for examples of this distinction.

The following lemma is referenced throughout, and is the basis of Bruin and Molnar’s algorithm for finding minimal models:

**Lemma 4.3.1.** *(Lemma 3.1 in [1]) If \( d \) is even and \( v(\text{Res}_d(F, G)) < d \) or if \( d \) is odd and \( v(\text{Res}_d(F, G)) < 2d \) then \([F, G]\) is an \( R \)-minimal model for \([\phi]\).*

Their algorithm begins with a rational function \( \phi \in \text{Rat}_d(K) \), given by a model \([F, G]\) over a discrete valuation ring \( R \). They first prove the existence of a minimal model:

**Proposition 4.3.2.** *(Proposition 2.12 in [1]) Let \( R \) be a discrete valuation ring with field of fractions \( K \) and uniformizer \( \pi \). Let \( \phi \in \text{Rat}_d(K) \) be a rational function given by a model \([F, G] \in M_d(K)\). Then there are \( e_1, e_2, e_3 \in \mathbb{Z} \) and \( \beta \in K \) such that for any \( \beta' \in \beta + \pi^{e_3}R \) we can set

\[
(\lambda, A) = (\pi^{e_1}, \begin{pmatrix} \pi^{e_2} & \beta' \\ 0 & 1 \end{pmatrix}) \in (\mathbb{G}_m \times \text{GL}_2)(K)
\]

and have that \([\lambda F_A, \lambda G_A]\) is an \( R \)-minimal model for \( \phi \).
The algorithm is seeded with initial values for \( e_1 \) and \( e_2 \), derived from the original map, then it tests the map for minimality via Lemma 4.3.1. If the resulting conjugated map is not minimal, \( e_1 \) and \( e_2 \) are replaced by values based on the new map. This process is iterated until an \( R \)-minimal model is found.

We give several examples of finding the minimal resultant of a given degree 2 rational map, first using methods from [1], then also by using the algorithm from this thesis. In each case, the map is presented in the normal form of Lemma 2.2.1, where the coefficients correspond to two of the three multipliers. Since both are integers, all three multipliers must be integral, therefore the symmetric functions \( \sigma_1 \) and \( \sigma_2 \) are integral. In other words, each of these maps corresponds to an integral point in the moduli space, so by Theorem 3.0.3, they have potential good reduction.

**Example** Let \( \phi(z) = z^2 - 2z - 2 \). \( \text{Res}(\phi) = -3 \). Since we are working with the 3-adic valuation, \( v(\text{Res}_d(F, G)) = 1 < 2 = d \). By Lemma 4.3.1, \( \phi(z) \) is already locally minimal, and the algorithm of Bruin and Molnar would not change it.

However, we can find a conjugate map with good reduction, by letting \( f(z) = z - 1 \) and \( g(z) = \sqrt{3}z \) to get

\[
(\phi f)^g = \frac{z^2 - 2\sqrt{3}z + 2}{-2z + \sqrt{3}}
\]

which has resultant 1.

**Example** Let \( \phi(z) = \frac{z^2 + 9z}{z + 1} \). \( \text{Res}(\phi) = -8 \). Note that both the numerator and the denominator of \( \phi(z) \) are monic and that the degree of the denominator is half the degree of the numerator. By [1, Remark 3.4], \( \phi(z) \) is minimal according to the algorithm of Bruin and Molnar.

Our algorithm finds a map with good reduction, via conjugating first by \( f(z) = z - 1 \), then by \( g(z) = 2z\sqrt{2} \) to get

\[
(\phi f)^g = \frac{z^2 + 2\sqrt{2}z - 1}{z}
\]

which has resultant \(-1\).

**Example** Let \( \phi(z) = \frac{z^2 - 3z}{z + 1} \). \( \text{Res}(\phi) = -2 \). We are working with the 2-adic valuation, so \( v(\text{Res}_d(F, G)) = 1 < 2 = d \). By Lemma 4.3.1, \( \phi(z) \) is found by the algorithm of [1] to be locally minimal.
However, to obtain a good reduction, we can conjugate first by $f(z) = z - 1$, then by $g(z) = \sqrt{2}z$ to get
\[
(\phi f)^g = \frac{z^2 - 3\sqrt{2}z + 3}{-z + \sqrt{2}}
\]
which has resultant 1.

Finally, consider the following example which has a resultant divisible by more than one prime $p$:

**Example** Let $\phi(z) = \frac{z^2 + 13z}{z + 1}$. $\text{Res}(\phi) = -12$. Note that both the numerator and the denominator of $\phi(z)$ are monic and that the degree of the denominator is half the degree of the numerator. Again by [1, Remark 3.4], $\phi(z)$ is considered to be minimal.

Now, for a map with good reduction via our algorithm, conjugate first by $f(z) = z - 1$, then by $g(z) = \sqrt{12}z$ to get
\[
(\phi f)^g = \frac{z^2 + 2\sqrt{3}z - 1}{z}
\]
which has resultant $-1$. 

29
Chapter 5

Post-Critically Finite Maps

In this section, we list all post critically finite maps of degree two over $\mathbb{Q}$ after showing why there are only finitely many and that our search space is comprehensive.

Recall from Lemma 2.3.1 that if $\lambda$ is a fixed-point multiplier of a degree 2 PCF map $\phi$, then its height is bounded by $H(\lambda) \leq 4$. This provides us with a finite search space. For our algorithm, we derive and use new height bounds of the first and second symmetric functions of the multipliers, not the height of the multipliers themselves. Though this choice results in a large increase of the height bound, it is necessary because we need the normal form of Theorem 2.2.3. The choice of this normal form arises from the fact that it is possible for a map $\phi$ defined over $K$ to have its multipliers defined over a quadratic or cubic extension of $K$. In other words, the conjugate map in the normal form of Lemma 2.2.1 might not be defined over $K$. Additionally, using the normal form of Lemma 2.2.1 would not give us a unique form for each set of multipliers as there are 6 ways to assign the 3 multipliers. The following is a height bound on the symmetric functions, derived from Lemma 2.3.1.

**Proposition 5.0.3.** Let $\phi(z) \in \overline{\mathbb{Q}}$ be a degree 2 PCF map and suppose that $\sigma_1$ and $\sigma_2$ are the first and second symmetric functions on the multipliers, $\lambda_1, \lambda_2, \lambda_3$, of $\phi(z)$. Then $H(\sigma_1) \leq 192$ and $H(\sigma_2) \leq 12288$.

**Proof.** Working with the definition of height given in Section 2.3 and simplifying notation by setting $d = [K : \mathbb{Q}]$

$$H(\sigma_1) = \prod_{v \in M_K} (\max\{\sigma_1|_v, 1\}^{n_v})^{1/d}.$$
By the non-archimedean triangle inequality, we have

$$|\sigma_1|_v = |\lambda_1 + \lambda_2 + \lambda_3|_v \leq \max \{|\lambda_1|_v, |\lambda_2|_v, |\lambda_3|_v\}$$

for each finite place.

Similarly, the triangle inequality gives us

$$|\sigma_1|_v = |\lambda_1 + \lambda_2 + \lambda_3|_v \leq 3 \max \{|\lambda_1|_v, |\lambda_2|_v, |\lambda_3|_v\}$$

for any infinite place. For an extension of degree $d$, there are $d$ infinite places, so we can move the 3 out of the product:

$$H(\sigma_1) \leq 3 \prod_{v \in M_K} \left( \max_{1 \leq i \leq 3} \{|\lambda_i|_v, 1\}^{n_v} \right)^{1/d}$$

$$\leq 3 \prod_{v \in M_K} (\max\{|\lambda_1|_v, 1\}^{n_v} \cdot \max\{|\lambda_2|_v, 1\}^{n_v} \cdot \max\{|\lambda_3|_v, 1\}^{n_v})^{1/d}$$

$$\leq 3 \prod_{v \in M_K} (\max\{|\lambda_1|_v, 1\}^{n_v})^{1/d} \prod_{v \in M_K} (\max\{|\lambda_2|_v, 1\}^{n_v})^{1/d} \prod_{v \in M_K} (\max\{|\lambda_3|_v, 1\}^{n_v})^{1/d}$$

$$= 3H(\lambda_1)H(\lambda_2)H(\lambda_3) \leq 3 \cdot 4^3 = 198.$$ 

The proof for the bound of $\sigma_2$ follows similarly:

$$H(\sigma_2) = H(\lambda_1 \lambda_2 + \lambda_1 \lambda_3 + \lambda_2 \lambda_3)$$

$$\leq 3 \prod_{v \in M_K} \left( \max_{i \neq j} \{|\lambda_i \lambda_j|_v, 1\}^{n_v} \right)^{1/d}$$

$$\leq 3 \prod_{v \in M_K} (\max\{|\lambda_1 \lambda_2|_v, 1\}^{n_v} \cdot \max\{|\lambda_2 \lambda_3|_v, 1\}^{n_v} \cdot \max\{|\lambda_1 \lambda_3|_v, 1\}^{n_v})^{1/d}$$

$$\leq 3 \prod_{v \in M_K} (\max\{|\lambda_1 \lambda_2|_v, 1\}^{n_v})^{1/d} \prod_{v \in M_K} (\max\{|\lambda_2 \lambda_3|_v, 1\}^{n_v})^{1/d} \prod_{v \in M_K} (\max\{|\lambda_1 \lambda_3|_v, 1\}^{n_v})^{1/d}$$
\[ = 3H(\lambda_1\lambda_2)H(\lambda_2\lambda_3)H(\lambda_1\lambda_3) = 3H(\lambda_1)^2H(\lambda_2)^2H(\lambda_3)^2 \leq 3 \cdot 4^6 = 12288. \]

In fact, our search space is much smaller than that. We know of an upcoming result which limits the search to 2-integers – rationals with powers of 2 in the denominator [5]. The PCF maps currently included are from a search over the integers, but calculations are currently running over the 2-integers. To date, no additional (non-integral) PCF maps have been found, and we do not expect to find any. We will allow the search to complete before submitting the complete list for publication.

In the algorithm, the normal form of Manes and Yasufuku (Theorem 2.2.3), only case (a) is used, as this is the case of maps with no nontrivial automorphism groups. Those maps corresponding to the point \((\sigma_1, \sigma_2)\) where \(\sigma_1\) and \(\sigma_2\) fulfill the following

\[ 36 - 12\sigma_2 + 4\sigma_2^2 = 12\sigma_1 - \sigma_1^2 + 2\sigma_1^3 - 8\sigma_1\sigma_2 + \sigma_1^2\sigma_2 \]

exactly comprise the symmetry locus \(S_2\), and have been described fully in [4]. The PCF maps defined over \(\mathbb{Q}\) with nontrivial automorphisms are shown in Table 5.1, below.

<table>
<thead>
<tr>
<th>(\phi(z))</th>
<th>Critical Points</th>
<th>Orbit Graph</th>
<th>Conjugate map with good reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\frac{z^2+1}{2z})</td>
<td>{-1, 1}</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td>(z^2)</td>
</tr>
<tr>
<td>(\frac{z^2+1}{2z})</td>
<td>{-1, 1}</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td>(1/z^2)</td>
</tr>
</tbody>
</table>

Table 5.1. PCF maps with nontrivial automorphisms (from [4])

### 5.1 Algorithm

The algorithm used was written in Sage [S+09] and uses a subroutine for finding orbits from the ProjSpace package developed at ICERM [2]. It also relies on the following two theorems.

**Theorem 5.1.1.** *(Theorem 2.21 from [12]) Let \(\phi : \mathbb{P}^1 \to \mathbb{P}^1\) be a rational function of degree \(d \geq 2\) defined over a local field with a nonarchimedean absolute value \(\cdot |_{\nu}\). Assume that \(\phi\) has good reduction, let \(P \in \mathbb{P}^1(K)\) be a periodic point of \(\phi\), and define the following quantities:
The exact period of $P$ for the map $\phi$.

$m$ The exact period of $\tilde{P}$ for the map $\tilde{\phi}$.

$r$ The order of $\lambda_{\tilde{\phi}}(\tilde{P}) = (\tilde{\phi}^m)'(\tilde{P})$ in $k^*$. (Set $r = \infty$ if $\lambda_{\tilde{\phi}}(\tilde{P})$ is not a root of unity.)

$p$ The characteristic of the residue field $k$ of $K$.

Then $n$ has one of the following forms:

$$n = m \quad \text{or} \quad n = mr \quad \text{or} \quad n = mr^p$$

**Theorem 5.1.2.** *(Theorem 2.28 from [12])* We continue with the notation and assumptions from Theorem 5.1.1. We further assume that $K$ has characteristic 0 and we let $v : K^* \rightarrow \mathbb{Z}$ be the normalized valuation on $K$. If the period $n$ of $P \in \mathbb{P}^1(K)$ has the form $n = mr^p$, then the exponent $e$ satisfies

$$p^{e-1} \leq \frac{2v(p)}{p - 1}.$$  

Since we are working over $\mathbb{Q}$, $\nu(p) = 1$ for all $p$, so Theorem 5.1.2 allows us to assert $e = 0$, when $p \neq 2$ and $e \in \{0, 1\}$ when $p = 2$. In the algorithm, we exclude $p = 2$ from consideration and use the following possibilities for $n$:

$$n = m \quad \text{or} \quad n = mr.$$

We first sketch the flow of the algorithm. Iterating over all degree 2 rational maps $\phi$ not in the symmetry locus, the algorithm:

1. Finds the resultant $R$ of $\phi$.
2. Lists the first $n$ primes $p$ such that $\gcd(R, p) = 1$, the primes of good reduction.
3. Finds the critical points of $\phi$.
4. Iterates over each critical point, finding sets of potential global period lengths for the orbits containing the critical point.
5. Intersects the potential critical point orbit lengths and discards the map if the intersection is empty.

For further reference, the code itself is in Appendix A.

We make use of the above theorem in step (4) by finding possible global period lengths based on each good prime $p$. Note that this algorithm filters out maps which are certainly not PCF, but does not guarantee that the maps which remain are PCF. The initial run over all integers eliminated all but a handful of maps. Of these, false positives were removed by increasing the number of primes.
$n$ used to seed the algorithm from $n = 25$ to $n = 50$. The remaining maps were verified to be PCF, and their orbit graphs are included in the following tables.

**Algorithm 1** — Filters out maps $\phi$ which are not PCF

**Input:**
- a degree 2 rational map $\phi(z) \in \mathbb{Z}(z)$
- the number of primes to test

**Output:** $\phi(z)$, if it passes the filter

create a list $P$ of good primes by taking the first $n + 10$ primes and deleting the bad primes

for $c$ a critical point of $\phi$:
- if $c \in \mathbb{Q}$:
  - create list $L_p$ of possible periods for each prime $p$ in $P$
  - intersect all lists $L_p$
  - if the intersection is non-empty: continue
  - else: exit
- else (if $c \notin \mathbb{Q}$):
  - for $p \in P$:
    - check that $c \in \mathbb{F}_p$ (where $\mathbb{F}_p$ is the finite field of $p$ elements)
    - create list $L_p$ of possible periods for $p$
    - intersect all lists $L_p$
    - if the intersection is non-empty: continue
    - else: exit

return $\phi(z)$

**Algorithm 2** — Executes Algorithm 1 (*is_PCF*) over 2-integers

**Input:** [none]

**Output:** list of possible PCF maps

for $\sigma_2$ a 2-integer of height $\leq 12288$:
- for $\sigma_1$ a 2-integer of height $\leq 192$:
  - if $\phi(\sigma_1, \sigma_2)$ is not in the symmetry locus:
    - if *is_PCF*($\phi$, 25):
      - print f
5.2 List of Degree 2 Rational Maps with Potential Good Reduction

The Table 5.2 lists all degree 2 PCF maps with no non-trivial automorphisms over \( \mathbb{Q} \) in the normal form from [6]. The three maps in the table without a stated simpler form with good reduction do also, in fact, have potential good reduction. Following the format of the proof of Corollary 4.2.1, we can write

\[
\phi(z) = \frac{z^2 + \lambda_1 z}{\lambda_2 z + 1}.
\]

In all three cases, we can calculate

\[
\text{Res}(\phi) = 1 - \lambda_1 \lambda_2 = (\alpha)^2,
\]

where \( \alpha \) is an integral principle ideal. Since the resultant is the square of a principle ideal, we can follow the algorithm as outlined. Let \( \alpha = \alpha \), and conjugate \( \phi(z) \) first by \( f(z) = z - 1 \) then by \( g(z) = cz \) to arrive at a map with good reduction.

5.3 Preperiodic Structures for Quadratic PCF Maps with Symmetries

Also of interest is the portrait of all rational preperiodic points for each PCF map. For those maps with no nontrivial automorphisms, these structures are given in Table 5.3. As to the other case, the only PCF maps in the symmetry locus are the ones conjugate to \( \psi_1(z) = z^2 \) and \( \psi_2(z) = 1/z^2 \) [4]. We depict all rational preperiodic structures for maps in these two families. Details on their derivation will be available in an upcoming joint paper on quadratic PCF maps and their preperiodic structures.

If \( \phi \) is a rational map, \( \psi \) is a twist of \( \phi \) if \( \phi^f = \psi \) for some \( f \in \text{PGL}_2(\mathbb{Q}) \). The twist is nontrivial if \( f \not\in \text{PGL}_2(\mathbb{Q}) \). Since the rational preperiodic points are not preserved under the conjugation, to form a complete description of the rational preperiodic structures, we must understand the possible structures for all twists. Only maps in the symmetry locus have nontrivial twists [12, Proposition 4.73].

Throughout this section, \( \zeta_n \) means a primitive \( n^{th} \) root of unity. Preperiodic point portraits are given for \( \psi_1(z) = z^2 \) in Figure 5.1. The remaining figures correspond to twists of \( \psi_2(z) = 1/z^2 \).
<table>
<thead>
<tr>
<th>$\phi(z)$</th>
<th>Critical Points</th>
<th>Orbit Graph</th>
<th>Conjugate map with good reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{2z^2}{z^2+4z+8}$</td>
<td>${-4, 0}$</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td>$z^2 - 2$</td>
</tr>
<tr>
<td>$\frac{2z^2}{-z^2+4z+4}$</td>
<td>${-2, 0}$</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td>$z^2 - 1$</td>
</tr>
<tr>
<td>$\frac{2z^2+8z+8}{-z^2-4z-2}$</td>
<td>${-2, \infty}$</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td>$\frac{z^2+(-1-i)z}{(i-1)z+1}$</td>
</tr>
<tr>
<td>$\frac{2z^2+8z+8}{-z^2+4z+4}$</td>
<td>${-2, \infty}$</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td></td>
</tr>
<tr>
<td>$\frac{2z^2+4z+4}{-z^2}$</td>
<td>${-2, 0}$</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td></td>
</tr>
<tr>
<td>$\frac{2z^2+8z+8}{-z^2-4z}$</td>
<td>${-2, \infty}$</td>
<td><img src="image" alt="Orbit Graph" /></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.2. PCF maps with no nontrivial automorphisms
<table>
<thead>
<tr>
<th>$\phi(z)$</th>
<th>Rational Preperiodic Points Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{2z^2}{-z^2+4z+8}$</td>
<td>![Diagram 1]</td>
</tr>
<tr>
<td>$\frac{2z^2}{-z^2+4z+4}$</td>
<td>![Diagram 2]</td>
</tr>
<tr>
<td>$\frac{2z^2+8z+8}{-z^2-4z-2}$</td>
<td>![Diagram 3]</td>
</tr>
<tr>
<td>$\frac{2z^2+8z+8}{-z^2-4z+4}$</td>
<td>![Diagram 4]</td>
</tr>
<tr>
<td>$\frac{2z^2+4z+4}{-z^2}$</td>
<td>![Diagram 5]</td>
</tr>
<tr>
<td>$\frac{2z^2+8z+8}{-z^2-4z}$</td>
<td>![Diagram 6]</td>
</tr>
</tbody>
</table>

Table 5.3. Rational preperiodic points portrait
Figure 5.1. All possible rational preperiodic graphs for \( \phi_b(z) = z^2 + \frac{b}{z} \).

(a) \( b = 1 \)

(b) \( b = 1/2 \)

(c) \( b = -3/2 \)

(d) \( b = -1/2 \)

Figure 5.2. All possible rational preperiodic graphs for \( \theta_t(z) = \frac{t}{z^2} \).

(a) \( \theta_1(z) = \frac{1}{z^2} \)

(b) \( \theta_2(z) = \frac{2}{z^2} \)

Figure 5.3. More possibilities and their related maps

(a) \( \phi(z) = \frac{z^2 - 4z + 3}{z^2 - 2z + 2} \)

(b) \( \phi(z) = -\frac{4z}{z^2 + 2} \)

(c) \( \phi(z) = \frac{z^2 + 2z + 1}{z^2 + 2z - 1} \)

(d) \( \phi(z) = -\frac{(z-2)z}{2z-1} \)

Figure 5.4. \( \phi(z) = \frac{2z - 1}{z^2 - 1} \) has rational points on a three-cycle.
Appendix A

Sage Code

# This is based on orbit_structure_modp
# n is the number of primes you want to compare.

load "ProjSpace.sage"

PS.<x,y>=ProjSpace(1,QQ)
H = Hom(PS,PS)

def is_pcf(f, n):
    a = gcd(f[0],f[1])
    b = lcm(f[0].denominator(),f[1].denominator())
    f.scale_by(b/a)
    res = f.resultant()
    bp = set(res.support())
    primes = set(primes_first_n(n+10)).difference(bp)
    plist = list(primes)[2:n]
    cp = f.critical_points()
    F = f.change_ring(ZZ)
    wronskian = [F.wronskian().change_ring(ZZ), y^2]
for c in cp:
P = c[0]
P.scale_by(lcm(P[0].denominator(),P[1].denominator()))

# If the critical point is rational:
if P[0] in QQ:
    Q = P.change_ring(ZZ)
    if check_periods(F, Q, plist):
        continue
    else:
        return False

# Non-rational critical points
else:
    AS.<x> = AffSpace(1,QQ)
    R = AS.coordinate_ring()
    w = H(wronskian).dehomogenize(1)
    d = R(w[0]).discriminant(x)

    # find the good primes coprime to d
    ps = []
    for p in plist:
        if kronecker(d, p) == 1:
            ps.append(p)

    # For each such p, solve for the critical point equation
    for p in ps:
        PF = PS.change_ring(GF(p))
        G = Hom(PF, PF)
        crits = G(wronskian).critical_points()

    # check global periods
    for c in crits:
        C1 = c[0]
        # C1.scale_by(lcm(C1[0].denominator(), C1[1].denominator()))
C = C1.change_ring(ZZ)
if check_periods(F, C, ps):
    continue
else:
    return False

return True

def check_periods(F, P, plist):
    periods = []
copy = set(plist).copy()
p1 = copy.pop()
period1 = possible_periods(F, P, p1)
periods.extend(period1)

for p in copy:
    new_periods = possible_periods(F, P, p)
    periods = set(periods) & set(new_periods)

if len(periods) == 0:
    return False
else:
    return True

# Find possible period lengths of Q mod p
def possible_periods(F, Q, p):
    orbit = F.orbit_structure_modp(Q,p)
    tail = orbit[0]
m = orbit[1]
periods = []
periods.append(m)

if tail == 0:
    return periods
else:
PF = PS.change_ring(GF(p))
HF = Hom(PF, PF)
R = Q.change_ring(GF(p))
G = HF([F[0], F[1]])

periodic_point = G.nth_iterate(R, tail)
multiplier = G.multiplier(periodic_point, m)

if mod(multiplier[0,0], p) == 0:
    return periods
else:
    r = multiplicative_order(mod(multiplier[0,0], p))
    periods.append(m*r)
    return periods

# For rational maps of the form F(z), with parameters s1, s2.

N1 = iter(IntegerRange(-192, 193, 1, 0))
for n1 in N1:
    D1 = iter(IntegerRange(0, 8))
    for d1 in D1:
        if d1 == 0 or n1/2 not in ZZ:
            s1 = n1/2^d1
    N2 = iter(IntegerRange(-12288, 12289, 1, 0))
    for n2 in N2:
        D2 = iter(IntegerRange(0, 14))
        for d2 in D2:
            if d2 == 0 or n2/2 not in ZZ:
                s2 = n2/2^d2
                if 36 - 12*s2 + 4*s2^2 == 12*s1 - s1^2 + 2*s1 - s2 + s1^2*s2:
                    f = H([2*x^2 + (2-s1)*x*y + (2-s1)*y^2, -x^2 + (2-s1)*x*y + (2-s1-s2)*y^2])
                    if is_pcf(f, 25):
                        print "(s1, s2) = ", (s1, s2)
                        print f
Bibliography


