# FRACTIONAL LINEAR MINIMAL MODELS OF RATIONAL FUNCTIONS

by

Alexander Molnar

B.Sc. (Mathematics), Simon Fraser University, 2009

Thesis submitted in partial fulfillment

of the requirements for the degree of

Master of Science

in the

Department of Mathematics

Faculty of Science

© Alexander Molnar 2011

SIMON FRASER UNIVERSITY

Fall 2011

All rights reserved.
However, in accordance with the *Copyright Act of Canada*, this work may be reproduced, without authorization, under the conditions for "Fair Dealing." Therefore, limited reproduction of this work for the purposes of private study, research, criticism, review, and news reporting is likely to be in accordance with the law, particularly if cited appropriately.

# APPROVAL

**Name:** Alexander Molnar

**Degree:** Master of Science

**Title of Thesis:** Fractional linear minimal models of rational functions

**Examining Committee:** Dr. Jonathan Jedwab (Chair)

---

Dr. Nils Bruin
Associate Professor of Mathematics
Simon Fraser University
Senior Supervisor

---

Dr. Imin Chen
Associate Professor of Mathematics
Simon Fraser University
Supervisor

---

Dr. Karen Yeats
Assistant Professor of Mathematics
Simon Fraser University
Internal examiner

**Date Approved:** September 9, 2011

# Partial Copyright Licence


The author, whose copyright is declared on the title page of this work, has granted to Simon Fraser University the right to lend this thesis, project or extended essay to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users.

The author has further granted permission to Simon Fraser University to keep or make a digital copy for use in its circulating collection (currently available to the public at the "Institutional Repository" link of the SFU Library website (www.lib.sfu.ca) at http://summit/sfu.ca and, without changing the content, to translate the thesis/project or extended essays, if technically possible, to any medium or format for the purpose of preservation of the digital work.

The author has further agreed that permission for multiple copying of this work for scholarly purposes may be granted by either the author or the Dean of Graduate Studies.

It is understood that copying or publication of this work for financial gain shall not be allowed without the author's written permission.

Permission for public performance, or limited permission for private scholarly use, of any multimedia materials forming part of this work, may have been granted by the author. This information may be found on the separately catalogued multimedia material and in the signed Partial Copyright Licence.

While licensing SFU to permit the above uses, the author retains copyright in the thesis, project or extended essays, including the right to change the work for subsequent purposes, including editing and publishing the work in whole or in part, and licensing other parties, as the author may desire.

The original Partial Copyright Licence attesting to these terms, and signed by this author, may be found in the original bound copy of this work, retained in the Simon Fraser University Archive.

Simon Fraser University Library
Burnaby, British Columbia, Canada

revised Fall 2011

# Abstract

Many arithmetic geometric results have an arithmetic dynamic analogue. For instance, Siegel's theorem, that an elliptic curve has only finitely many integer points, is analogous to the fact that any orbit under a rational function whose second iterate has a non-constant denominator has only finitely many distinct integer values.

A conjecture of Lang states that the number of integer points on a minimal Weierstrass model of an elliptic curve is uniformly bounded. In order to translate this conjecture, one needs a dynamic concept of minimality. We present two such notions, affine minimality and full $\mathrm{PGL}_2(\mathbb{Q})$-minimality, and prove they are equivalent. We also present an algorithm to test minimality.

Finally, we present the results of an exhaustive search for rational functions with many integers in an orbit. These provide the best known minima for uniform bounds on the number of integers in orbits.

*To skiing... May life always be a little more than interesting.*

# Acknowledgments

I would like to thank everyone that stood by to help me through my recovery since March. Lily, my parents, Michael, all my friends who came by to see how I was doing, all the medical staff who kept me going, all the staff at SFU who helped me get everything sorted out once I returned, and most importantly my supervisor, Nils, for his never-ending patience dealing with my slow return to 'normal'.

# Contents

# Chapter 1

# Overview

Much attention has been given to the study of iterations of rational functions over $\mathbb{Q}$ recently. Many fundamental questions from the study of elliptic curves have been asked in an arithmetic dynamical setting. In particular, we are interested in the analogue of a conjecture of Lang on the number of integral points that can be found on certain elliptic curves ([4, page 140]). In our setting, we are interested in how many integers can occur in orbits of rational maps over $\mathbb{Q}$, where an orbit is the set of all iterated images (i.e., for $\alpha \in \mathbb{Q}$, the orbit of $\alpha$ is the set $\{\phi^n(\alpha) : n \geq 0\}$, where $\phi^n(\alpha) = \underbrace{\phi(\phi(\ldots\phi(\alpha)))}_{n}$. Obviously, the orbit of an integer under a polynomial with integer coefficients consists entirely of integers. However, Silverman proved that if $\phi(\phi(z))$ is not a polynomial, then any orbit of $\phi(z)$ contains only finitely many integers.

One may wonder if one can give a uniform bound on the number of integers that can occur in an orbit of a rational map. In general the answer is negative, as the following example shows. Take the map $\phi(z) = (z^2 + z + 1)/(z + 1)$ and look at the orbit of 0. The orbit is $\{0, 1, 3/2, \ldots\}$ and we have a denominator of two appearing, so we consider the map $\psi(z) = 2\phi(z/2)$ and the corresponding orbit of 0 under $\phi$. We have $\{0, 2, 3, \ldots\}$ and we have scaled away the denominator! We can do this repeatedly, and get arbitrarily many integers in an orbit. Note that the two functions $\phi$ and $\psi$ above have orbits $\{0 = z_0, z_1, z_2, \ldots\}$ and $\{0 = z'_0, z'_1, z'_2, \ldots\}$ respectively, where $z'_i = 2z_i$ for $i = 0, 1, \ldots$. In this sense, $\phi$ and $\psi$ represent the same map, up to

a change of coordinates. We will define a quantity, called the *resultant* of a rational map, that can detect this scaling. We will see that $\mathrm{Res}(\psi) = 2^4 \mathrm{Res}(\phi)$.

We can consider all possible changes of coordinates $z' = \frac{az+b}{cz+d}$. The corresponding changed functions are called $\mathrm{PGL}_2(\mathbb{Q})$-conjugates of $\phi$. We say that $\phi$ is $\mathrm{PGL}_2(\mathbb{Q})$-minimal if $\mathrm{Res}(\phi)$ is minimal among its $\mathrm{PGL}_2(\mathbb{Q})$-conjugates.

In Chapter 3, we restrict ourselves to affine changes of coordinates, i.e., $z' = az+b$. This gives rise to the notion of affine minimal maps. We prove that the notion coincides with full $\mathrm{PGL}_2(\mathbb{Q})$-minimality. We also develop an algorithm to test whether a rational map is minimal, and if it is not, return a minimal representation of the map.

In Chapter 4, we present results from two large searches. We search degree 2 and 3 rational maps to see how many integers we can get in a single orbit of a minimal model. For the degree 2 case we searched through 160 billion rational maps and found 5 minimal, with 8 integer points in an orbit such as

$$\phi(z) = \frac{86z^2 - 1068z - 338}{z^2 + 7z - 338},$$

with the orbit $\{0, 1, 4, 11, 12, 7, 15, -374, 59183/652, \ldots\}$ of 0 under $\phi$. We did not find any orbits with 9 integer values. In the degree 3 case, we searched 640 000 000 rational maps. We found 56 minimal rational maps with 10 integer points in an orbit. For example

$$\psi(z) = \frac{115z^3 + 558z^2 + 257z - 90}{-6z^3 - 74z^2 - 110z - 90},$$

with orbit $\{0, 1, -3, -4, -1, -2, -6, 8, -11, -582, -3746989832/192970427, \ldots\}$ of 0 under $\psi$. We did not find any orbits with 11 integer values. Interestingly, in both cases we were able to find degree $d$ maps with $2d + 4$ integers.

# Chapter 2

# Background and Notation

## 2.1 Motivation

Most questions we consider for dynamical systems are analogous to questions and results from the already well established field of arithmetic of elliptic curves. We briefly introduce some concepts in the arithmetic of elliptic curves. For a thorough introduction, see [6]. Let $K$ be a field. If $K$ is a number field, let $R$ be its ring of integers. For our purposes, we consider a model of an elliptic curve over a field $K$, the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{where } a_1, a_2, a_3, a_4, a_6 \in K. \tag{2.1}$$

We consider the *points on* $E$, the $(x, y) \in K^2$ that satisfy the equation, together with an extra point (the point 'at infinity') $\mathcal{O}$. It is a requirement that the curve described by (2.1) is non-singular. This can be detected by the discriminant of the cubic equation (2.1). The general formula is a bit too bulky to reproduce here. When $a_1 = a_3 = a_2 = 0$ (a situation one can always reduce to if $K$ is of characteristic different from $2, 3$), the discriminant is given by

$$\Delta = -16(4a_4^3 + 27a_6^2).$$

Equation (2.1) describes a non-singular curve if and only if the discriminant is non-zero. We consider models isomorphic if they are related by transformations of the form $(x, y) \mapsto (a^2x + b, a^3y + ca^2x + d)$, where $a, b, c, d \in K$. We call the set of all

isomorphic models an elliptic curve. When confusion is unlikely, we use $E$ to refer to both the elliptic curve and to a representing model.

Let $n \in \mathbb{Q}$, $n \neq 0$, and let $p$ be a prime number. We can always find unique integers $v, N, D$ with $N > 0$, $D \neq 0$ and $p \nmid N, D$ such that $n = p^v \frac{N}{D}$.

**Definition 2.1.1.** We define the *valuation* of $n \neq 0$ at $p$, the exponent $v$ described above, and denote it by $\mathrm{ord}_p(n)$. We also define the *p-adic absolute value*, $|n|_p = p^{-v}$.

It is easy to show that the $p$-adic absolute value is actually a metric on $\mathbb{Q}$.

**Definition 2.1.2.** Let $p$ be a prime. We define the *p-adic numbers*, $\mathbb{Q}_p$, to be the completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value. We also define the *p-adic integers*, $\mathbb{Z}_p$, as the completion of $\mathbb{Z}$ under the $p$-adic absolute value.

The most striking difference between $p$-adic absolute values and the ordinary one, is the *non-Archimedean* triangle inequality. For any two elements, $a, b \in \mathbb{Q}_p$, we have

$$|a+b|_p \leq \max(|a|_p, |b|_p) \text{ or}$$
$$\mathrm{ord}_p(a+b) \geq \min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$$

where equality holds if $|a|_p \neq |b|_p$ (or $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(b)$). For a thorough introduction to $p$-adic numbers, see [3].

If we let $K = \mathbb{Q}_p$ for some prime $p$ we can see that the change of coordinates of models of elliptic curve may change the discriminant. In particular, the valuation of the discriminant, $\mathrm{ord}_p(\Delta)$, may change, and we measure a representation using the valuation of the discriminant.

**Definition 2.1.3.** Let $E$ be an elliptic curve over $\mathbb{Q}$. An equation of the form (2.1) is called a *minimal equation at p for E* if $\mathrm{ord}_p(\Delta)$ is minimal among all the equations describing $E$, subject to the condition that $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$.

We also have a global version.

**Definition 2.1.4.** Let $E$ be an elliptic curve over $\mathbb{Q}$. An equation as above is called a *minimal equation for E* if $\mathrm{ord}_p(\Delta)$ is minimized in the isomorphism class $E$ for all primes $p$, subject to the condition that $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$.

These concepts for minimal equations of elliptic curves can be generalized to local fields. It is known that every elliptic curve over $\mathbb{Q}$ has a minimal equation. More generally, we have that every elliptic curve over $\mathbb{Q}_p$ has a minimal equation [6, Proposition 1.3(a) of Chapter VII] and an algorithm of Tate [7, Chapter IV Section 9] can take an equation for an elliptic curve and test whether it is minimal at $p$ or not, and if not return a minimal representation at $p$.

We say a point, $(x, y)$, on a model of an elliptic curve is an *integral point* if $x, y \in \mathbb{Z}$. This notion is dependent on the equation chosen to represent $E$. There is a nice theorem due to Siegel on the number of integral points that can occur on an elliptic curve over $\mathbb{Q}$.

**Theorem 2.1.5** (Siegel. Theorem 4.3 in [6]). *Let $f(x) \in \mathbb{Q}[x]$ be a cubic polynomial with distinct roots. Then the equation*

$$y^2 = f(x)$$

*has only finitely many solutions such that $x, y \in \mathbb{Z}$.*

Given this, one can ask how many integral points can appear on a particular model for an elliptic curve. The answer is arbitrarily many (see [9]), due to a nice scaling trick. For example, consider the elliptic curve given by $y^2 = x^3 + c$ for $c \in \mathbb{Z}$. If we have a rational solution $(p, q)$, then we have $q^2 = p^3 + c$. For any $r \in \mathbb{Q}$ we then have $rq^2 = rp^3 + rc$, so if we choose $r$ a 6-th power of an integer, say $r = s^6$, we have $(s^3q)^2 = (s^2p)^3 + s^6c$. Thus if we let $s$ be the lowest common multiple of the denominators of $p$ and $q$, the rational point $(p, q)$ on $y^2 = x^3 + c$ corresponds to the integral point $(s^2p, s^3q)$ on $\tilde{y}^2 = \tilde{x}^3 + cs^6$. Further, notice any integral point on $y^2 = x^3 + c$ will also correspond to an integral point on $\tilde{y}^2 = \tilde{x}^3 + cs^6$, so every time we apply a scaling, we increase the number of integral points satisfying the equation. If we have a model of an elliptic curve with infinitely many rational points, we could scale them one by one, to get elliptic curves with an arbitrarily large number of integral points. As an example, $y^2 = x^3 - 2$ is such a curve [6, Chapter IX].

However this scaling of the equation to get more integral points has an effect on the discriminant. The curve $y^2 = x^3 + c$ has discriminant $-432c^2$ whereas the discriminant of $\tilde{y}^2 = \tilde{x^3} + cs^6$ is $-432c^2s^{12}$, with $s \geq 1$. The model with more integral

points has a larger discriminant, so we may ask the question: How many integral points can appear on a minimal model of an elliptic curve? A conjecture of Lang ([4, page 140]) says the number of integral points that can occur on a minimal model of an elliptic curve over $\mathbb{Q}$ is uniformly bounded.

## 2.2 Dynamics

Given the questions studied on elliptic curves, we would like to investigate their analogues in the dynamical setting, where we study rational maps. We develop notions for changes of coordinates for rational maps which preserve the dynamics. We then study the effect of these changes, and construct an object similar to the discriminant, to put a notion of size on each rational map. From here we define our minimal rational maps, and ask integrality question about the orbits of minimal maps.

**Definition 2.2.1.** A *dynamical system* is a set $S$ together with a map $\phi\colon S \to S$.

**Definition 2.2.2.** We call the *forward orbit* of a point $\alpha \in S$ the set

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

where $\phi^n(\alpha) = \phi(\phi(\dots\phi(\alpha)))$.

We distinguish points in $S$ by their orbits as follows

**Definition 2.2.3.** (a) If the forward orbit of a point $\alpha \in S$ is finite, we call $\alpha$ *preperiodic*.

(b) As a special case for preperiodic points, we call a point $\alpha$ *periodic* if there exists a positive integer $n$ with $\phi^n(\alpha) = \alpha$. The smallest such $n$ is called the *period* of $\alpha$.

(c) If the orbit of $\alpha$ is infinite, $\alpha$ is called a *wandering point*.

A *homogeneous polynomial* is a polynomial whose monomials with non-zero coefficients all have the same total degree. For any polynomial $P \in \mathbb{Q}[z]$ of degree at most $d$, we call the *d-form homogenization*, the polynomial

$$h(z, z') = (z')^d P\left(\frac{z}{z'}\right).$$

As a special case, if the degree of $P$ is $d$, we simply call $h(z, z')$ the homogenization of $P$. All the monomials of $h$ with non-zero coefficients have the same total degree, hence $h$ is a homogeneous polynomial. We call a homogeneous polynomial with each monomial having total degree $d$, a *$d$-form.*

We are ultimately interested in studying the dynamics of rational functions over $\mathbb{Q}$. However, rational functions are not defined at points where their denominators vanish, so we must extend the domain to the projective line $\mathbb{P}^1$, in particular, $\mathbb{P}^1(\mathbb{Q})$.

**Definition 2.2.4.** The *projective line* of a field $K$ is the set $\mathbb{P}^1(K) = \{(a, b) : a, b \in K \text{ and } (a, b) \neq (0, 0)\}/\sim$ where $(z, y) \sim (\lambda z, \lambda y)$ for all non-zero $\lambda \in K$

Now set $K = \mathbb{Q}$. We write $(a : b) \in \mathbb{P}^1(\mathbb{Q})$ for the equivalence class of $(a, b)$. If $F, G \in \mathbb{Q}[z, y]$ are homogeneous polynomials of equal degree $d$, then

$$(F(\lambda a, \lambda b) : G(\lambda a, \lambda b)) = (\lambda^d F(a, b) : \lambda^d G(a, b)).$$

Hence

$$\begin{aligned} \phi\colon \mathbb{P}^1(\mathbb{Q}) &\to \mathbb{P}^1(\mathbb{Q}) \\ (a : b) &\mapsto (F(a, b) : G(a, b)) \end{aligned}$$

is well-defined outside common zeros of $F, G$. We call this a *rational map.* If we have three homogeneous polynomials $F, G$ and $H$ in $\mathbb{Q}[z, y]$, we note $(FH : GH)$ and $(F : G)$ agree where they are both defined, since if they are defined at a point $(a, b)$ we have $(F(a, b)H(a, b) : G(a, b)H(a, b)) = (\lambda F(a, b) : \lambda G(a, b))$ with $\lambda = H(a, b)$. We wish to show, for polynomials $F, G \in \mathbb{Q}[z, y]$, we can always find $R \in \mathbb{Q}[z, y]$ such that $F = R\tilde{F}$ and $G = R\tilde{G}$ where $\tilde{F}$ and $\tilde{G}$ have no complex roots in common. To this end, we have

**Lemma 2.2.5.** *Let $F, R \in \mathbb{Q}[z, y]$ be irreducible homogeneous polynomials with $\deg(R) \leq \deg(F)$ and $F \neq \lambda R$ for any $\lambda \in \mathbb{Q}$. There are no $(a, b) \in \mathbb{C}^2$, not $(0, 0)$ such that $F(a, b) = R(a, b) = 0$.*

*Proof.* We use a proof by contradiction. Assume we have $(a, b) \neq (0, 0)$ such that $F(a, b) = R(a, b) = 0$ and suppose $b \neq 0$ (otherwise, exchange the roles of $z$ and $y$). Write $F_d(z) = F(z, 1)$ and $R_d(z) = R(z, 1)$. As $F$ and $R$ are irreducible, this

implies $F_d$ and $R_d$ are irreducible, and must be relatively prime, so there exist two polynomials $P, Q \in \mathbb{Q}[z]$ such that $F_d(z)P(z) + R_d(z)Q(z) = 1$. Plugging in $a/b$ shows $0 = 1$, which is not possible. Hence $R_d$ divides $F_d$, and $R$ divides $F$, our desired contradiction. □

Given this lemma, for any pair of polynomials $F, G \in \mathbb{Q}[z, y]$ we may write $F = RF'$ and $G = RG'$, where $R$ is the product of all the common factors of $F$ and $G$, and $\gcd(F', G') = 1$. Hence any rational map can be extended to all of $\mathbb{P}^1(\mathbb{Q})$. When dealing with a rational map, unless stated otherwise, we will always be referring to a map that exists on all of $\mathbb{P}^1(\mathbb{Q})$.

If $F(z, y) = az + by$ and $G(z, y) = cz + dy$, with $a, b, c, d \in \mathbb{Q}$, then

$$\begin{aligned} A\colon \mathbb{P}^1(\mathbb{Q}) &\to \mathbb{P}^1(\mathbb{Q}) \\ (x : y) &\mapsto (ax + by : cx + dy) \end{aligned}$$

is bijective if and only if $ad - bc \neq 0$, i.e., if the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible. Indeed, the inverse of $A$ is

$$\begin{aligned} A^{-1}\colon \mathbb{P}^1(\mathbb{Q}) &\to \mathbb{P}^1(\mathbb{Q}) \\ (x : y) &\mapsto (dx - by : -cx + ay) \end{aligned}$$

where $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ is the inverse matrix of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We call these rational maps *fractional linear transformations*. It is straightforward to check that two matrices $A, B \in \mathrm{GL}_2(\mathbb{Q})$ give rise to the same fractional linear transformation if and only if $A = \lambda B$ for some $\lambda \in \mathbb{Q}$. Thus, we see that fractional linear transformations are in bijection with $\mathrm{PGL}_2(\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Q})/\left\{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{Q}^*\right\}$. One can check that composition of fractional linear transformations corresponds to matrix multiplication so the bijection is a group isomorphism. Any fractional linear transformation $A \in \mathrm{PGL}_2(\mathbb{Q})$ is an automorphism of $\mathbb{P}^1(\mathbb{Q})$, and it turns out these are the only automorphisms, as proved in [2, Example 7.1.1]. We will also have use for the group $\mathrm{PGL}_2(\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z})/\left\{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \{-1, 1\}\right\}$.

*Remark.* We may consider $\mathrm{PGL}_2(\mathbb{Z})$ a subgroup of $\mathrm{PGL}_2(\mathbb{Q})$. Since

$$\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{Q}^* \right\} \cap \mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{Z}^* \right\}$$

we do indeed have that the natural map from $\mathrm{GL}_2(\mathbb{Z})$ to $\mathrm{GL}_2(\mathbb{Q})$ descends to a well-defined injection of $\mathrm{PGL}_2(\mathbb{Z})$ into $\mathrm{PGL}_2(\mathbb{Q})$.

Now fix

$$\begin{aligned} \mathbb{Q} &\to \mathbb{P}^1(\mathbb{Q}) \\ a &\mapsto (a:1) \end{aligned}$$

and notice that any rational map $\phi \in \mathbb{Q}(z)$, say $\phi = F/G$, with $\gcd(F,G) = 1$ and $d = \max(\deg(F), \deg(G))$ corresponds to the rational map

$$\begin{aligned} \phi\colon \mathbb{P}^1(\mathbb{Q}) &\to \mathbb{P}^1(\mathbb{Q}) \\ (a:1) &\mapsto (h_F(a,1) : h_G(a,1)), \end{aligned}$$

where $h_F$ and $h_G$ are the respective $d$-form homogenizations of $F$ and $G$. Hence, we may do all our work in $\mathbb{P}^1(\mathbb{Q})$ just by working with our map $\phi \in \mathbb{Q}(z)$ as long as the denominator of $\phi$ does not vanish. We define the degree of a rational function $F/G$ to be the maximum of the degrees of $F$ and $G$, when $\gcd(F,G) = 1$.

We can ask how many integers we can have occur in a single orbit for a dynamical system. We notice a polynomial map, such as $\phi(z) = z^2 + 2$ can certainly admit an infinite number of integers. For example, we may look at the forward orbit of zero. $\mathcal{O}_\phi(0) = \{0, 2, 6, 38, \ldots\}$. Even a non-polynomial rational map can have infinitely many distinct integral points in an orbit, as $\phi(z) = 1/z^2$ shows. Notice $\phi(\phi(z)) = z^4$ so every second point in a forward orbit of an integer will be an integer. If an iterate of a rational map is a polynomial it may be possible to have an orbit with infinitely many distinct integer values. Note that if a polynomial has non-integral coefficients, then an orbit of an integer does not need to consist of integers. Silverman characterized when a rational map has a polynomial iterate by studying the ramification of the iterates, and uses Riemann-Hurwitz to bound the possible ramification types. We state the result here, but the proof is beyond the scope of this thesis.

**Theorem 2.2.6** (Theorem 1.7 in [8]). *Let $\phi\colon \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$ be a rational map of degree $d \geq 2$, and suppose that $\phi^n$ is a polynomial map for some $n \geq 1$. Then already $\phi^2$ is a polynomial map. Furthermore, if $\phi$ itself is not a polynomial map, then there exists an $f \in \mathrm{PGL}_2(\mathbb{Q})$ such that $f^{-1} \circ \phi \circ f$ is the function $1/z^d$.*

This characterizes the rational maps that can trivially have infinitely many integers in an orbit, so we can ask what happens when we have a rational map $\phi \in \mathbb{Q}(z)$ such that $\phi^2 \notin \mathbb{Q}[z]$. In fact, Siegel has a corresponding theorem for any rational map with at least 3 poles, that uses some Diophantine approximation results of Roth and Thue.

**Theorem 2.2.7** (Theorem 3.36 in [8]). *Let $\phi \in \mathbb{Q}(z)$ be a rational function with at least three distinct poles in $\mathbb{P}^1(\mathbb{C})$. Then*

$$\{\alpha \in \mathbb{Q} : \phi(\alpha) \in \mathbb{Z}\}$$

*is a finite set.*

This answers our question of how many integers can appear in a single orbit, for all rational maps with at least three distinct poles.

**Corollary 2.2.8.** *Let $\phi \in \mathbb{Q}(z)$ be a rational function with at least three distinct poles in $\mathbb{P}^1(\mathbb{C})$. Then any orbit under $\phi$ contains only finitely many distinct integers.*

*Proof.* As above, we have the set $\{\alpha \in \mathbb{Q} : \phi(\alpha) \in \mathbb{Z}\}$ contains only finitely many integers. Let $\beta \in \mathbb{Q}$ and consider the orbit of $\beta$ under $\phi$. This is the set $\mathcal{O}_\phi(\beta) = \{\beta, \phi(\beta), \phi(\phi(\beta)), \ldots\}$, so any integers in $\mathcal{O}_\phi(\beta)$ must occur in $\{\beta\} \cup \{\alpha \in \mathbb{Q} : \phi(\alpha) \in \mathbb{Z}\}$, hence the orbit can only contain finitely many distinct integers. □

We would like to remove the requirement of three distinct poles, but this is not quite elementary, as Theorem 2.2.7 is sharp in the sense that a rational function over $\mathbb{Q}$ with only two poles can indeed have infinitely many integral values. Consider

$$\phi(z) = \frac{F(z)}{(z^2 - D)^d}$$

where $D > 1$ is a square free integer, and $F \in \mathbb{Z}[z]$ is a polynomial of degree $2d$. The Pell equation $u^2 - Dv^2 = 1$, has infinitely many solutions $(u, v) \in \mathbb{Z}^2$. These give

infinitely many values $\frac{u}{v} \in \mathbb{Q}$ such that $\phi(\frac{u}{v}) = v^{2d}F(\frac{u}{v})$ is an integer. However, with a little extra work, Theorem 2.2.7 can still provide a result on integer points in orbits of rational functions with less than 3 poles.

In fact, with careful analysis of the preimages of $\infty$, one can appeal to the Riemann-Hurwitz formula once more to find that any rational map $\phi \in \mathbb{Q}(z)$, of degree at least 2, with $\phi^2 \notin \mathbb{Q}[z]$ has has a fourth iterate ($\phi^4(z)$) with at least 3 poles. One can then appeal to Theorem 2.2.7 and find that $\phi^2 \notin \mathbb{Q}[z]$ is enough to guarantee every orbit of $\phi$ can have only finitely many integers. Again the proof is beyond the scope of the thesis, but we state the result.

**Theorem 2.2.9** (Theorem 3.43 in [8]). *Let $\phi \in \mathbb{Q}(z)$ be a rational map of degree $d \geq 2$ with the property that $\phi^2 \notin \mathbb{Q}[z]$. Let $\alpha \in \mathbb{Q}$ be a wandering point for $\phi$. Then the orbit $\mathcal{O}_\phi(\alpha)$ contains only finitely many integers.*

If we try to determine how many integer points can occur in an orbit, we find ourselves in a situation similar to the one for elliptic curves, where we can get arbitrarily many.

**Example 2.2.10.** Let $\phi(z) = (z^2+z+1)/(z^2-z+1)$ and consider the forward orbit of 0. We have $\mathcal{O}_\phi(0) = \{0, 1, 3, 13/7, \ldots\}$. Consider the map $\psi(z) = 7\phi(z/7)$ and the corresponding orbit of 0. We have $\mathcal{O}_\psi(0) = \{0, 7, 21, 13, \ldots\}$ and we have scaled away the denominator of 7.

By applying this trick repeatedly we can have arbitrarily many integer points in a single orbit. We consider this cheating, as with the trick for elliptic curves. and we wish to find conditions on rational maps to prevent this. We start with some definitions to introduce a quantity that can detect when scaling occurs.

**Definition 2.2.11.** Let $\phi \in \mathbb{Q}(z)$ be a rational map. We call a pair of polynomials $[F, G]$ a *representation* of $\phi$ if $\phi = F/G$. We call a representation *normalized* if $F, G \in \mathbb{Z}[z]$, no prime divides all the coefficients of $F$ and $G$ and $F, G$ have no complex roots in common.

We define the $p$-adic valuation of a polynomial over $\mathbb{Q}$, to be the minimum valu-

ation of its coefficients.

$$\mathrm{ord}_p\left(\sum_i f_i z^i\right) = \min_i(\mathrm{ord}_p(f_i)).$$

**Definition 2.2.12.** We say a representation is *normalized at p* if $F, G \in \mathbb{Q}[z]$, $F$ and $G$ have no complex roots in common, and $\min(\mathrm{ord}_p(F), \mathrm{ord}_p(G)) = 0$.

**Proposition 2.2.13.** *Let $\phi \in \mathbb{Q}(z)$ be a rational map and let $[F, G]$ be a representation of $\phi$. This representation is normalized if and only if it is normalized at $p$ for every prime $p$.*

*Proof.* First, suppose $[F, G]$ is a normalized representation of $\phi$. Hence, $F, G \in \mathbb{Z}[z]$. Let $p$ be a prime. Since the representation is normalized, $p$ does not divide all the coefficients, hence there is a coefficient $c$, of $F$ or $G$, such that $\mathrm{ord}_p(c) = 0$. Therefore the representation is normalized at $p$ for every prime $p$. Conversely, suppose $[F, G]$ is a normalized representation at $p$ for every prime $p$. For every prime there is a coefficient, $c$, of $F$ or $G$ with $\mathrm{ord}_p(c) = 0$, and no coefficients have negative valuation. This means, for every prime $p$ there exists a coefficient not divisible by $p$, and no coefficients have a prime in their denominator, which is precisely the definition of being normalized. Hence a representation is normalized if and only if it is normalized at every prime. □

**Lemma 2.2.14.** *Every non-constant rational map $\phi \in \mathbb{Q}(z)$ has a normalized representation. We shall denote the normalized representation by $[F_\phi, G_\phi]$. In order to ensure the representation is well defined, we always ask that the leading non-zero coefficient of $F_\phi$ be positive.*

*Proof.* Naively, if we have a rational map $\phi(z) = F(z)/G(z) = (a_n z^n + a_{n+1} z^{n+1} + \ldots + a_1 z + a_0)/(b_n z^n + b_{n+1} z^{n+1} + \ldots + b_1 z + b_0)$ where $a_i, b_i \in \mathbb{Q}$ for all $i$, $1 \leq i \leq n$ and $n > 0$ we can take the product of all the denominators of the $a_i$ and $b_i$ and call it $c$. Multiplying the numerator and denominator by $c$ then gives us an integral representation $\phi = cF/cG = F_c/G_c$ with $F_c, G_c \in \mathbb{Z}[z]$. Taking the greatest common divisor of the coefficients of $F_c$ and $G_c$ and calling it $g$, we have that $\phi = [(c/g)F, (c/g)G]$ is the normalized representation of $\phi$ if the leading non-zero coefficient of $F$ is positive, otherwise $\phi = [(-c/g)F, (-c/g)G]$ is the normalized representation of $\phi$. □

Write $F(z) = a_m z^m + a_{m-1} z^{m-1} + \dots a_1 z + a_0$ and $G(z) = b_n z^n + b_{n-1} z^{n-1} + \dots b_1 z + b_0$. We define the $(m,n)$-*Sylvester matrix* for $F$ and $G$ as the square $(m+n)\times(m+n)$ matrix

$$\mathrm{Syl}_{m,n}(F,G) = \begin{pmatrix} a_m & a_{m-1} & \dots & a_1 & a_0 & & & & \\ & a_m & a_{m-1} & \dots & a_1 & a_0 & & & \\ & & \ddots & \ddots & & \ddots & \ddots & & \\ & & & a_m & a_{m-1} & \dots & a_1 & a_0 & \\ & & & & a_m & a_{m-1} & \dots & a_1 & a_0 \\ b_n & b_{n-1} & \dots & b_1 & b_0 & & & & \\ & b_n & b_{n-1} & \dots & b_1 & b_0 & & & \\ & & \ddots & \ddots & & \ddots & \ddots & & \\ & & & b_n & b_{n-1} & \dots & b_1 & b_0 & \\ & & & & b_n & b_{n-1} & \dots & b_1 & b_0 \end{pmatrix}$$

where there are $n$ rows with coefficients $a_i$ and $m$ rows with coefficients $b_j$.

**Definition 2.2.15.** Let $F, G \in \mathbb{Q}[z]$. We define the *polynomial resultant* of $F$ and $G$ to be

$$\mathrm{res}(F,G) = \det(\mathrm{Syl}_{m,n}(F,G))$$

where $m = \deg(F)$ and $n = \deg(G)$.

We also have another nice characterization of the polynomial resultant.

**Lemma 2.2.16.** *Write* $F = a_m \prod_i^m (z - \alpha_i)$ *and* $G = b_n \prod_j^n (z - \beta_j)$. *Then the polynomial resultant of* $F$ *and* $G$ *is* $\mathrm{res}(F,G) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j)$.

The fact that these are equivalent can be found in, for example, Section 3.3.2 of [1].

**Definition 2.2.17.** Let $d$ be a positive integer. The *d-form resultant* of a pair of $d$-forms $F, G \in \mathbb{Q}[z,y]$ is

$$\mathrm{Res}_d(F,G) = |\det(\mathrm{Syl}_{d,d}(F(z,1), G(z,1)))|.$$

For univariate polynomials $F, G$ of degree less than or equal to $d$ (with at least one being degree $d$) we also write

$$\mathrm{Res}_d(F,G) = |\det \mathrm{Syl}_{d,d}(F,G)|$$

We call the *resultant of a rational map* $\phi = F/G$ the $d$-form resultant of the normalized representation for $\phi$. Namely,

$$\mathrm{Res}(\phi) = |\det(\mathrm{Syl}_{d,d}(F_\phi, G_\phi))|.$$

We shall require the following facts in Chapter 3,

**Proposition 2.2.18.** *Let $\phi = F/G \in \mathbb{Q}(z)$ be a rational map of degree $d$ and* $\gcd(F,G) = 1$. *Then*

*(a)* $\mathrm{Res}_d(F - \lambda G, G) = \mathrm{Res}_d(F,G)$ *for* $\lambda \in \mathbb{Q}$

*(b)* $\mathrm{Res}_d(F,G) = \mathrm{Res}_d(G,F)$.

*(c) Write* $F(z) = a_n z^n + \ldots + a_1 z + a_0$ *and* $G(z) = b_d z^d + \ldots + b_1 z + b_0$, *with* $n \leq d$ *and* $a_n b_d \neq 0$. *Then* $\mathrm{Res}_d(F,G) = |b_d^{d-n}\mathrm{res}(F,G)|$.

*For the next two parts, assume further that* $F, G \in \mathbb{Z}[z]$.

*(d) There exist polynomials* $A, B \in \mathbb{Z}[z]$ *of degree at most* $d-1$ *such that*

$$F(z)A(z) + G(z)B(z) = z^{2d-1}\mathrm{Res}_d(F,G)$$

*(e) There exist polynomials* $C, D \in \mathbb{Z}[z]$ *of degree at most* $d-1$ *such that*

$$F(z)C(z) + G(z)D(z) = \mathrm{Res}_d(F,G)$$

*Proof.* (a) Notice from the definition of the resultant, that $\mathrm{Res}_d(F - \lambda G, G)$ is the determinant of a Sylvester matrix which can be obtained from $\mathrm{Syl}_{d,d}(F,G)$ via $d$ row operations. Hence $\mathrm{Res}_d(F - \lambda G, G) = \mathrm{Res}_d(F,G)$.

(b) If we require $r$ row swaps to transform the matrix $\mathrm{Syl}_{d,d}(F,G)$ into $\mathrm{Syl}_{d,d}(G,F)$, the effect on the determinant is

$$\det(\mathrm{Syl}_{d,d}(F,G)) = (-1)^r \deg(\mathrm{Syl}_{d,d}(G,F)).$$

Since the $d$-form resultants are defined to be the absolute values of these, we have

$$\mathrm{Res}_d(F,G) = \mathrm{Res}_d(G,F).$$

(c) This is clear from writing out the Sylvester matrix $\mathrm{Syl}_{d,d}(F,G)$.

(d) See [8, Proposition 2.13]

(e) See [8, Proposition 2.13]

□

*Remark.* Part (b) of Proposition 2.2.18 tells us that if we are in a situation similar to part (c), with polynomials $F(z) = a_0+a_1z+\ldots+a_dz^d$ and $G(z) = b_0+b_1z+\ldots+b_mz^m$ with $m \leq d$, then we have

$$\mathrm{Res}_d(F,G) = |a_d^{d-n}\mathrm{res}(G,F)|.$$

Recall we are interested in an object in the dynamical setting that is analogous to the discriminant of an elliptic curve. We want an object that can tell us when this scaling has occurred, and we are ultimately interested in using the object to find maps where with no scaling. Let us investigate what happened to the resultant of the rational map in Example 2.2.10, where we scaled the entire orbit by 7. Recall we had

$$\begin{aligned}\phi(z) &= \frac{z^2+z+1}{z^2-z+1}, \text{ and}\\ \psi(z) &= 7\phi\left(\frac{z}{7}\right).\end{aligned}$$

Thus in order to consider the resultants $\mathrm{Res}(\phi)$ and $\mathrm{Res}(\psi)$ we must ensure we have normalized representations of both maps. We can see $F_\phi(z) = z^2+z+1$ and $G_\phi(z) = z^2 - z + 1$, but we must actually do a little work to find $F_\psi$ and $G_\psi$. We have

$$\begin{aligned}\psi(z) &= \frac{7(\left(\frac{z}{7}\right)^2 + \frac{z}{7} + 1)}{\left(\frac{z}{7}\right)^2 + \frac{z}{7} + 1} \\ &= \frac{49 \cdot 7(\left(\frac{z}{7}\right)^2 + \frac{z}{7} + 1)}{49(\left(\frac{z}{7}\right)^2 + \frac{z}{7} + 1)} \\ &= \frac{7z^2 + 49z + 343}{z^2 + 7z + 49}.\end{aligned}$$

Hence

$$\begin{aligned}\mathrm{Res}(\phi) &= \mathrm{Res}_2(z^2 + z + 1, z^2 - z + 1) = 2^2, \text{ and} \\ \mathrm{Res}(\psi) &= \mathrm{Res}_2(7z^2 + 49z + 343, z^2 - 7z + 49) = 2^2 \cdot 7^6.\end{aligned}$$

The resultant picked up the denominator we scaled out of the orbit! Applying a change in choice of coordinates corresponds to conjugating by $A \in \mathrm{PGL}_2(\mathbb{Q})$. Hence, in dynamics, the natural action of $\mathrm{PGL}_2(\mathbb{Q})$ on rational maps is via conjugation. Write

$$\phi^A = A^{-1} \circ \phi \circ A.$$

From

$$(\phi^A)^n = (A^{-1} \circ \phi \circ A) \circ \cdots \circ (A^{-1} \circ \phi \circ A) = A^{-1} \circ \phi^n \circ A$$

it follows that, up to choice of coordinates, the dynamics of $\phi$ and $\phi^A$ are the same. We also consider conjugating only by affine linear transformations, and we are interested in maps with minimal resultant in their affine conjugacy classes. To be precise, let

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}) \right\} \subset \mathrm{GL}_2(\mathbb{Q})$$

and define $\mathrm{Aff}_2(\mathbb{Q}) \subset \mathrm{PGL}_2(\mathbb{Q})$ to be the image of $T$ under $\mathrm{GL}_2 \to \mathrm{PGL}_2$. Then any element of $\mathrm{Aff}_2(\mathbb{Q})$ can be represented in the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, and these are precisely the transformations we wish to allow for conjugation.

**Definition 2.2.19.** Let $\phi \in \mathbb{Q}(z)$ be a rational map and let $p$ be a prime. We call $\phi$ *minimal at* $p$ (or $\mathrm{PGL}_2(\mathbb{Q})$-minimal at $p$) if

$$\mathrm{ord}_p(\mathrm{Res}(\phi)) = \min_{A \in \mathrm{PGL}_2(\mathbb{Q})} \mathrm{ord}_p(\mathrm{Res}(\phi^A)).$$

We say $\phi$ is *affine minimal at* $p$ if

$$\mathrm{ord}_p(\mathrm{Res}(\phi)) = \min_{A \in \mathrm{Aff}_2(\mathbb{Q})} \mathrm{ord}_p(\mathrm{Res}(\phi^A))$$

We also define global versions:

**Definition 2.2.20.** Let $\phi \in \mathbb{Q}(z)$ be a rational map. We call $\phi$ *minimal* or $\mathrm{PGL}_2(\mathbb{Q})$-*minimal* if

$$\mathrm{Res}(\phi) = \min_{A \in \mathrm{PGL}_2(\mathbb{Q})} \mathrm{Res}(\phi^A)$$

and we call $\phi$ *affine minimal* if

$$\mathrm{Res}(\phi) = \min_{A \in \mathrm{Aff}_2(\mathbb{Q})} \mathrm{Res}(\phi^A).$$

We will show in Chapter 3 that a rational map is affine minimal if and only if it is affine minimal at $p$ for every prime $p$. It is obvious from Definitions 2.2.19 and 2.2.20, that minimality implies affine minimality. In Theorem 3.1.3 we will show that we also have the converse.

We ask how many integer points can occur in a forward orbit of a point of an affine minimal function. Similar to Lang's conjecture on the number of integer points on elliptic curves, Silverman conjectures that the number of integers in any orbit of an affine minimal rational map is uniformly bounded.

**Conjecture 2.2.21** (Silverman, Conjecture 3.47 in [8])**.** Let $\phi \in \mathbb{Q}(z)$ be a rational map of degree $d \geq 2$ with $\phi^2 \notin \mathbb{Q}[z]$, and let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a wandering point for $\phi$. Assume further that $\phi$ is affine minimal. Then there is a constant $C = C(d)$ depending only on the degree of $\phi$ such that

$$\#(\mathcal{O}_\phi(\alpha) \cap \mathbb{Z}) \leq C.$$

In Chapter 3 we investigate what affine minimality of a rational map requires and develop an algorithm to compute affine minimal rational maps. We investigate finding rational maps with many integer points in a single orbit in Chapter 4.

# Chapter 3

# Minimality

## 3.1 Equivalence of Affine Minimality and $\mathrm{PGL}_2(\mathbb{Q})$-Minimality

We study some of the preliminaries of conjugation by $\mathrm{PGL}_2(\mathbb{Q})$ transformations and $\mathrm{PGL}_2(\mathbb{Z})$ transformations, then prove that affine minimality guarantees $\mathrm{PGL}_2(\mathbb{Q})$-minimality.

From the definition, any map $\phi \in \mathbb{Q}(z)$ of degree $d$, such that $\mathrm{Res}(\phi) = 1$ must be minimal. However, at this point, even if we have $\mathrm{Res}(\phi) = 2$, we cannot conclude $\phi$ is minimal. We investigate the effects of conjugation on the resultant a little more in depth.

Let $\phi = F/G \in \mathbb{Q}(z)$ be a rational map of degree $d$, and consider a transformation $A\colon z \mapsto \frac{rz+s}{tz+u} \in \mathrm{PGL}_2(\mathbb{Q})$ with $ru - st \neq 0$. We write $\phi^A$ to mean conjugation of $\phi$ by $A$, namely $A^{-1} \circ \phi \circ A$. Thus we have

$$A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

and

$$A^{-1} = \frac{1}{ru - st} \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$$

so

$$(A^{-1}\circ\phi\circ A)(z)=\frac{1}{ru-st}\cdot\frac{uF(\frac{rz+s}{tz+u})-sG(\frac{rz+s}{tz+u})}{-tF(\frac{rz+s}{tz+u})+rG(\frac{rz+s}{tz+u})}.$$

Hence, if $[F,G]$ is a normalized representation of $\phi$, we have new polynomials $F_A, G_A \in \mathbb{Q}[z]$ given by

$$F_A(z)=uF\left(\left(\frac{rz+s}{tz+u}\right)\right)-sG\left(\left(\frac{rz+s}{tz+u}\right)\right) \text{ and}$$
$$G_A(z)=-tF\left(\left(\frac{rz+s}{tz+u}\right)\right)+rG\left(\left(\frac{rz+s}{tz+u}\right)\right)$$

such that $\phi^A = F_A/G_A$. We may compute the $d$-form resultant,

$$\begin{aligned}
&\mathrm{Res}_d(F_A,G_A)\\
&=\mathrm{Res}_d\left(uF\left(\frac{rz+s}{tz+u}\right)-sG\left(\frac{rz+s}{tz+u}\right),rG\left(\frac{rz+s}{tz+u}\right)-tF\left(\frac{rz+s}{tz+u}\right)\right)\\
&=(sr)^d\mathrm{Res}_d\left(\frac{u}{s}F\left(\frac{rz+s}{tz+u}\right)-G\left(\frac{rz+s}{tz+u}\right),G\left(\frac{rz+s}{tz+u}\right)-\frac{t}{r}F\left(\frac{rz+s}{tz+u}\right)\right)\\
&=(sr)^d\mathrm{Res}_d\left(\left(\frac{u}{s}-\frac{t}{r}\right)F\left(\frac{rz+s}{tz+u}\right),G\left(\frac{rz+s}{tz+u}\right)-\frac{t}{r}F\left(\frac{rz+s}{tz+u}\right)\right)\\
&=\mathrm{Res}_d\left((ur-ts)F\left(\frac{rz+s}{tz+u}\right),G\left(\frac{rz+s}{tz+u}\right)-\frac{t}{r}F\left(\frac{rz+s}{tz+u}\right)\right)\\
&=(ur-ts)^d\mathrm{Res}_d\left(F\left(\frac{rz+s}{tz+u}\right),G\left(\frac{rz+s}{tz+u}\right)-\frac{t}{r}F\left(\frac{rz+s}{tz+u}\right)\right)\\
&=(ur-ts)^d\mathrm{Res}_d\left(F\left(\frac{rz+s}{tz+u}\right),G\left(\frac{rz+s}{tz+u}\right)\right), \qquad (3.1)
\end{aligned}$$

where we repeatedly used part (a) of Proposition 2.2.18. To simplify this even further, if we have a root of $F(\frac{rz+s}{tz+u})$, say $h_1$, and a root of $G(\frac{rz+s}{tz+u})$, say $h_2$, we have

$$\begin{aligned}
\frac{h_2r+s}{h_2t+u}-\frac{h_1r+s}{h_1t+u}&=(h_2r+s)(h_1t+u)-(h_1r+s)(h_2t+u)\\
&=h_1h_2rt+h_2ru+h_1st+su-h_1h_2rt-h_1ru-h_2st-su\\
&=(h_2-h_1)ru+(h_1-h_2)st\\
&=(h_2-h_1)(ru-st).
\end{aligned}$$

Using Proposition 2.2.18 part (c) combined with Lemma 2.2.16, this implies

$$\mathrm{Res}_d\left(F\left(\frac{rz+s}{tz+u}\right), G\left(\frac{rz+s}{tz+u}\right)\right) = (ru-st)^{d^2}\mathrm{Res}_d(F(z),G(z))$$

so combining this with (3.1) gives

$$\mathrm{Res}_d(F_A, G_A) = (ru-st)^{d^2+d}\mathrm{Res}_d(F(z),G(z)). \tag{3.2}$$

Note that $F_A$ and $G_A$ may not form a normalized representation of $\phi^A$. In order to compute $\mathrm{Res}(\phi^A)$ we need to study the effect of normalization.

**Proposition 3.1.1** (Proposition 4.95 in [8]). *Let $\phi = F/G \in \mathbb{Q}(z)$ be a rational map of degree $d$ with $[F,G]$ a normalized representation, and let $A \in \mathrm{PGL}_2(\mathbb{Q})$. Then*

$$\mathrm{ord}_p(\mathrm{Res}(\phi^A)) = (d^2+d)\mathrm{ord}_p(\det A) - 2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) + \mathrm{ord}_p(\mathrm{Res}(\phi))$$

*Proof.* Note that if $\lambda \in \mathbb{Q}$ and $F \in \mathbb{Q}[z]$ then $\mathrm{ord}_p(\lambda F) = \mathrm{ord}_p(\lambda) + \mathrm{ord}_p(F)$. Recall from Definition 2.2.12 that if $[F,G]$ is a normalized representation of $\phi$ at $p$, then $\min(\mathrm{ord}_p(F), \mathrm{ord}_p(G)) = 0$. Therefore if we define

$$\lambda = \lambda(F_A, G_A) = p^{-\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A))},$$

we have that, $[\lambda F_A, \lambda G_A]$ is a normalized representation of $\phi^A$ at $p$. Hence

$$\begin{aligned}\mathrm{ord}_p(\mathrm{Res}(\phi^A)) &= \mathrm{ord}_p(\mathrm{Res}_d(\lambda F_A, \lambda G_A)) \\ &= \mathrm{ord}_p(\lambda^{2d}\mathrm{Res}_d(F_A, G_A)) \\ &= -2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) + \mathrm{ord}_p(\mathrm{Res}_d(F_A, G_A)).\end{aligned}$$

Thus from (3.2) we have

$$\mathrm{ord}_p(\mathrm{Res}(\phi^A)) = (d^2+d)\mathrm{ord}_p(\det A) - 2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) + \mathrm{ord}_p(\mathrm{Res}(\phi)),$$

as required. □

We ask what happens to the resultant when conjugating with a transformation in $\mathrm{PGL}_2(\mathbb{Z})$. We have the following,

**Theorem 3.1.2.** *Let $[F, G]$ be a normalized representation of a rational map $\phi \in \mathbb{Q}(z)$ of degree $d$, and let $A \in \mathrm{PGL}_2(\mathbb{Z})$. Then* $\mathrm{Res}(\phi^A) = \mathrm{Res}(\phi)$.

*Proof.* If $A \in \mathrm{PGL}_2(\mathbb{Z})$ then we can represent $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ with $r, s, t, u \in \mathbb{Z}$ and $ru - st = \pm 1$, so $A^{-1} = \pm \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$. For $F(z) = \sum_{i=0}^{d} f_i z^i$ and $G(z) = \sum_{i=0}^{d} g_i z^i$, we have

$$F_A(z) = uF(z_0) - sG(z_0)$$
$$G_A(z) = -tF(z_0) + rG(z_0)$$

where $z_0 = \frac{v}{w}$ with

$$\begin{pmatrix} v \\ w \end{pmatrix} = A \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} rz + s \\ tz + u \end{pmatrix}.$$

Write

$$F(z, y) = y^d F\left(\frac{z}{y}\right) = \sum f_i z^i y^{d-i}$$
$$G(z, y) = y^d G\left(\frac{z}{y}\right) = \sum g_i z^i y^{d-i}.$$

We have $\phi\left(\frac{z}{y}\right) = \frac{F(z,y)}{G(z,y)}$ and $\phi^A\left(\frac{z}{y}\right) = \frac{F_A(z,y)}{G_A(z,y)}$ where

$$F_A(z, y) = y^d F_A\left(\frac{z}{y}\right) = uF(z', y') - sG(z', y')$$
$$G_A(z, y) = y^d G_A\left(\frac{z}{y}\right) = -tF(z', y') + uG(z', y')$$

with

$$\begin{pmatrix} z' \\ y' \end{pmatrix} = A \begin{pmatrix} z \\ y \end{pmatrix} = \begin{pmatrix} rz + sy \\ tz + uy \end{pmatrix}.$$

Conversely,

$$F(z', y') = rF_A(z, y) + sG_A(z, y)$$
$$G(z', y') = tF_A(z, y) + uG_A(z, y).$$

If we let

$$\begin{pmatrix} z'' \\ y'' \end{pmatrix} = A^{-1} \begin{pmatrix} z \\ y \end{pmatrix} = \pm \begin{pmatrix} uz - sy \\ -tz + ry \end{pmatrix}.$$

We find

$$\begin{pmatrix} F(z,y) \\ G(z,y) \end{pmatrix} = A \begin{pmatrix} F_A(z'',y'') \\ G_A(z'',y'') \end{pmatrix}.$$

If all the coefficients of $F_A$ and $G_A$ are divisible by some prime $p$, then so are the coefficients of $F$ and $G$. However, we assumed that $[F,G]$ is a normalized representation, so no such $p$ exists. Hence from Proposition 3.1.1 we have

$$\begin{aligned} \mathrm{ord}_p(\mathrm{Res}(\phi^A)) &= (d^2+d)\mathrm{ord}_p(ru-st) - 2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) + \mathrm{ord}_p(\mathrm{Res}(\phi)) \\ &= -2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) + \mathrm{ord}_p(\mathrm{Res}(\phi)) \\ &= \mathrm{ord}_p(\mathrm{Res}(\phi)) \end{aligned}$$

for all primes, and hence $\mathrm{Res}(\phi^A) = \mathrm{Res}(\phi)$. □

*Remark.* Note that the proof of Theorem 3.1.2 yields a bit more. If we have a linear transformation $A \in \mathrm{PGL}_2(\mathbb{Q})$ represented by a matrix $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ such that $\mathrm{ord}_q(r), \ldots, \mathrm{ord}_q(u) \geq 0$ and $\mathrm{ord}_q(ru-st) = 0$ for some prime $q$, then $\mathrm{ord}_q(\mathrm{Res}(\phi^A)) = \mathrm{ord}_q(\mathrm{Res}(\phi))$.

We are now able to show that affine minimality implies $\mathrm{PGL}_2(\mathbb{Q})$-minimality.

**Theorem 3.1.3.** *Let $\phi \in \mathbb{Q}(z)$ be a rational map. If $\phi$ is affine minimal, then $\phi$ is $\mathrm{PGL}_2(\mathbb{Q})$-minimal.*

*Proof.* Our strategy is as follows. We claim that for any $B \in \mathrm{PGL}_2(\mathbb{Q})$ there exists $A \in \mathrm{Aff}_2(\mathbb{Q})$ and $C \in \mathrm{PGL}_2(\mathbb{Z})$ such that $A = BC$. Next we see if $\psi = \phi^B$ then $\psi^C = \phi^{BC} = \phi^A$. By Theorem 3.1.2, we know that $\mathrm{Res}(\psi) = \mathrm{Res}(\psi^C)$, so any change in resultant by $B \in \mathrm{PGL}_2(\mathbb{Q})$ can also be made by an appropriate $A \in \mathrm{Aff}_2(\mathbb{Q})$. This establishes the theorem. We now prove our claim. Let $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Q})$.

Write

$$A = \begin{pmatrix} f & g \\ 0 & 1 \end{pmatrix}$$
$$C = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

where $f, g \in \mathbb{Q}$, $r, s, t, u \in \mathbb{Z}$ and $ru - st = \pm 1$. We want to have $A = BC$. To this end, we compute the product $BC$,

$$\begin{aligned} BC &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \\ &= \begin{pmatrix} ar + bt & as + bu \\ cr + dt & cs + du \end{pmatrix}. \end{aligned}$$

If we want $A = BC$, we must have $cr + dt = 0$. We know, for some $\lambda \in \mathbb{Q}$, we have that $c' = \frac{c}{\lambda}$, $d' = \frac{d}{\lambda}$ are integers with $\gcd(c', d') = 1$. Pick $r = -d'$ and $t = c'$ so that

$$\begin{aligned} BC &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -d' & s \\ c' & u \end{pmatrix} \\ &= \begin{pmatrix} -ad' + bc' & as + bu \\ -cd' + dc' & cs + du \end{pmatrix} \\ &= \begin{pmatrix} -ad' + bc' & as + bu \\ \frac{-cd+dc}{\lambda} & cs + du \end{pmatrix} \\ &= \begin{pmatrix} -ad' + bc' & as + bu \\ 0 & cs + du \end{pmatrix} \end{aligned}$$

We need to ensure $ru - st = \pm 1$ since we want $C \in \mathrm{PGL}_2(\mathbb{Z})$. Fortunately, this is not too difficult. As $\gcd(c', d') = 1$, we know there are integers $v, w$ such that $vc' + wd' = 1$, so if we take $s = v$ and $u = w$ then

$$C = \begin{pmatrix} -d' & v \\ c' & w \end{pmatrix}$$

satisfies $A = BC$. Since $\det C = -d'w - cv = -1$, we have $C \in \mathrm{PGL}_2(\mathbb{Z})$, which proves the claim. $\square$

Given this, we disregard the word affine when showing a map has minimal resultant among its affine conjugates. We simply say it is minimal. Given the two concepts are equivalent, with the goal of building an algorithm to compute minimal representations of rational maps, we wish to use only affine transformations, as the computations will be far simpler. In particular, if $A\colon z \mapsto az+b \in \mathrm{Aff}_2(\mathbb{Q})$, we have the following simplifications,

$$\begin{aligned} F_A &= F(az+b) - bG(az+b) \\ G_A &= aG(az+b) \end{aligned}$$

where $\phi^A = F_A/G_A$ and

$$\mathrm{Res}(\phi^A) = (d^2+d)\mathrm{ord}_p(a) - 2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}(G_A)) + \mathrm{Res}(\phi).$$

With these in hand, we now wish to study minimality in depth.

## 3.2 Minimality

In order to test Silverman's conjecture we need to be able to recognize when a function is minimal. This is not completely straightforward. Consider the following three maps,

$$\begin{aligned} \phi_1(z) &= \frac{245z^2 - 540z - 299}{3z^2 + 98z - 299}, \\ \phi_2(z) &= \frac{367z^2 - 15104z + 143325}{12z^2 - 469z - 4095}, \text{ and} \\ \phi_3(z) &= \frac{86z^2 - 1068z - 338}{z^2 + 7z - 338}. \end{aligned}$$

In order to check minimality for any of these maps straight from the definition, one would need to compute the resultants for all affine conjugates and see if any are smaller. This is not a finite procedure.

We need to develop more theory for minimality and the effects of conjugation. As a start, we prove that being minimal at $p$ for all primes $p$ minimality. The converse is also true, however we will need some theory from Section 3.3 to show this. We relegate the proof to Proposition 3.3.7.

**Proposition 3.2.1.** *Let $\phi \in \mathbb{Q}(z)$ be a rational map. Then $\phi$ is minimal only if it is minimal at $p$ for every prime $p$.*

*Proof.* Assume $\phi$ is minimal at $p$ for every prime $p$. If $\phi$ were not minimal, there would be some affine transformation $A\colon z \mapsto az+b$ with $a, b \in \mathbb{Q}$ such that $\mathrm{Res}(\phi^A) < \mathrm{Res}(\phi)$. Then there must be some prime $p$ so that

$$\mathrm{ord}_p(\mathrm{Res}(\phi^A)) < \mathrm{ord}_p(\mathrm{Res}(\phi)).$$

But this implies $\phi$ is not minimal at $p$, a contradiction. Hence a rational map is minimal if and only if it is minimal at every prime. □

It is worth reflecting a little more on Proposition 3.1.1, since it allows us to conclude minimality for many rational maps. For example, let $F(z) = z^2 + 1$ and $G(z) = z^2 + z$ and consider the map $\psi = F/G$, where $[F, G]$ is certainly a normalized representation. We can compute the resultant to find $\mathrm{Res}(\psi) = 2$. Before Proposition 3.1.1 we mentioned the definition did not immediately suggest a finite approach to showing this map to be minimal or not. Let us investigate what Proposition 3.1.1 tells us. For any affine transformation $B\colon z \mapsto az + b$, with $a, b \in \mathbb{Q}$ and $a \neq 0$, we have

$$\mathrm{ord}_2(\mathrm{Res}(\psi^B)) = -2d\min(\mathrm{ord}_2(F_B), \mathrm{ord}_2(G_B)) + (d^2 + d)\mathrm{ord}_2(a) + \mathrm{ord}_2(\mathrm{Res}(\psi)).$$

We know $d = 2$ as well, hence as $\mathrm{ord}_2(\mathrm{Res}(\psi)) = 1$, we have

$$\mathrm{ord}_2(\mathrm{Res}(\psi^B)) = -4\lambda + 6\mathrm{ord}_2(a) + 1.$$

for some integer $\lambda$. Any resultant of a rational map must be a positive integer, so the order of the resultant of $\psi^B$ at 2 can not be less than 1. If $B$ reduces the resultant of $\psi$ we would have a solution to the equation $-4\lambda + 6\mathrm{ord}_p(a) = -1$, of which none exist. Hence as $\psi$ is minimal at every other prime, we have that $\psi$ is minimal. In a similar manner, consider the rational map

$$\tau(z) = \frac{z^2 + 1}{z^2 - 13z},$$

with resultant $\mathrm{Res}(\tau) = 2 \cdot 85$. The map $\tau$ is minimal at 2 as well, and at 85, so as above, we know $\tau$ is minimal at every prime, and so $\tau$ is minimal. In general we have the following.

**Theorem 3.2.2.** *Let $\phi \in \mathbb{Q}(z)$ be a rational map with degree $d \geq 2$. Furthermore, let $g = d$ if $d$ is even and $g = 2d$ if $d$ is odd. If the resultant $\mathrm{Res}(\phi)$ is $g$-th power free, then $\phi$ is minimal.*

*Proof.* Suppose the resultant is $g$-th power free and factors into the product of distinct prime powers
$\mathrm{Res}(\phi) = p_1^{n_1} \cdot p_2^{n_2} \cdots p_r^{n_r}$. For each $i$, $1 \leq i \leq r$ we know from Proposition 3.1.1, if a transformation $A\colon z \mapsto az + b \in \mathbb{Q}[z]$, with $\mathrm{ord}_p(a) = k$ reduces the resultant of $\phi$, then we have a solution to the Diophantine equation

$$-2d\lambda + (d^2 + d)k = c, \tag{3.3}$$

where $\lambda$ is an integer and $c$ is a negative integer of magnitude at most $g$, since $\mathrm{Res}(\phi)$ is $g$-th power free. Note that $g = \gcd(d^2 + d, 2d) = d\gcd(d + 1, 2)$. If $d$ is even, we can write $d = 2m$ for some integer $m$, and we have

$$d\gcd(2m + 1, 2) = d.$$

If $d$ is odd, we write $d = 2m + 1$ so that

$$\begin{aligned} d\gcd(2m + 2, 2) &= 2d\gcd(m + 1, 1) \\ &= 2d. \end{aligned}$$

Thus with our choice of $g$, we can see no such solution exists for (3.3), and hence no choice of $k$ and $b$ can make $\mathrm{ord}_{p_i}(\mathrm{Res}(\phi^A)) < \mathrm{ord}_{p_i}(\mathrm{Res}(\phi))$. Thus $\phi$ is minimal. □

From Proposition 3.1.1, in order for $A\colon z \mapsto az + b \in \mathrm{Aff}_2(\mathbb{Q})$ to be a transformation that reduces the valuation of the resultant of $\phi$ at some prime $p$, we require

$$-2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) + (d^2 + d)\mathrm{ord}_p(a) < 0.$$

In other words, if $A$ reduces the valuation of the resultant, we have

$$\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) > \frac{d + 1}{2}\mathrm{ord}_p(a). \tag{3.4}$$

Recall the valuation of a polynomial is the minimal valuation of its coefficients, and we know the coefficients of $F_A$ and $G_A$, in terms of the coefficients of $F_\phi$ and $G_\phi$. We focus

first on $G_A$ then $F_A$. Denote the degree of $G_\phi$ by $d_G$ and write $G_\phi(z) = \sum_{i=0}^{d_G} g_i z^i$. Furthermore, we set $g_{d_G+1} = \ldots = g_d = 0$. Writing

$$G_A(z) = aG_\phi(az+b) = \sum_{i=0}^{d_G} h_i z^i,$$

we have

$$h_j = a^{j+1} \sum_{i=j}^{d_G} \binom{i}{j} g_i b^{i-j}. \tag{3.5}$$

In particular, we have

$$\begin{aligned} h_0 &= aG_\phi(b) \\ h_1 &= a^2 G'_\phi(b) \\ h_{d_G} &= a^{d_G+1} g_{d_G} \end{aligned}$$

and if (3.4) is satisfied, we must have

$$\begin{aligned} \mathrm{ord}_p(a) + \mathrm{ord}_p(G_\phi(b)) &> \frac{d+1}{2}\mathrm{ord}_p(a), \\ 2\mathrm{ord}_p(a) + \mathrm{ord}_p(G'_\phi(b)) &> \frac{d+1}{2}\mathrm{ord}_p(a), \\ &\vdots \\ (d_G+1)\mathrm{ord}_p(a) + \mathrm{ord}_p(g_{d_G}) &> \frac{d+1}{2}\mathrm{ord}_p(a). \end{aligned} \tag{3.6}$$

Focusing on the numerator, we let $F_\phi(z) = \sum_{i=0}^{d} f_i z^d$ where if the degree of $F_\phi$ is less than $d$ we let the respective coefficients be 0. Writing

$$F_A(z) = F_\phi(az+b) - bG_\phi(az+b) = \sum_{i=0}^{d} r_i z^i$$

we have

$$r_j = a^j \sum_{i=j}^{d} \binom{i}{j} (f_i b^{i-j} - g_i b^{i-j+1}) \tag{3.7}$$

and again, if (3.4) holds we must have

$$\begin{aligned} \operatorname{ord}_p(F_\phi(b) - bG_\phi(b)) &> \frac{d+1}{2}\operatorname{ord}_p(a), \\ \operatorname{ord}_p(a) + \operatorname{ord}_p(F'_\phi(b) - bG'_\phi(b)) &> \frac{d+1}{2}\operatorname{ord}_p(a), \\ &\vdots \\ d\operatorname{ord}_p(a) + \operatorname{ord}_p(f_d - bg_d) &> \frac{d+1}{2}\operatorname{ord}_p(a), \end{aligned} \tag{3.8}$$

where at most one of $f_d$ and $g_d$ can be zero (as $\phi$ has degree $d$). These inequalities, which we shall refer to as the *coefficient inequalities*, are necessary and sufficient conditions for the transformation $A$ to reduce the resultant of $\phi$ at $p$. If no choices of $a$ and $b$ can satisfy the inequalities, then $\phi$ is minimal at $p$. With these in hand, we are now able to develop our algorithm.

## 3.3 Algorithm

Given a rational map $\phi \in \mathbb{Q}(z)$, we would like to know if it is minimal. If not, we would like a rational map $\psi \in \mathbb{Q}(z)$ such that $\psi$ is minimal and there exists some affine transformation $A \in \mathrm{Aff}_2(\mathbb{Q})$ with $\psi^A = \phi$. We develop an algorithm to do this in this section, with the following main steps.

- Note that $\mathrm{Res}(\phi)$ has only finitely many prime divisors. If $p \nmid \mathrm{Res}(\phi)$, then $\phi$ is automatically minimal at $p$.

- Let $a, b \in \mathbb{Q}$, $a \neq 0$ and let $p$ be a prime. We observe that if conjugating by $z \mapsto az+b$ reduces the resultant of $\phi$, with $\operatorname{ord}_p(a) = k$, then so does conjugating by $z \mapsto p^k z + b$. We find finite bounds for values of $k$ that can possibly reduce $\mathrm{Res}(\phi)$.

- For each possible $k$, we determine $b$ satisfying (3.6) and (3.8) or prove that none exists.

The rest of this section explains the approach in detail and proves it valid. First, we fix some notation for the rest of the section. Let $[F, G]$ be a normalized representation of $\phi \in \mathbb{Q}(z)$, a rational map of degree $d \geq 2$. Further, let $A \in \mathrm{Aff}_2(\mathbb{Q})$

**Lemma 3.3.1.** *Let $\phi \in \mathbb{Q}(z)$ be a rational function, let $p$ be a prime and let $a \in \mathbb{Q}^\times, b \in \mathbb{Q}$ with $\mathrm{ord}_p(a) = k$. Let $A\colon z \mapsto az + b$ and $B\colon z \mapsto p^k z + b$. Then $\mathrm{ord}_p(\mathrm{Res}(\phi^A)) = \mathrm{ord}_p(\mathrm{Res}(\phi^B))$.*

*Proof.* From Proposition 3.1.1 we have

$$\mathrm{ord}_p(\mathrm{Res}(\phi^A)) = -2d\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) + (d^2+d)k + \mathrm{ord}_p(\mathrm{Res}(\phi))$$
$$\mathrm{ord}_p(\mathrm{Res}(\phi^B)) = -2d\min(\mathrm{ord}_p(F_B), \mathrm{ord}_p(G_B)) + (d^2+d)k + \mathrm{ord}_p(\mathrm{Res}(\phi))$$

so what we must show is, $\min(\mathrm{ord}_p(F_A), \mathrm{ord}_p(G_A)) = \min(\mathrm{ord}_p(F_B), \mathrm{ord}_p(G_B))$. This comes straight from (3.5) and (3.7), where we can see the respective coefficients of $G_A$ and $G_B$ have the same order, as well as the respective coefficients of $F_A$ and $F_B$. Hence $\mathrm{ord}_p(\mathrm{Res}(\phi^A)) = \mathrm{ord}_p(\mathrm{Res}(\phi^B))$. □

Write $F = f_0 + f_1 z + \ldots + f_d z^d$ and $G = g_0 + g_1 z + \ldots + g_{d_G} z^{d_G}$ where $d_G \leq d$ is the degree of $G$. We are able to find bounds on the values of $k$ that may lead to $\mathrm{ord}_p(\mathrm{Res}(\phi^A)) < \mathrm{ord}_p(\mathrm{Res}(\phi))$.

**Theorem 3.3.2.** *Suppose $\phi \in \mathbb{Q}(z)$ and $A \in \mathrm{Aff}_2(\mathbb{Q})$ such that $\mathrm{ord}_p(\mathrm{Res}(\phi^A)) < \mathrm{ord}_p(\mathrm{Res}(\phi))$. If $d_G > (d+1)/2$ then $k > -\frac{2}{2d_G - d + 1}\mathrm{ord}_p(g_{d_G})$, otherwise if $d_G \leq (d+1)/2$ we have $k > -\frac{2}{d+1}\mathrm{ord}_p(f_d)$.*

*Proof.* We have two cases to consider depending on the degree of $G$. If $d_G > (d+1)/2$, from the last coefficient inequality in (3.6) we have

$$\frac{2d_G - d + 1}{2}\mathrm{ord}_p(a) > -\mathrm{ord}_p(g_{d_G}),$$

and so

$$\mathrm{ord}_p(a) > -\frac{2}{2d_G - d + 1}\mathrm{ord}_p(g_{d_G}).$$

Otherwise, we must have that $d_G \leq (d+1)/2$, so in particular the coefficient $g_d$ of $G$ must be 0. We appeal to the last coefficient inequality in (3.8) to see

$$\frac{d-1}{2}\mathrm{ord}_p(a) > -\mathrm{ord}_p(f_d),$$

and rearranging gives

$$\mathrm{ord}_p(a) > -\frac{2}{d-1}\mathrm{ord}_p(f_d).$$

Notice in the respective cases, $g_{d_G}$ and $f_d$ must be non-zero, so their respective orders are always well defined finite values. □

We now look for an upper bound.

**Theorem 3.3.3.** *Suppose $\phi \in \mathbb{Q}(z)$ and $A\colon z \mapsto p^k z + b \in \mathrm{Aff}_2(\mathbb{Q})$ such that $\mathrm{ord}_p(\mathrm{Res}(\phi^A)) < \mathrm{ord}_p(\mathrm{Res}(\phi))$. Then there is an explicitly computable upper bound for $k$, depending only on $\phi$.*

*Proof.* Recall the inequalities from (3.6) and (3.8) have the form

$$\mathrm{ord}_p(c(b)) > \alpha k$$

for some polynomial $c(b)$ and rational number $\alpha$. We will select two of these inequalities

$$\mathrm{ord}_p(c_1(b)) > \alpha_1 k$$
$$\mathrm{ord}_p(c_2(b)) > \alpha_2 k$$

such that $\mathrm{Res}_m(c_1, c_2) \neq 0$ where $m = \max(\deg c_1, \deg c_2)$. For instance, from the inequalities (3.5) and (3.7), we can take

$$\mathrm{ord}_p(F_\phi - bG_\phi) > \frac{d+1}{2}k$$
$$\mathrm{ord}_p(G_\phi) > \frac{d-1}{2}k$$

where $Res_m(c_1, c_2) \neq 0$ follows from the fact that $F, G$ are coprime by assumption and hence $F(b) - bG(b), G(b)$ are as well. If we can find an upper bound for $\mathrm{ord}_p(c_1(b))$ or $\mathrm{ord}_p(c_2(b))$ we can find an upper bound for $k$. We have two cases to consider, since the values we plug in to $c_1$ and $c_2$ may have positive or negative valuation. If we plug in some value $b_0 \in \mathbb{Q}$ with $\mathrm{ord}_p(b_0) < 0$, we recall Proposition 2.2.18 part (d). Namely, there exist polynomials $R, S \in \mathbb{Z}[b]$ such that

$$Rc_1 + Sc_2 = b_0^{2m-1}\mathrm{Res}_m(c_1, c_2).$$

Write $R(b) = R_0 + R_1 b + \ldots + R_m b^m$ and $S(b) = S_0 + S_1 b + \ldots + S_m b^m$. Taking the valuation of both sides, we use the non-Archimedean triangle inequality to find

$$\begin{aligned}
\mathrm{ord}_p(b_0^{2m-1}\mathrm{Res}_m(c_1,c_2)) &= \mathrm{ord}_p(R(b_0)c_1(b_0) + S(b_0)c_2(b_0)) \\
&= \mathrm{ord}_p\left(\left(c_1(b_0)\sum_i R_i b_0^i\right) + \left(c_2(b_0)\sum_j S_j b_0^j\right)\right) \\
&\geq \mathrm{ord}_p(c_1(b_0)b_0^{m-1} + c_2(b_0)b_0^{m-1}) \\
&\geq \min(\mathrm{ord}_p(c_1(b_0)b_0^{m-1}), \mathrm{ord}_p(c_2(b_0)b_0^{m-1})) \\
&\geq (m-1)\mathrm{ord}_p(b_0) + \min(\mathrm{ord}_p(c_1(b_0)), \mathrm{ord}_p(c_2(b_0))).
\end{aligned}$$

We may write

$$\min(\mathrm{ord}_p(c_1(b_0)), \mathrm{ord}_p(c_2(b_0))) \leq m\,\mathrm{ord}_p(b_0) + \mathrm{ord}_p(\mathrm{Res}_m(c_1,c_2))$$

and so,

$$k < \frac{\min(\mathrm{ord}_p(c_1(b)), \mathrm{ord}_p(c_2(b)))}{\min(\alpha_1,\alpha_2)}$$

hence

$$\begin{aligned}
k &< \frac{m\,\mathrm{ord}_p(b_0) + \mathrm{ord}_p(\mathrm{Res}_m(c_1,c_2))}{\min(\alpha_1,\alpha_2)} \\
&< \frac{\mathrm{ord}_p(\mathrm{Res}_m(c_1,c_2))}{\min(\alpha_1,\alpha_2)},
\end{aligned}$$

as $\mathrm{ord}_p(b_0) < 0$. On the other hand, if we plug in some value $b_1 \in \mathbb{Q}$ with $\mathrm{ord}_p(b_1) \geq 0$, we recall part (e) of Proposition 2.2.18 to find polynomials $C, D \in \mathbb{Z}[b]$, such that

$$Cc_1 + Dc_2 = \mathrm{Res}_m(c_1,c_2).$$

With the similar process, we take valuations and find

$$\min(\mathrm{ord}_p(c_1(b_1)), \mathrm{ord}_p(c_2(b_1))) \leq \mathrm{ord}_p(\mathrm{Res}_m(c_1,c_2))$$

and hence

$$k < \mathrm{ord}_p(\mathrm{Res}_m(c_1,c_2))/\min(\alpha_1,\alpha_2).$$

□

Thus if the algorithm searches values of $k$ starting from the lower bound and increments until the upper bound, we have searched all the necessary values of $k$.

**Example 3.3.4.** Recall $\phi_3$ from the beginning of Section 3.2,

$$\phi_3(z) = \frac{86z^2 - 1068z - 338}{z^2 + 7z - 338}.$$

For a fixed prime $p$, integer $k$ and rational number $b$, we want to investigate the effect of conjugating $\phi_3$ by the affine transformation $A\colon z \mapsto p^k z + b$. Conjugating $\phi_3$ by $A$ gives

$$\phi_3^A(z) = \frac{(-b+344)p^{2k}z^2 + (-2b^2+165b-1068)p^k z - b^3 + 79b^2 - 730b - 338}{p^{3k}z^2 + (2b+7)p^{2k}z + p^k(b^2+7b-338)}.$$

We can see $\mathrm{Res}(\phi_3) = 2^5 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13^2$. If we focus on the prime $p = 2$, Theorems 3.3.2 and 3.3.3 tell us we must have $k < \mathrm{ord}_p(\mathrm{Res}_m(c_1, c_2))/\max(\alpha_1, \alpha_2)$ where we may pick

$$\begin{aligned} c_1 &= F'(b) - bG'(b) = -2b^2 + 165b - 1068 \\ c_2 &= G(b) = b^2 + 7b - 338 \end{aligned}$$

while $\alpha_1 = \alpha_2 = 1/2$ and $m = 2$. Hence with

$$\mathrm{res}(c_1, c_2) = 2 \cdot 5 \cdot 29 \cdot 139^2$$

we have $\mathrm{ord}_2(\mathrm{Res}_2(c_1, c_2)) = 1$, and so $0 < k < 2$.

Continuing with the development of our algorithm, with fixed values of $k$, we need to see what effects $b$ can have on the order of the coefficients of $\phi^A$ at $p$. We will proceed as follows,

- We will compute a lower bound, $\ell$, on the valuation of $b$, and consider $b' = p^{-\ell}b$ with $b' \in \mathbb{Z}_p$.

- We prove that having $b' \in \mathbb{Z}$ gives us a finite procedure for determining if $\mathrm{ord}_p(\mathrm{Res}(\phi^A)) < \mathrm{ord}_p(\mathrm{Res}(\phi))$ for some $A \in \mathrm{Aff}_2(\mathbb{Q})$.

**Theorem 3.3.5.** *Let $\phi \in \mathbb{Q}(z)$ be a rational map of degree $d$, and $A\colon z \mapsto az+b$ an affine transformation. Write the coefficients of $\phi^A$ (both $F_A$ and $G_A$) as $c_i(b) = c_{i,0} + c_{i,1}b + \ldots + c_{i,d_i}b^{d_i}$. If $\mathrm{Res}(\phi^A) < \mathrm{Res}(\phi)$, then*

$$\mathrm{ord}_p(b) \geq \max_{c_i}\left(\min\left\{\frac{\alpha - \mathrm{ord}_p(c_{i,d_i})}{d_i}, \min_{0\leq j<d_i}\left(\frac{\mathrm{ord}_p(c_{i,j}) - \mathrm{ord}_p(c_{i,d_i})}{d_i - j}\right)\right\}\right),$$

*where $\alpha = (d+1)\mathrm{ord}_p(a)/2$.*

*Proof.* Pick any coefficient inequality. The inequality has the form

$$\mathrm{ord}_p(c_i(b)) > \alpha. \tag{3.9}$$

With $\deg(c_i) = d_i$, we try bounding the valuation of $b$ below, by observing that if $\mathrm{ord}_p(b)$ is sufficiently small, then $\mathrm{ord}_p(c_i(b)) = \mathrm{ord}_p(c_{i,d_i}b^{d_i})$ by the non-Archimedean triangle inequality. Thus, assume $\mathrm{ord}_p(b)$ is small enough so that $\mathrm{ord}_p(c_{i,d_i}b^{d_i}) < \mathrm{ord}_p(c_{i,j}b^j)$ for all $j, 0 \leq j < d_i$. As $\mathrm{ord}_p(c_{i,d_i}b^{d_i}) < \mathrm{ord}_p(c_{i,j}b^j)$, simply by expanding, one gets

$$\mathrm{ord}(c_{i,d_i}) + d_i\mathrm{ord}_p(b) < \mathrm{ord}_p(c_{i,j}) + j\mathrm{ord}_p(b).$$

Rearranging, we have

$$\mathrm{ord}_p(b) < \frac{\mathrm{ord}_p(c_{i,j}) - \mathrm{ord}_p(c_{i,d_i})}{d_i - j}.$$

Going back to (3.9), we require $\mathrm{ord}_p(c_i(b)) > \alpha$. If $\mathrm{ord}_p(c_{i,d_i}b^{d_i}) \leq \alpha$, by the non-Archimedean triangle inequality, we would not be able to satisfy (3.9) and (3.10), so our choice of $b$ was too small, and any $b$ must have

$$\mathrm{ord}_p(b) \geq \frac{\mathrm{ord}_p(c_{i,j}) - \mathrm{ord}_p(c_{i,d_i})}{d_i - j}$$

for some $j, 0 \leq j < d$. On the other hand, if $\mathrm{ord}_p(c_{i,d_i}b^{d_i}) > \alpha$, the following inequality holds:

$$\mathrm{ord}_p(b) > \frac{\alpha - \mathrm{ord}_p(c_{i,d_i})}{d_i}.$$

Putting both together, and doing this for each coefficient, $c_i$, we must have

$$\mathrm{ord}_p(b) \geq \max_{i}\left(\min\left\{\frac{\alpha - \mathrm{ord}_p(c_{i,d_i})}{d_i}, \min_{0\leq j<d_i}\left(\frac{\mathrm{ord}_p(c_{i,j}) - \mathrm{ord}_p(c_{i,d_i})}{d_i - j}\right)\right\}\right).$$

□

We may always find a lower bound on the valuation of possible solutions, $b$, to the inequalities (3.6) and (3.8). Write the lower bound as $\ell$, then we may rewrite the inequalities, using $b' = p^{-\ell}b$, so that we may always have $\mathrm{ord}_p(b') \geq 0$. From here, we simply need to find if there exists a $b_0 \in \mathbb{Q}$, that satisfies the inequalities. After the following Lemma, we will see that we need only find such a $b_0 \in \mathbb{Z}$ (or that none exists.)

**Lemma 3.3.6.** *Let $f_1, \ldots, f_r \in \mathbb{Z}_p[x]$ and let $v_1, \ldots, v_r \in \mathbb{R}$. For any $\beta \in \mathbb{Z}_p$, we can determine if*

$$\beta \in \{b_0 \in \mathbb{Z}_p : \mathrm{ord}_p f_i(b_0) > v_i \text{ for each } i\}.$$

*simply by considering the congruence class of $\beta$ in $\mathbb{Z}_p/p^e\mathbb{Z}_p$, where $e$ is $\max_i(\lfloor v_i + 1 \rfloor)$.*

*Proof.* For notational purposes, write $g$ for one of the $f_i$, write

$$g(b) = g_0 + g_1 x + \ldots + g_{e-1}x^{e-1} + g_e x^e + \ldots$$

and let $\beta, \epsilon \in \mathbb{Z}_p$. Then we have

$$g(\beta + \epsilon) = g_0 + g_1(\beta + \epsilon) + g_2(\beta + \epsilon)^2 + \ldots$$

and

$$g(\beta) = g_0 + g_1\beta + g_2\beta^2 + \ldots$$

so that

$$\begin{aligned} g(\beta + \epsilon) - g(\beta) &= g_1\epsilon + g_2(2\beta\epsilon + \epsilon^2) + \ldots \\ &= \epsilon(g_1 + g_2(2\beta + \epsilon) + \ldots) \end{aligned}$$

and hence

$$\mathrm{ord}_p(g(\beta + \epsilon) - g(\beta)) \geq \mathrm{ord}_p(\epsilon).$$

Notice, if we have $\beta' \in \mathbb{Z}_p$, then $\beta$ and $\beta'$ have the same image in $\mathbb{Z}_p/p^e\mathbb{Z}_p$ if and only if $\mathrm{ord}_p(\beta' - \beta) \geq e$, in which case $\beta' = \beta + \epsilon$, with $\mathrm{ord}_p(\epsilon) \geq e$. Thus $\mathrm{ord}_p(g(\beta')) \geq e$ if and only if $\mathrm{ord}_p(g(\beta)) \geq e$. As $g$ was an arbitrary $f_i$, we are done. □

*Remark.* If we have some map $\phi \in \mathbb{Q}(z)$ that is not minimal at $p$, Lemma 3.3.6 states we may find an affine transformation of the form $A\colon z \mapsto p^k z + p^l b'$, for some $k, l, b' \in \mathbb{Z}$, such that $\mathrm{ord}_p(\mathrm{Res}(\phi^A)) < \mathrm{ord}_p(\mathrm{Res}(\phi))$. The transformation $A$ corresponds to the matrix

$$\begin{pmatrix} p^k & p^l b' \\ 0 & 1 \end{pmatrix},$$

hence from the remark after Theorem 3.1.2, the transformation $A$ does not affect the resultant at any prime $q \neq p$. Namely, we have $\mathrm{ord}_q(\mathrm{Res}(\phi^A)) = \mathrm{ord}_q(\mathrm{Res}(\phi))$ for all primes $q \neq p$. Thus we may attempt to minimize a rational map, focusing on each prime dividing the resultant, one at a time.

Given this, we may now show:

**Proposition 3.3.7.** *A map $\phi \in \mathbb{Q}(z)$ is minimal if and only if it is minimal at $p$ for all primes $p$.*

*Proof.* We already have Proposition 3.2.1, so all we need to show is that $\phi$ being minimal implies $\phi$ being minimal at $p$ for all primes $p$. But this follows straight from the remark. The remark tells us if we have a map that is not minimal at every prime $p$, then it is not minimal. □

For any particular $p$ and $k$, there is obviously a finite procedure to test whether the set

$$\{b_0 \in \mathbb{Z}_p : \mathrm{ord}_p f_i(b_0) > v_i \text{ for each } i\}$$

in Lemma 3.3.6 is non-empty: for each class of $\mathbb{Z}_p/p^e\mathbb{Z}_p$, pick a representative $b_0$ in $\mathbb{Z}_p$ and see if $b_0$ is in the set. This is a finite procedure, but inefficient if $p^e$ gets large, so we put in a little more work, taking more advantage of our $p$-adic setting.

We have an algorithm that, given $c(b) \in \mathbb{Z}_p[b]$, and $\alpha \in \mathbb{R}$, either finds a solution $b_0 \in \mathbb{Z}_p$ such that $\mathrm{ord}_p(b_0) > \alpha$ or proves such an element does not exist. The expected runtime of this algorithm, as a function of $p$, is $O(\log p)$.

We wish to consider some value $b' \in \mathbb{Z}_p$, say $b' = x_0 + x_1 p + x_2 p^2 + \ldots$ with each $x_i \in \{0, 1, \ldots, p-1\}$. If $b'$ satisfies the inequalities, then certainly $b_0 = x_0 + x_1 p +$

$x_2p^2 + \ldots + x_np^n$ with $n = \lfloor \alpha + 1 \rfloor$ satisfies the inequalities too, by Lemma 3.3.6. Suppose we have some $b_0 \in \mathbb{Z}_p$ such that $c(b_0) \equiv 0(\text{mod } p^n)$. Then $b_0$ is congruent to 0 modulo any smaller powers of $p$. Writing this out we have,

$$\begin{aligned}
c(x_0 + x_1p + x_2p^2 + \ldots + x_{n-1}p^{n-1} + x_np^n) &\equiv 0(\text{mod } p^{n+1}) \\
c(x_0 + x_1p + x_2p^2 + \ldots + x_{n-1}p^{n-1} + x_np^n) &\equiv 0(\text{mod } p^n) \\
&\vdots \\
c(x_0 + x_1p + x_2p^2 + \ldots + x_{n-1}p^{n-1} + x_np^n) &\equiv 0(\text{mod } p^3) \\
c(x_0 + x_1p + x_2p^2 + \ldots + x_{n-1}p^{n-1} + x_np^n) &\equiv 0(\text{mod } p^2) \\
c(x_0 + x_1p + x_2p^2 + \ldots + x_{n-1}p^{n-1} + x_np^n) &\equiv 0(\text{mod } p).
\end{aligned}$$

Canceling the obvious powers of $p$ on both sides gives,

$$\begin{aligned}
c(x_0 + x_1p + x_2p^2 + \ldots + x_{n-1}p^{n-1} + x_np^n) &\equiv 0(\text{mod } p^{n+1}) \\
c(x_0 + x_1p + x_2p^2 + \ldots + x_{n-1}p^{n-1}) &\equiv 0(\text{mod } p^n) \\
&\vdots \\
c(x_0 + x_1p + x_2p^2) &\equiv 0(\text{mod } p^3) \\
c(x_0 + x_1p) &\equiv 0(\text{mod } p^2) \\
c(x_0) &\equiv 0(\text{mod } p). \qquad (3.10)
\end{aligned}$$

Since $c(x_0) \equiv 0(\text{mod } p)$, writing $c(x_0 + x_1p) = c(x_0) + pc'$, where $c' \in \mathbb{Z}[b]$, we can see as $c(x_0 + x_1p) \equiv 0(\text{mod } p^2)$,

$$\frac{c(x_0 + x_1p)}{p} \equiv 0(\text{mod } p).$$

More generally, we may rewrite the $i$-th congruence of (3.10) as

$$c(x_0 + x_1p + \ldots + x_{i-1}p^{i-1}) = c(x_0 + x_1p + \ldots + x_{i-1}p^{i-2}) + p^{i-1}f$$

where $f \in \mathbb{Z}_p[b]$ is some polynomial. The right summand, $p^{i-1}f$ is certainly divisible by $p^{i-1}$. If the left summand, $c(x_0 + x_1p + \ldots + x_{i-1}p^{i-2})$ is congruent to 0 modulo

$p^{i-1}$, and hence divisible by $p^{i-1}$, we may rewrite the congruences as

$$\begin{aligned} c(x_0 + x_1 p + x_2 p^2 + \ldots + x_{n-1} p^{n-1} + x_n p^n)/p^n &\equiv 0 (\text{mod } p) \\ c(x_0 + x_1 p + x_2 p^2 + \ldots + x_{n-1} p^{n-1})/p^{n-1} &\equiv 0 (\text{mod } p) \\ &\vdots \\ c(x_0 + x_1 p + x_2 p^2)/p^2 &\equiv 0 (\text{mod } p) \\ c(x_0 + x_1 p)/p &\equiv 0 (\text{mod } p) \\ c(x_0) &\equiv 0 (\text{mod } p). \end{aligned}$$

Hence in trying to find a $b_0$ that is a solution to the inequality, we write out all of these congruences and search for each $x_i$ starting with $x_0$, then $x_1$ and going to $x_n$.

We can come across a set $\{x_0, x_1, \ldots, x_m\}$ with $m < n$ that does not extend to a solution and we must backtrack, and pick another choice of $x_0, \ldots, x_m$ to see if they extend to a solution to the inequalities. Given each congruence has a polynomial of finite degree on the left hand side, if no solution exists, the backtracking will be finite and this process will terminate in a finite amount of time.

Given the set of inequalities

$$\{\text{ord}_p(f_1(b)) \geq e_1, \ldots, \text{ord}_p(f_r(b)) \geq e_r\},$$

to decide whether the set is empty or not (i.e., to find a solution), using our algorithm, we have the following main steps:

- Remove common factors of $p$ in the coefficients of each $f_i$ and reduce $e_i$ correspondingly: $O(\sum_i \deg(f_i))$ ring operations.

- Determine reductions $g_1, \ldots, g_r$ of $f_1, \ldots, f_r \bmod p$: $O(1)$, we simply address the polynomials as elements in $\mathbb{F}_p$.

- Determine $g = \gcd(g_1, \ldots, g_r)$: $O(M(d+1)\log(d+1))$ ring operations, where $M(k)$ is the time is takes to multiply two degree $k$ polynomials (Theorem 11.5 in [10]). Naively we can use classical polynomial multiplication to have $M(k) = 2k^2$ arithmetic ring operations. Then determining $g$ is $O(2(d+1)^2 \log(d+1))$ ring operations.

- Determine roots of $g$ in $\mathbb{F}_p$: $O(\deg(g)^2 mL(m)L(\deg g)\log p)$ ring operations, where $m = \max e_i$, and $L(k) = \log k \log\log k$ (Pages 276-277 in[5]).

- For each root $b_0$ of $g$, repeat the procedure for

$$\{\mathrm{ord}_p(f_1(b_0 + pb)) \geq e_1, \ldots, \mathrm{ord}_p(f_r(b_0 + pb)) \geq e_r\}.$$

This procedure needs to go at most $\max(e_i)$ levels deep, so the number of times the procedure gets executed is at most

$$1 + \deg(g) + \deg(g)^2 + \ldots + \deg(g)^n$$

times. The run time on some simple small examples using this method may certainly be larger, but we note $\deg(f_i), d, \deg(g)$ and $e_i$ are of bounded size for maps of a bounded degree, whereas the primes dividing the resultant can grow arbitrarily. The only complexity involving $p$ in the algorithm being $O(\log p)$ instead of $O(p^e)$, and the fact that the number of times the loop will run is independent of $p$, allows this method to handle much larger primes, which will be very useful in Chapter 4.

Given this method, for a fixed $k$ we would like to know if there exists a solution to our inequalities (3.6) and (3.8),

$$\begin{aligned}
\mathrm{ord}_p(p^k G_\phi(b)) &> \frac{d+1}{2}k, \\
\mathrm{ord}_p(p^{2k} G'_\phi(b)) &> \frac{d+1}{2}k, \\
&\vdots \\
\mathrm{ord}_p(p^{(d_G+1)k} g_{d_G}) &> \frac{d+1}{2}k \\
\mathrm{ord}_p(F_\phi(b) - bG_\phi(b)) &> \frac{d+1}{2}k, \\
\mathrm{ord}_p(p^k(F'_\phi(b) - bG'_\phi(b))) &> \frac{d+1}{2}k, \\
&\vdots \\
\mathrm{ord}_p(p^{dk}(f_d - bg_d)) &> \frac{d+1}{2}k.
\end{aligned}$$

We do this by first seeing if the inequalities independent of $b$ are satisfied. If so, we scale the inequalities, to ensure the coefficients are integral, then reduce them modulo

$p$ and compute their greatest common divisor, $g$. We apply the above algorithm to determine a $b_0$ that satisfies $\text{ord}_p(g(b_0)) > \frac{d+1}{2}k$ if one exists, or determine no such $b_0$ exists. If such a $b_0$ is found, we conjugate the rational map and run the algorithm on the new map, otherwise increment $k$.

If we try every possible choice of $k$ and none of them leads to a solution, $b_0$, then our map is minimal at $p$. The resultant must strictly decrease after every conjugation and is always a positive number, hence this process must terminate.

**Example 3.3.8.** Returning to the rational map in Example 3.3.4, $\phi_3$, suppose we are interested in the case $p = 2$ and $k = 1$. Theorem 3.3.5 tells us $\text{ord}_p(b) \geq 0$ and we do not need to scale, so our inequalities are

$$\begin{aligned}
\text{ord}_2(2(b^2 + 7b - 338)) &> \frac{3}{2} \\
\text{ord}_2(2^2(2b + 7)) &> \frac{3}{2} \\
\text{ord}_2(2^3) &> \frac{3}{2} \\
\text{ord}_2(-b^3 + 79b^2 - 730b - 338) &> \frac{3}{2} \\
\text{ord}_2(2(-2b^2 + 165b - 1068)) &> \frac{3}{2} \\
\text{ord}_p(2^2(-b + 344)) &> \frac{3}{2}.
\end{aligned}$$

As the third inequality is satisfied, we look to the other five polynomials reduced modulo $p = 2$. We have that the greatest common divisor of the reduced non-constant polynomials is 1, and hence no value in $\mathbb{Q}$ can satisfy each inequality. With every possible choice of $p$ and $k$, we never find an affine transformation that reduces the resultant, hence $\phi_3$ is minimal.

We present pseudo code for an algorithm to determine minimal representations of rational functions in Appendix A.

## 3.4 Examples

First we show there are very simple minimal maps for any degree $d$ at least 2.

**Example 3.4.1.** Let $d \geq 2$ and consider $\phi(z) = \frac{z^d+1}{z}$. Then $\text{Res}(\phi) = 1$, and hence $\phi$ is minimal.

Also, we can have minimal maps with resultant $c$ for any positive integer $c$.

**Example 3.4.2.** Consider the polynomials $F_c(z) = z^3 + c$ for some positive $c \in \mathbb{Z}$ and $G(z) = z$. The rational map $\phi_c = F_c/G$ has normalized representation $[F_c, G]$, with resultant $c$. We will show that each of the $\phi_c$ are minimal, so in particular there exist minimal rational maps of arbitrary resultant.

*Proof.* From the last coefficient inequality in (3.6), in order for some affine transformation $A\colon z \mapsto az + b$ to reduce the resultant of $\phi_c$, we must have

$$2\text{ord}_p(a) > 2\text{ord}_p(a)$$

which is certainly not possible. □

There was no special importance to Example 3.4.2 being degree 3. The key to the last example was the denominator being $z$.

**Example 3.4.3** (Tom Boothby)**.** The rational map

$$\phi(z) = \frac{F(z)}{G(z)} = \frac{z^d + a_{d-1}z^{d-1} + \ldots + a_1 z + a_0}{z} \in \mathbb{Q}(z),$$

with $d \geq 3$, is minimal.

*Proof.* As with the last example, we look to the last coefficient inequality in (3.6). For any affine transformation $A\colon z \mapsto az+b$, if conjugating by $A$ gives a rational map with smaller resultant, we have

$$2\text{ord}_p(a) > \frac{d+1}{2}\text{ord}_p(a) \geq 2\text{ord}_p(a)$$

as $d \geq 3$. This is again, not possible. Hence $\phi$ is minimal. □

With a little work one can see that for $d = 2$ these maps do not have to be minimal. E.g.,

$$\phi(z) = \frac{F(z)}{G(z)} = \frac{z^2 + 24}{z}$$

has resultant $24 = 2^3 \cdot 3$ , which can be reduced by conjugating with $A\colon z \mapsto 2z$, to $6 = 2 \cdot 3$ as

$$\phi^A(z) = \frac{4z^2 + 24}{4z} = \frac{z^2 + 6}{z}.$$

We can generalize this further, continuing with our examples having monic denominator.

**Example 3.4.4.** If we write $\phi = F/G \in \mathbb{Q}(z)$ with $G$ monic, and $\deg(G) < \frac{1}{2}\deg(F)$. Then $\phi(z)$ is minimal.

*Proof.* For some affine transformation $A\colon z \mapsto az + b$, we again look to the last inequality in (3.6). As $\deg(G) < \frac{1}{2}\deg(F)$, we see

$$(\deg(G) + 1)\mathrm{ord}_p(a) > \frac{d+1}{2}\mathrm{ord}_p(a)$$

and hence, when $\mathrm{ord}_p(a) \neq 0$, in order to reduce the resultant of $\phi$ via conjugation by $A$, we must have

$$\deg(G) > \frac{d-1}{2} = \frac{d}{2} - \frac{1}{2} < \frac{d}{2} < \deg(G).$$

When $\mathrm{ord}_p(a) = 0$ in order to reduce the resultant by conjugation by $A$, we require $0 > 0$, which certainly cannot occur, so $\phi$ is minimal. □

This bound on the degree of $G$ is sharp. If we have monic polynomials with $\deg(G) \geq \frac{1}{2}\deg(F)$, minimality is no longer guaranteed. One can take $F(z) = z^3 - 5z^2 - 25z + 125$ and $G(z) = z^2 - 5z - 25$. Then $[F, G]$ is a normalized rational map, say $\psi$, with $\mathrm{Res}(\psi) = 15625 = 5^6$. Letting $A\colon z \mapsto 5z$ we have

$$\begin{aligned}\psi^A(z) &= \frac{(5z)^3 - 5(5z)^2 - 25(5z) + 125}{5((5z)^2 - 5(5z) - 25)} \\ &= \frac{z^3 - z^2 - z + 1}{z^2 - z - 1},\end{aligned}$$

which has the much smaller resultant 1.

# Chapter 4

# Integer Points in Orbits

## 4.1 Constructing a Rational Function with a Prescribed Orbit

Suppose we want to construct a degree $d$ rational map, with the orbit

$$\{c_1, c_2, \ldots, c_m, \ldots\}$$

for $c_1, c_2, \ldots, c_m \in \mathbb{Z}$. Writing the rational map

$$\phi(z) = (a_d z^d + \ldots + a_1 z + a_0)/(b_d z^d + \ldots + b_1 z + b_0)$$

with $a_0, a_1, \ldots, a_d, b_0, b_1, \ldots, b_d \in \mathbb{Z}$ we have the following equations

$$\begin{aligned}
\phi(c_1) &= \frac{a_d c_1^d + \ldots + a_1 c_1 + a_0}{b_d c_1^d + \ldots + b_1 c_1 + b_0} = c_2 \\
\phi(c_2) &= \frac{a_d c_2^d + \ldots + a_1 c_2 + a_0}{b_d c_2^d + \ldots + b_1 c_2 + b_0} = c_3 \\
&\vdots \\
\phi(c_{m-1}) &= \frac{a_d c_{m-1}^d + \ldots + a_1 c_{m-1} + a_0}{b_d c_{m-1}^d + \ldots + b_1 c_{m-1} + b_0} = c_m.
\end{aligned}$$

By rearranging each equation to be some expression equal to zero, we have

$$\begin{gathered}(a_d c_1^d + \ldots + a_1 c_1 + a_0) - (b_d c_1^d + \ldots + b_1 c_1 + b_0) c_2 = 0 \\ (a_d c_2^d + \ldots + a_1 c_2 + a_0) - (b_d c_2^d + \ldots + b_1 c_2 + b_0) c_3 = 0 \\ \vdots \\ (a_d c_{m-1}^d + \ldots + a_1 c_{m-1} + a_0) - (b_d c_{m-1}^d + \ldots + b_1 c_{m-1} + b_0) c_m = 0.\end{gathered}$$

We obtain a homogeneous linear system in $a_0, \ldots, a_d, b_0, \ldots, b_d$, and we can see a solution exists if there is a non-zero kernel to the following matrix

$$\begin{pmatrix} c_1^d & c_1^{d-1} & \ldots & c_1 & 1 & -c_1^d c_2 & -c_1^{d-1} c_2 & \ldots & -c_1 c_2 & c_2 \\ c_2^d & c_2^{d-1} & \ldots & c_2 & 1 & -c_2^d c_3 & -c_2^{d-1} c_3 & \ldots & -c_2 c_3 & c_3 \\ c_3^d & c_3^{d-1} & \ldots & c_3 & 1 & -c_3^d c_4 & -c_3^{d-1} c_4 & \ldots & -c_3 c_4 & c_4 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m-1}^d & c_{m-1}^{d-1} & \ldots & c_{m-1} & 1 & -c_{m-1}^d c_m & -c_{m-1}^{d-1} c_m & \ldots & -c_{m-1} c_m & c_m \end{pmatrix}. \quad (4.1)$$

In general, as we want a solution, we prescribe $2d+2$ points for a degree $d$ map, and expect a one dimensional kernel as long as the points are distinct, and hence a unique rational function with orbit $\{c_1, c_2, \ldots, c_m, \ldots\}$.

**Theorem 4.1.1.** *If $\{c_1, c_2, \ldots, c_m\}$ are distinct points for some even integer $m$, then there is a unique rational function of degree at most $d = \frac{m-2}{2}$ with the orbit $\{c_1, c_2, \ldots, c_m, \ldots\}$.*

*Proof.* Assume we have two distinct rational functions, $\phi$ and $\psi$, of degree $d$ and orbit $\{c_1, c_2, \ldots, c_m, \ldots\}$. Then the map $(\phi - \psi)(z)$ has $m-1$ roots, just by plugging in $z = c_i$ for $1 \leq i < m$. The numerator of $(\phi - \psi)$ has degree at most $2d$, and $2d \leq m-2$, so there are too many roots if the numerator is a non-zero polynomial, hence we must have that $\phi - \psi = 0$. Therefore $\phi = \psi$ and the map $\phi$ constructed from the orbit $\{c_1, \ldots, c_m, \ldots\}$ is unique. To show there is at least one rational function with the orbit $\{c_1, c_2, \ldots, c_m, \ldots\}$ we note the matrix (4.1) has $m-1$ rows and $m$ columns, hence will always have a non-zero kernel. □

For example, to find a degree two rational map with the orbit $\{0, 1, 2, 3, 5, 7, \ldots\}$,

we must find the kernel of the matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & -1 \\ 1 & 1 & 1 & -2 & -2 & -2 \\ 4 & 2 & 1 & -12 & -6 & -3 \\ 9 & 3 & 1 & -45 & -15 & -5 \\ 25 & 5 & 1 & -175 & -35 & -7 \end{pmatrix}$$

which we can easily find, has basis $[31, -53, -90, 1, -35, 90]$. Our desired function is

$$\frac{31z^2 - 53z - 90}{-z^2 + 35z - 90}.$$

The fact that this map has the orbit $\{0, 1, 2, 3, 5, 7, \ldots\}$ can easily be checked just by plugging in each value. With this construction in mind, our search method will be to prescribe orbits of the form $\{c_1, \ldots, c_{2d+2}, \ldots\}$ and see whether the corresponding rational maps are of the appropriate degree. If they are, we can check if the maps have any more integers in their orbits, that the orbits are not preperiodic, and if so, check to see if the maps are minimal.

## 4.2 Search Method

We outline our main search method, a naive exhaustive search. We also mention the main obstruction in the method.

With the construction process outlined above, we would like to see how many extra integers in the orbit we get for a minimal map. We may search all orbits from $(0, -c, -c, \ldots, -c, \ldots)$ to $(0, c, c, \ldots, c, \ldots)$ for some upper bound $c$. Notice the orbits $(0, c_1, c_2, \ldots, c_m, \ldots)$ and $(0, -c_1, -c_2, \ldots, -c_m, \ldots)$ would create rational maps $F_1/G_1$ and $F_2/G_2$ where $F_1(z)/G_1(z) = -F_2(-z)/G_2(-z)$. Then if $F_1/G_1$ is minimal, $F_2/G_2$ is also minimal as they are $\mathrm{PGL}_2(\mathbb{Z})$-conjugate. Thus we need only search the orbits $(0, 1, -c, \ldots, -c, \ldots)$ to $(0, c, c, \ldots, c, \ldots)$.

We recall that Silverman conjectures (see Conjecture 2.2.21) the number of integer points that can occur in a wandering orbit of an minimal rational map of degree $d$ is uniformly bounded by a constant in terms of $d$.

The only part we have yet to explain, is how to determine if 0 is a preperiodic point or a wandering point in each case. For any map $\phi \in \mathbb{Q}(z)$ we will use related maps, called the reduction of $\phi$ at $p$ for some prime $p$. Let $[F, G]$ be a normalized representation of $\phi$, and let $p$ be a prime. We call the *reduction of $\phi$ at $p$* the map $\tilde{\phi} = \tilde{F}/\tilde{G}$ where $\tilde{F}$ and $\tilde{G}$ are the images of the polynomials $F$ and $G$ over the finite field with $p$ elements, $\mathbb{F}_p$. The reduction of any map $\psi \in \mathbb{Q}(z)$ is computed by first getting a normalized representation $[S, T]$ and then $\tilde{\psi} = \tilde{S}/\tilde{T}$. Similarly, for $P \in \mathbb{Q}$, denote the reduction of $P$ modulo $p$ by $\tilde{P}$, where $\tilde{P} = \infty$ if $\mathrm{ord}_p(P) < 0$.

Suppose we have a rational map $\phi \in \mathbb{Q}(z)$, with orbit $\mathcal{O}$ of 0. Our goal will be to study the orbit of 0 under $\phi$ based on the orbits of the reductions of $\phi$ at some primes.

**Theorem 4.2.1** (Theorem 2.21 in [8]). *Let $\phi\colon \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{P}^1(\mathbb{Q}_p)$ be a rational function of degree $d \geq 2$. Assume that $\phi$ and $\tilde{\phi}$ have the same degree, let $P \in \mathbb{P}^1(\mathbb{Q}_p)$ be a periodic point of $\phi$, and define the following quantities:*

$n$ *The period of $P$ for the map $\phi$.*

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

$r$ *The order of $(\tilde{\phi}^m)'(\tilde{P})$ in $(\mathbb{Z}/p\mathbb{Z})^*$, or $\infty$ if $(\tilde{\phi}^m)'(\tilde{P}) = 0$.*

*Then $n$ has one of the following forms:*

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

It is simple to see when 0 is preperiodic for a map, when the orbit of 0 contains only integers. For a given map $\phi \in \mathbb{Q}(z)$ with $\mathcal{O}_\phi(0)$ containing some rational numbers, our goal will be to use multiple primes and show this theorem implies there is no possible integer $n$, such that a point $P \in \mathcal{O}_\phi(0)$ satisfies $\phi^n(P) = \phi(P)$. The strategy to show 0 is not preperiodic under $\phi$ is as follows:

- Find a short list of primes of good reduction (i.e., primes that do not divide the resultant)
- For each prime $p$ in the list, compute the following

  - The period of a point in the orbit of 0 under $\tilde{\phi}$
  - The order of $(\tilde{\phi}^m)'(\tilde{P})$

- For each prime $p$, write the list of possible period lengths $n$ as $L_p$
- Take the intersection of all the $L_p$

If the intersection of the $L_p$, the lists of possible periods, is empty, no point in the orbit of 0 under $\phi$ can be periodic, hence 0 is a wandering point. Continuing with Example 3.3.4, we wish to show our rational map $\phi_3$ has 0 as a wandering point.

**Example 4.2.2.** We have $\text{Res}(\phi_3) = 2^5 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13$, and so two primes of good reduction are 17 and 19. Reducing $\phi_3$ at 17 we have

$$\psi_{17}(z) = \frac{z^2 + 3z + 2}{z^2 + 7z + 2} \in \mathbb{F}_{17}(z)$$

and at 19 we have

$$\psi_{19}(z) = \frac{10z^2 + 15z + 4}{z^2 + 7z + 4} \in \mathbb{F}_{19}(z).$$

Observing the forward orbit of 0 under each map, we see

$$\begin{aligned}\mathcal{O}_{\psi_{17}}(0) &= \{0, 1, 4, 11, 12, 7, 15, 0, \ldots\} \\ \mathcal{O}_{\psi_{19}}(0) &= \{0, 1, 4, 11, 12, 7, 15, 6, 6, \ldots\}.\end{aligned}$$

At 17, our map has 0 as a periodic point with period length 7 whereas at 19 our map has 6 as a periodic point of length 1. By the chain rule, we may compute

$$\begin{aligned}(\psi_{17}^7)'(0) &= \psi_{17}'(0)\psi_{17}'(1)\psi_{17}'(4)\psi_{17}'(11)\psi_{17}'(12)\psi_{17}'(7)\psi_{17}'(15) \\ &= 0.\end{aligned}$$

Thus $r_{17} = \infty$. Similarly, one can find $r_{19} = 18$. Hence if 0 is preperiodic under $\phi_3$, some point in the forward orbit of 0 is periodic with period length in

$$\{7\} \cap \{1, 18, 18 \cdot 19^e\} = \emptyset.$$

Therefore under $\phi_3$, 0 must be a wandering point. Hence we have a minimal map with 0 a wandering point and 8 integer points in the forward orbit of 0, as

$$\mathcal{O}_{\phi_3}(0) = \{0, 1, 4, 11, 12, 7, 15, -374, 59183/652, \ldots\}.$$

We conducted exhaustive searches on degree two and three maps to investigate the conjecture on a small scale. For the degree two case, we searched orbits $\{0, c_1, c_2, \ldots, c_6, \ldots\}$ with $c_1 \in \{1, \ldots, 100\}$, $c_2, \ldots, c_5 \in \{-100, \ldots, 100\}$ and $c_6 \in \mathbb{Z}$. For the degree 3 case, we searched for orbits $\{0, c_1, c_2, \ldots, c_8, \ldots\}$ with $c_1 \in \{1, \ldots, 10\}$, $c_2, \ldots, c_7 \in \{-100, \ldots, 100\}$ and $c_8 \in \mathbb{Z}$. The bounds are governed by the hardware that we used, as described in the following sections.

## 4.3 Results

### 4.3.1 Degree Two Rational Maps

In the degree two search, we want our prescribed orbits to have length $2 \cdot 2 + 2 = 6$. Our setting is an orbit $(0, c_1, c_2, c_3, c_4, c_5, \ldots)$, with $c_1, \ldots, c_5 \in \mathbb{Z}$, corresponding to a rational map $\phi(z) = (a_2z^2 + a_1z + a_0)/(b_2z^2 + b_1z + b_0)$. First we wish to determine whether $c_6 = \phi(c_5)$ is an integer. We can determine the value of $c_6$ using an elementary method. To this end, we know plugging an orbit in to the rational map $\phi$ gives rise to a number of equations, (4.1), so including $\phi(c_5) = c_6$ we get the matrix

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & -c_1 \\ c_1^2 & c_1 & 1 & -c_1^2c_2 & -c_1c_2 & -c_2 \\ c_2^2 & c_2 & 1 & -c_2^2c_3 & -c_2c_3 & -c_3 \\ c_3^2 & c_3 & 1 & -c_3^2c_4 & -c_3c_4 & -c_4 \\ c_4^2 & c_4 & 1 & -c_4^2c_5 & -c_4c_5 & -c_5 \\ c_5^2 & c_5 & 1 & -c_5^2c_6 & -c_5c_6 & -c_6 \end{pmatrix}.$$

If there exists a rational function with the orbit $\{0, c_1, c_2, \ldots, c_6, \ldots\}$, the determinant of the matrix above must be 0. The determinant is linear in $c_6$, so we get a rational expression for $c_6$ in terms of the previous integer points, $c_1, \ldots, c_5$. The determinant is $D_1c_6 + D_2$ where,

$D_1 = -c_1^2 \cdot c_2^2 \cdot c_3^3 \cdot c_4 + c_1 \cdot c_2^3 \cdot c_3^3 \cdot c_4 + c_1^2 \cdot c_2^3 \cdot c_3 \cdot c_4^2 - 2 \cdot c_1 \cdot c_2^3 \cdot c_3^2 \cdot c_4^2 + c_1^2 \cdot c_2 \cdot c_3^3 \cdot c_4^2 - c_1^2 \cdot c_2^2 \cdot c_3 \cdot c_4^3 + 2 \cdot c_1 \cdot c_2^2 \cdot c_3^2 \cdot c_4^3 - c_1 \cdot c_2 \cdot c_3^3 \cdot c_4^3 - c_1^3 \cdot c_2^3 \cdot c_3 \cdot c_5 + 2 \cdot c_1^3 \cdot c_2^2 \cdot c_3^2 \cdot c_5 - c_1^2 \cdot c_2^2 \cdot c_3^3 \cdot c_5 + c_1^3 \cdot c_2^3 \cdot c_4 \cdot c_5 - c_1^3 \cdot c_2^2 \cdot c_3 \cdot c_4 \cdot c_5 - c_1^2 \cdot c_2^3 \cdot c_3 \cdot c_4 \cdot c_5 - 2 \cdot c_1^3 \cdot c_2 \cdot c_3^2 \cdot c_4 \cdot c_5 + 3 \cdot c_1^2 \cdot c_2^2 \cdot c_3^2 \cdot c_4 \cdot c_5 + c_1^2 \cdot c_2 \cdot c_3^3 \cdot c_4 \cdot c_5 - c_2^3 \cdot c_3^3 \cdot c_4 \cdot c_5 - c_1^3 \cdot c_2^2 \cdot c_4^2 \cdot c_5 - c_1^2 \cdot c_2^3 \cdot c_4^2 \cdot c_5 + c_1^3 \cdot c_2 \cdot c_3 \cdot c_4^2 \cdot c_5 + 2 \cdot c_1^2 \cdot c_2^2 \cdot c_3 \cdot c_4^2 \cdot c_5 + c_1 \cdot c_2^3 \cdot c_3 \cdot c_4^2 \cdot c_5 + c_1^3 \cdot c_3^2 \cdot c_4^2 \cdot c_5 - 3 \cdot c_1^2 \cdot c_2 \cdot c_3^2 \cdot c_4^2 \cdot$

$c_5-2\cdot c_1\cdot c_2^2\cdot c_3^2\cdot c_4^2\cdot c_5+2\cdot c_2^3\cdot c_3^2\cdot c_4^2\cdot c_5-c_1^2\cdot c_3^3\cdot c_4^2\cdot c_5+c_1\cdot c_2\cdot c_3^3\cdot c_4^2\cdot c_5+c_1^2\cdot c_2^2\cdot c_4^3\cdot c_5+c_1^2\cdot c_2\cdot c_3\cdot c_4^3\cdot c_5-2\cdot c_1\cdot c_2^2\cdot c_3\cdot c_4^3\cdot c_5-c_1^2\cdot c_3^2\cdot c_4^3\cdot c_5+c_1\cdot c_2\cdot c_3^2\cdot c_4^3\cdot c_5-c_2^2\cdot c_3^2\cdot c_4^3\cdot c_5+c_1\cdot c_3^3\cdot c_4^3\cdot c_5+2\cdot c_1^2\cdot c_2^3\cdot c_3\cdot c_5^2-c_1^3\cdot c_2\cdot c_3^2\cdot c_5^2-3\cdot c_1^2\cdot c_2^2\cdot c_3^2\cdot c_5^2+c_1^2\cdot c_2\cdot c_3^3\cdot c_5^2+c_1\cdot c_2^2\cdot c_3^3\cdot c_5^2-c_1^2\cdot c_2^3\cdot c_4\cdot c_5^2+2\cdot c_1^3\cdot c_2\cdot c_3\cdot c_4\cdot c_5^2-c_1^2\cdot c_2^2\cdot c_3\cdot c_4\cdot c_5^2+2\cdot c_1^2\cdot c_2\cdot c_3^2\cdot c_4\cdot c_5^2-c_1\cdot c_2^2\cdot c_3^2\cdot c_4\cdot c_5^2-2\cdot c_1\cdot c_2\cdot c_3^3\cdot c_4\cdot c_5^2+c_2^2\cdot c_3^3\cdot c_4\cdot c_5^2+c_1^3\cdot c_2\cdot c_4^2\cdot c_5^2+c_1\cdot c_2^3\cdot c_4^2\cdot c_5^2-2\cdot c_1^3\cdot c_3\cdot c_4^2\cdot c_5^2-3\cdot c_1^2\cdot c_2\cdot c_3\cdot c_4^2\cdot c_5^2+2\cdot c_1\cdot c_2^2\cdot c_3\cdot c_4^2\cdot c_5^2-2\cdot c_2^3\cdot c_3\cdot c_4^2\cdot c_5^2+3\cdot c_1^2\cdot c_3^2\cdot c_4^2\cdot c_5^2+c_1\cdot c_2\cdot c_3^2\cdot c_4^2\cdot c_5^2-c_1\cdot c_3^3\cdot c_4^2\cdot c_5^2-c_1^2\cdot c_2\cdot c_4^3\cdot c_5^2+c_1^2\cdot c_3\cdot c_4^3\cdot c_5^2+c_2^2\cdot c_3\cdot c_4^3\cdot c_5^2-c_1\cdot c_3^2\cdot c_4^3\cdot c_5^2-c_1\cdot c_2^3\cdot c_3\cdot c_5^3+c_1^2\cdot c_2\cdot c_3^2\cdot c_5^3+c_1\cdot c_2^2\cdot c_3^2\cdot c_5^3-c_1\cdot c_2\cdot c_3^3\cdot c_5^3-c_1^3\cdot c_2\cdot c_4\cdot c_5^3+c_1^2\cdot c_2^2\cdot c_4\cdot c_5^3+c_1^3\cdot c_3\cdot c_4\cdot c_5^3-c_1^2\cdot c_2\cdot c_3\cdot c_4\cdot c_5^3+c_2^3\cdot c_3\cdot c_4\cdot c_5^3-2\cdot c_1^2\cdot c_3^2\cdot c_4\cdot c_5^3+c_1\cdot c_2\cdot c_3^2\cdot c_4\cdot c_5^3-c_2^2\cdot c_3^2\cdot c_4\cdot c_5^3+c_1\cdot c_3^3\cdot c_4\cdot c_5^3+c_1^2\cdot c_2\cdot c_4^2\cdot c_5^3-c_1\cdot c_2^2\cdot c_4^2\cdot c_5^3$

and

$D_2=c_1^3\cdot c_2^2\cdot c_3^3\cdot c_4-c_1^2\cdot c_2^3\cdot c_3^3\cdot c_4-c_1^3\cdot c_2^3\cdot c_3\cdot c_4^2+2\cdot c_1^2\cdot c_2^3\cdot c_3^2\cdot c_4^2-c_1^3\cdot c_2\cdot c_3^3\cdot c_4^2+c_1^3\cdot c_2^2\cdot c_3\cdot c_4^3-2\cdot c_1^2\cdot c_2^2\cdot c_3^2\cdot c_4^3+c_1^2\cdot c_2\cdot c_3^3\cdot c_4^3-c_1^3\cdot c_2^2\cdot c_3^3\cdot c_5+c_1^2\cdot c_2^3\cdot c_3^3\cdot c_5+2\cdot c_1^3\cdot c_2^3\cdot c_3\cdot c_4\cdot c_5-3\cdot c_1^3\cdot c_2^2\cdot c_3^2\cdot c_4\cdot c_5-c_1^2\cdot c_2^3\cdot c_3^2\cdot c_4\cdot c_5+c_1^3\cdot c_2\cdot c_3^3\cdot c_4\cdot c_5+c_1^2\cdot c_2^2\cdot c_3^3\cdot c_4\cdot c_5+c_1^3\cdot c_2^2\cdot c_3\cdot c_4^2\cdot c_5-2\cdot c_1^2\cdot c_2^3\cdot c_3\cdot c_4^2\cdot c_5+2\cdot c_1^3\cdot c_2\cdot c_3^2\cdot c_4^2\cdot c_5-c_1^2\cdot c_2\cdot c_3^3\cdot c_4^2\cdot c_5-2\cdot c_1^3\cdot c_2\cdot c_3\cdot c_4^3\cdot c_5+c_1\cdot c_2^3\cdot c_3\cdot c_4^3\cdot c_5+2\cdot c_1^2\cdot c_2\cdot c_3^2\cdot c_4^3\cdot c_5+c_1\cdot c_2^2\cdot c_3^2\cdot c_4^3\cdot c_5-c_2^3\cdot c_3^2\cdot c_4^3\cdot c_5-2\cdot c_1\cdot c_2\cdot c_3^3\cdot c_4^3\cdot c_5+c_2^2\cdot c_3^3\cdot c_4^3\cdot c_5+c_1^3\cdot c_2^2\cdot c_3^2\cdot c_5^2-c_1^2\cdot c_2^3\cdot c_3^2\cdot c_5^2+c_1^2\cdot c_2^2\cdot c_3^3\cdot c_5^2-c_1\cdot c_2^3\cdot c_3^3\cdot c_5^2-c_1^3\cdot c_2^2\cdot c_3\cdot c_4\cdot c_5^2+c_1^2\cdot c_2^3\cdot c_3\cdot c_4\cdot c_5^2+3\cdot c_1^2\cdot c_2^2\cdot c_3^2\cdot c_4\cdot c_5^2+c_1\cdot c_2^3\cdot c_3^2\cdot c_4\cdot c_5^2-3\cdot c_1^2\cdot c_2\cdot c_3^3\cdot c_4\cdot c_5^2-c_1\cdot c_2^2\cdot c_3^3\cdot c_4\cdot c_5^2+c_2^3\cdot c_3^3\cdot c_4\cdot c_5^2+2\cdot c_1^2\cdot c_2^3\cdot c_4^2\cdot c_5^2-c_1\cdot c_2^3\cdot c_3\cdot c_4^2\cdot c_5^2-c_1^3\cdot c_2^2\cdot c_3^2\cdot c_4^2\cdot c_5^2-3\cdot c_1^2\cdot c_2\cdot c_3^2\cdot c_4^2\cdot c_5^2+c_1^2\cdot c_2\cdot c_3^3\cdot c_4^2\cdot c_5^2+4\cdot c_1\cdot c_2\cdot c_3^3\cdot c_4^2\cdot c_5^2-2\cdot c_2^2\cdot c_3^3\cdot c_4^2\cdot c_5^2-c_1\cdot c_2^3\cdot c_4^3\cdot c_5^2+c_1^3\cdot c_3\cdot c_4^3\cdot c_5^2+c_1^2\cdot c_2\cdot c_3\cdot c_4^3\cdot c_5^2-c_1\cdot c_2^2\cdot c_3\cdot c_4^3\cdot c_5^2+c_2^3\cdot c_3\cdot c_4^3\cdot c_5^2-c_1^2\cdot c_3^2\cdot c_4^3\cdot c_5^2-c_1^2\cdot c_2^2\cdot c_3^2\cdot c_5^3+c_1\cdot c_2^3\cdot c_3^2\cdot c_5^3+c_1^3\cdot c_2^2\cdot c_4\cdot c_5^3-c_1^3\cdot c_2\cdot c_3\cdot c_4\cdot c_5^3+c_1^2\cdot c_2\cdot c_3^2\cdot c_4\cdot c_5^3-c_1\cdot c_2^2\cdot c_3^2\cdot c_4\cdot c_5^3-c_2^3\cdot c_3^2\cdot c_4\cdot c_5^3+c_1\cdot c_2\cdot c_3^3\cdot c_4\cdot c_5^3-2\cdot c_1^2\cdot c_2^2\cdot c_4^2\cdot c_5^3+2\cdot c_1^2\cdot c_2\cdot c_3\cdot c_4^2\cdot c_5^3+c_1\cdot c_2^2\cdot c_3\cdot c_4^2\cdot c_5^3+c_1^2\cdot c_3^2\cdot c_4^2\cdot c_5^3-3\cdot c_1\cdot c_2\cdot c_3^2\cdot c_4^2\cdot c_5^3+2\cdot c_2^2\cdot c_3^2\cdot c_4^2\cdot c_5^3-c_1\cdot c_3^3\cdot c_4^2\cdot c_5^3+c_1\cdot c_2^2\cdot c_4^3\cdot c_5^3-c_1^2\cdot c_3\cdot c_4^3\cdot c_5^3-c_2^2\cdot c_3\cdot c_4^3\cdot c_5^3+c_1\cdot c_3^2\cdot c_4^3\cdot c_5^3$

so solving for $c_6$ gives

$$c_6=-D_2/D_1.$$

Checking whether $c_6\in\mathbb{Z}$ now amounts to checking whether $D_1$ divides $D_2$. Hence our search process is as follows:

- Enumerate tuples $(c_1,\ldots,c_5)$.
- Check, for each choice, if $D_1(c_1,\ldots,c_5)$ divides $D_2(c_1,\ldots,c_5)$. If so, store $(c_1,\ldots,c_5,-\frac{D_2}{D_1})$ for later processing.

We can execute this procedure quite quickly if we ensure that all integers we encounter fit inside the natural word length of the computer we use. We worked on a 64-bit computer. This means that integers in the range $-2^{63}+1,\ldots,2^{63}-1$ can be represented and computed with very quickly.

We observe that $D_2$ has total degree 9 and has 70 monomials and coefficients of absolute value at most 4. Hence, if we ensure that $70\cdot 4\cdot |c|^9 < 2^{63}$ we can compute the value of $D_2$ using system integers, without overflow. This means we can take $c_i \in \{-68,\ldots,68\}$

In fact, $D_1$ has total degree 8 and 76 monomials with coefficients of absolute value at most 3. This gives us a range $c_i \in \{-119,\ldots,119\}$. The following observation allows us to improve the range slightly. We only need to check the value of $D_2$ modulo $D_1$. We can do this by evaluating each monomial of $D_2$ separately, compute its remainder modulo $D_1$, add these, and check the remaining sum for divisibility by $D_1$. This way we only need each term of $D_2$ to individually fit inside a system integer. This means we require that $4\cdot|c|^9 < 2^{63}$, giving $c\in\{-109,\ldots,109\}$. Using this approach, we can search up to 100 while avoiding having to use computationally expensive arbitrary precision libraries. On a 2.3GHz machine, this search was completed in around 4 days.

We apply our minimality algorithm from Chapter 3. The minimality search took around 3 days. We found the following results: For degree 2 rational maps with at least 7 integer points in the orbit of 0,

| | |
|---|---|
| Search space | 160 000 000 000 |
| Orbits with a 7-th integer point | 2 112 933 |
| Orbits corresponding to minimal maps | 2 261 |
| Preperiodic orbits | 64 |
| Polynomials | 7 |
| Non-polynomial, non-preperiodic orbits with at least 7 integer points in the orbit of 0 | 2 190 |

For the list of non-polynomial, non-preperiodic orbits with at least 7 integer points in the orbit of 0, see `http://www.cecm.sfu.ca/~nbruin/intorbits/` . We also

searched for minimal rational maps with orbit

$$\{0, c_1, c_2, c_3, c_4, c_5, \infty, c_6, \ldots\}$$

where $c_1, \ldots, c_6 \in \mathbb{Z}$ and $-100 \leq c_i \leq c_5$ for $1 \leq i \leq 5$, but none exist.

One of the benefits of searching the orbits starting at 0 is we can check for points that map to 0 by simply checking for integral roots of $F$. We can search for an eighth integer point in the orbits by both checking for a point before 0 or a point after the seventh. The following shows the results of the search for 8 integer points in the orbit of 0,

| | |
|---|---|
| Orbits with an integer before 0 | 4 |
| Orbits with an 8-th point | 5 |
| Number of orbits in both cases that are $\mathrm{PGL}_2(\mathbb{Z})$ conjugates | 4 |
| Number of minimal orbits with 8 integer points in the orbit of 0 | 5 |

For the orbits with an 8-th integer point, see Appendix B.

We found no examples with 9 integer points in the orbit of 0. It is interesting to note the rational map

$$\phi(z) = \frac{12z^2 - 29z - 35}{z^2 + 8z - 35}$$

is the only map we found that has a finite non-integral point in between the integer points. Namely, the orbit of 0 is

$$\mathcal{O}_\phi(0) = \{0, 1, 2, 3, 7, 5, 4, \frac{41}{13}, -40, \frac{1355}{83}, \ldots\}$$

### 4.3.2 Degree Three Rational Maps

In the degree three case, our prescribed orbits have length $2 \cdot 3 + 2 = 8$. Our setting is an orbit $(0, c_1, c_2, c_3, c_4, c_5, c_6, c_7, \ldots)$, with $c_1, \ldots, c_7 \in \mathbb{Z}$, corresponding to a rational map $\phi(z) = (a_3z^3 + a_2z^2 + a_1z + a_0)/(b_3z^3 + b_2z^2 + b_1z + b_0)$. We wish to determine whether $c_8 = \phi(c_7)$ is an integer. This time, including $\phi(c_7) = c_8$, the equation (4.1) gives rise to the matrix

$$\begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 0 & -c_1 \\
c_1^3 & c_1^2 & c_1 & 1 & -c_1^3c_2 & -c_1^2c_2 & -c_1c_2 & -c_2 \\
c_2^3 & c_2^2 & c_2 & 1 & -c_2^3c_3 & -c_2^2c_3 & -c_2c_3 & -c_3 \\
c_3^3 & c_3^2 & c_3 & 1 & -c_3^3c_4 & -c_3^2c_4 & -c_3c_4 & -c_4 \\
c_4^3 & c_4^2 & c_4 & 1 & -c_4^3c_5 & -c_4^2c_5 & -c_4c_5 & -c_5 \\
c_5^3 & c_5^2 & c_5 & 1 & -c_5^3c_6 & -c_5^2c_6 & -c_5c_6 & -c_6 \\
c_6^3 & c_6^2 & c_6 & 1 & -c_6^3c_7 & -c_6^2c_7 & -c_6c_7 & -c_7 \\
c_7^3 & c_7^2 & c_7 & 1 & -c_7^3c_8 & -c_7^2c_8 & -c_7c_8 & -c_8
\end{pmatrix}.$$

We may compute the determinant of this matrix, and it must again be 0. It is linear in $c_8$, thus gives a rational expression for $c_8$ in the previous integer points, and it is easy to check whether this is an integer or not. This determinant has 5656 monomials so we omit writing it here. Also, if we write the determinant as $D_1c_8 + D_2$ we have that computing each monomial of $D_2$ modulo $D_1$ would be a significant amount of work, hence we restrict our intermediate steps in computing $D_2$ module $D_1$ to computing polynomials with less than 100 monomials modulo $D_1$, to increase our search bound. As $D_1$ has a total degree of 15, $D_2$ has total degree 16 and the coefficients of $D_2$ have magnitude at most 6, we have a bound of $\left(\frac{2^{63}-1}{6\cdot 100}\right)^{1/16} \approx 10.3$. For our search, each prescribed orbit point has absolute value at most 10. The initial search took around 31 hours, while the minimality sieve took around 90 minutes. The results from the search were as follows, for degree 3 rational maps with at least 9 integer points in the orbit of 0,

| | |
|---|---|
| Search space | 640 000 000 |
| Orbits with a 9-th integer point | 44 563 |
| Orbits belonging to minimal maps | 10 383 |
| Orbits corresponding to non-degree 3 maps | 806 |
| Degree 3 polynomial orbits | 0 |
| Degree 3, preperiodic orbits | 997 |
| Degree 3 non-preperiodic, orbits with at least 9 integer points in the orbit of 0 | 8 580 |

For the list of non-polynomial, non-preperiodic orbits of 0 with at least 9 integer points, see `http://www.cecm.sfu.ca/~nbruin/intorbits/`. We also searched for minimal rational maps with orbit

$$\{0, c_1, c_2, c_3, c_4, c_5, c_6, c_7, \infty, c_8, \ldots\}$$

where $c_1, \ldots, c_8 \in \mathbb{Z}$ and $-10 \leq c_i \leq 10$ for $1 \leq i \leq 7$. We found 5, and they can be found in Appendix B.

For degree 3 rational maps with 10 integer points in orbits containing 0,

| | |
|---|---|
| Orbits with an integer before 0 | 35 |
| Orbits with a 10-th integer point | 34 |
| Number of orbits in both cases that are $\mathrm{PGL}_2(\mathbb{Q})$ conjugates | 13 |
| Number of minimal orbits with 10 integer points in the orbit of 0 | 56 |

For the orbits with a 10-th integer point, see Appendix B.

We did not find any maps with 11 integer points in the orbit of 0. As with the degree two search, we find only one map with a finite non-integral point in between the integers in orbit. Namely,

$$\phi(z) = \frac{95z^3 - 1863z^2 + 11692z - 23520}{16z^3 - 300z^2 + 1778z - 3360}$$

has the forward orbit

$$\mathcal{O}_\phi(0) = \{0, 7, 3, 9, 10, 5, 8, 4, 20, \frac{28}{5}, -160, \frac{913973}{153133}, \ldots\}.$$

### 4.3.3 Degree Four and Beyond

Unfortunately, our search method using the determinant of a matrix to see if orbits have an additional integer point does not extend very well. For the degree 4 case, this determinant has over 100 000 monomials. Given this, to stay in 64 bits with an (small scale) exhaustive search, we need all our prescribed integer points to be in the range $\{-5, \ldots, 5\}$, which is much too small to have any reasonable search.

# Chapter 5

# Further Observations

From Proposition 3.1.1, one can see that for minimal rational maps, $\phi \in \mathbb{Q}(z)$, of degree at least two, and transformations $A \in \mathrm{PGL}_2(\mathbb{Z})$, one has $\mathrm{Res}(\phi^A) = \mathrm{Res}(\phi)$. One could ask if the converse is possible. Namely, if we have a minimal rational map $\phi \in \mathbb{Q}(z)$ of degree at least two, and a transformation $A \in \mathrm{PGL}_2(\mathbb{Q})$, then does $\mathrm{Res}(\phi^A) = \mathrm{Res}(\phi)$ imply that $A \in \mathrm{PGL}_2(\mathbb{Z})$?

Recall the map from Example 3.4.2, $\phi(z) = (z^3 + c)/z$ with $c \in \mathbb{Z}$, which is minimal. Let $A\colon z \mapsto az + b \in \mathrm{Aff}_2(\mathbb{Q})$ be an affine transformation. If we have $\phi$ and $\phi^A$ both minimal, then we must have

$$2d \min(\mathrm{ord}_p(F_A), \mathrm{ord}_P(G_A)) = (d^2 + d)\mathrm{ord}_p(a) \tag{5.1}$$

which means we require

$$\min(\mathrm{ord}_p(F_A), \mathrm{ord}_P(G_A)) = 2\mathrm{ord}_p(a).$$

If we pick $A\colon z \mapsto 2z$ we can write the conjugated rational map as $F_A = F(2z) = 2^3 z + c$ and $G_A = 2G(2z) = 4z$. As $a = 2$, $\mathrm{ord}_2(a) = 1$, so from (5.1), we require the minimum order of $F_A$ and $G_A$ at the prime 2 to be 2. This is clear from the denominator as long as $c$ is chosen to be divisible by 4. Both $\phi$ and $\phi^A$ are minimal, but $A \notin \mathrm{Aff}_2(\mathbb{Z})$. We can prove a more general result

**Theorem 5.0.1.** *Let $F(z) = z^d + c$ with $d \in \mathbb{Z}$ odd and $G(z) = z^{d_0}$ with $d_0 = \lceil d/2 \rceil$ and $c$ having valuation at least $d_0$ at some prime $p$. Then there exists an affine transformation $A$ such that $\phi$ and $\phi^A$ are both minimal, and $A \notin \mathrm{Aff}_2(\mathbb{Z})$.*

*Proof.* We attempt a similar argument. Notice what helped us in the degree three case in (5.1) was the fact that $(d^2+d)/2d$ was integral. This is true for any odd integer $d$. Let $d = 2m+1$ for some integer $m$; then $(d^2+d)/2d = (d+1)/2 = (2m+2)/2 = m+1 = \lceil d/2 \rceil$. Thus from Proposition 3.1.1 we must have

$$\min(\mathrm{ord}_p(F_A), \mathrm{ord}_P(G_A)) = \lceil d/2 \rceil \mathrm{ord}_p(a). \tag{5.2}$$

We use the same approach that worked with the case when $d = 3$. Set $A\colon z \mapsto pz \in \mathrm{Aff}_2(\mathbb{Q})$. Then (5.2) must be true, and hence $\phi$ and $\phi^A$ are both minimal, with $A \notin \mathrm{Aff}_2(\mathbb{Z})$. □

For even $d$, we no longer have that $(d^2+d)/2d$ is an integer, and hence, things are more complicated.

**Question 5.0.2.** Suppose that $\phi \in \mathbb{Q}(z)$ is of even degree and minimal. Does it follow that if $A \in \mathrm{PGL}_2(\mathbb{Q})$ and $\mathrm{Res}(\phi^A) = \mathrm{Res}(\phi)$ then $A \in \mathrm{PGL}_2(\mathbb{Z})$?

# Bibliography


[1] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[2] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[3] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984.

[4] Serge Lang. *Elliptic Curves Diophantine Analysis*, volume 231 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1978.

[5] Michael O. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, 9(2):273–280, 1980.

[6] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[7] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[8] Joseph H. Silverman. *The Arithmetic of Dynamical Systems*, volume 241 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2007.

[9] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, New York, 1992.

[10] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

# Appendix A

# Algorithms

Main affine minimality procedure, Affineminimal$(F, G)$:
Input: Co-prime polynomials $F$ and $G$, at least one of degree at least 2.
Output: (true,$F, G$) if $\phi$ is affine minimal, (false,$f, g$) if not, where $[f, g]$ is a normalized representation of a minimal model of $\phi$.

flag := true; $n :=$ lcm(denominators of coefficients of $F$ and $G$)
$F, G := nF, nG$; $d :=$ max(degree($F$),degree($G$)); Res := $\mathrm{Res}_d(F, G)$
$m :=$ max(deg$(F - zG)$, deg$(G)$); ubRes := $\mathrm{Res}_m(F - zG, G)$
**if** $d$ is even **then**
    $g = d$
**else**
    $g = 2d$
**for** $p$ in prime divisors of Res **do**
    **if** $\mathrm{ord}_p(Res) < g$ **then**
        $n :=$ true
    **else**
    **repeat** until $n$ is true
        $n, F, G :=$ Min($F, G, p, d$,ubRes)
        **if** $n$ is false **then**
            flag := false
**return** (flag,$F, G$)

Local affine minimality loop, Min$(F, G, p, d, ubRes)$:

Input: Two normalized polynomials $F$ and $G$, a prime $p$, the degree, $d$, of $F/G$ and a positive integer ubRes.

Output: (true, $F, G$) if $F/G$ is affine minimal at $p$, otherwise (false, $F_{new}, G_{new}$) where $F_{new}/G_{new}$ has resultant smaller than $F/G$.

$d_F :=$ degree$(F)$; $d_G :=$ degree$(G)$
**if** $G_d > (d+1)/2$ **then**
    $n := \lfloor -2(\text{ord}_p(\text{leading coeff of } G))/(2G_d - d + 1) + 1 \rfloor$
**else**
    $n := \lfloor (-2\text{ord}_p(\text{leading coeff of } F)/(d+1) + 1) \rfloor$
upperBound := ord$_p$(2·ubRes)
**while** $n <=$ upperBound **do**
    $F_t := F(p^n z + b) - bG(p^n z + b)$; $G_t := p^n G(p^n z + b)$; $v := (d+1)n/2$
    **if** constant coefficients of $F_t$ and $G_t$ have valuation larger than $v$ **then**
        **if** $b = 0$ gives ord$_p(F_t) > v$ and ord$_p(G_t) > v$ **then**
            $F := F_t(z, 0)$; $G := G_t(z, 0)$; $F, G :=$ normalize$(F, G)$
            **return**(false,$F, G$)
        $v_b :=$ lower bound on ord$_p(b)$, as per Theorem 3.3.5
        Set $F_t(z, b) := F_t(z, bp^{-v_b})$ and $G_t(z, b) := G_t(z, bp^{-v_b})$
        Scale $F_t$ and $G_t$ so that $[F_t, G_t]$ is a normalized representation
        Set $v := v + s$, where $s$ is the maximum exponent used in normalizing
        bound := $\lfloor v + 1 \rfloor$
        bool,$s :=$ solveb(normalized coefficients of $F_t, G_t$,bound,$p$)
        **if** bool **then**
            $s_b := sp^{v_b}$
            $F_t, G_t :=$ normalize$(F_t(z, s_b), G_t(z, s_b))$
            **return**(false,$F_t, G_t$)
    $n := n + 1$
**return**(true,$F, G$)

Procedure for determining a lower bound on $b$, bCheck(coeff,RHS,p,b):
Input: A polynomial $c = \sum_{i=0}^{d} c_i b^i$, a rational number RHS, and a prime $p$.
Output: Lower bound on the order of $b$ so that $\text{ord}_p(c) > \text{RHS}$.

$d$ := degree($c$)
lcoeff := $c_d$
chk1 := $\lceil(\text{ord}_p(c) - \text{ord}_p(\text{lcoeff}))/(d$ - i) for non-zero coefficients , $c_i$ of $c$, $i < d\rceil$
chk2 := (RHS - $\text{ord}_p$(lcoeff))/deg
bval := min(chk1,chk2)
**return** $\lfloor$ bval + 1 $\rfloor$

Procedure to determine if there exists a solution to a system of inequalities in one variable, solveb($L_F$,$L$,$p$):
Input: A list of polynomials $L_F$ in $b$, an integer $L$ and a prime $p$.
Output: (true,$b$) if there exists an integer $b$ so that each polynomial $F$ in $L_F$ satisfies $\text{ord}_p(F(b)) > L$, (false,0) otherwise.

keepScaledIneqs := $[F$ in $L_F$ if $F/p^L \notin \mathbb{Z}[b]]$
**if** keepScaledIneqs is an empty list **then**
    **return** (true,1)
keptScaledIneqs := keepScaledIneqs reduced mod $p$
rts := roots of gcd of keptScaledIneqs
**for** $r$ in rts **do**
    newInput := $r + pb$
    $L_G := [F(\text{newInput})$ for $F$ in $L_F]$
    lift,$c$ := solveb($L_G, L, p$)
    **if** lift **then**
        **return** (true,$r + pc$)
**return**(false,0)

# Appendix B

# Orbits that lead to Minimal Rational Maps

## B.1 Degree Two Results

The following orbits correspond to minimal degree two maps with at least 8 integer points in the orbit of 0,

$$[0, 1, 4, 11, 12, 7, 15, -374, \ldots]$$
$$[0, 1, 4, 11, 12, 7, 41/13, -40, \ldots]$$
$$[0, 7, -8, -21, -5, -33, -26, -1020, \ldots]$$
$$[0, 9, -10, 2, 12, -5, 1, 10, \ldots]$$
$$[0, 35, 27, 17, 18, 21, 26, -99, \ldots]$$

## B.2 Degree Three Results

The following orbits correspond to minimal degree three maps with 10 consecutive integer points in the forward orbit of 0,

$[0, 1, -3, -4, -1, -2, -6, 8, -11, -582, \ldots]$ $[0, 1, -2, -5, 4, -4, 2, -3, -8, 187, \ldots]$

$[0, 1, -1, 7, -5, -3, -8, -7, -2, -37, \ldots]$ $[0, 1, 2, -2, -10, -8, -7, -6, -4, -83, \ldots]$

$[0, 1, 9, -3, -5, -9, -4, -6, 2, 18, \ldots]$ $[0, 2, -6, 6, -3, 3, -9, 5, -5, 8, \ldots]$

$[0, 2, -6, 8, -2, 1, -1, 5, 15, -67, \ldots]$ $[0, 2, -5, 5, -1, 1, -7, 7, 25, 87, \ldots]$

$[0, 2, -3, 1, -8, -2, 3, -1, 12, 80, \ldots]$ $[0, 2, -3, 3, 1, -9, -1, 6, 11, 321, \ldots]$

$[0, 2, -2, -6, -5, -3, 3, 1, 9, 5, \ldots]$ $[0, 2, -1, -10, 5, -2, -7, 8, -4, -33, \ldots]$

$[0, 2, -1, 3, -6, -5, -8, -2, 4, 244, \ldots]$ $[0, 2, 1, 4, 8, 7, 6, -1, -2, -13, \ldots]$

$[0, 2, 4, 1, 3, -5, 7, 9, 6, -92, \ldots]$ $[0, 2, 6, 3, 10, 7, -5, -8, -18, 2735, \ldots]$

$[0, 3, -10, 8, -7, 7, -1, 5, 13, 89, \ldots]$ $[0, 3, -6, 9, 4, -1, -2, -3, 2, -83, \ldots]$

$[0, 3, -1, 2, 9, 4, 5, 8, 11, -8, \ldots]$ $[0, 3, 4, 1, 6, -8, -7, -2, 28, -195, \ldots]$

$[0, 4, -3, -2, 3, -1, 9, -8, -12, -13, \ldots]$ $[0, 4, -2, 3, 1, 5, -4, 10, -7, -24, \ldots]$

$[0, 4, -2, 3, 2, -1, 6, -4, -22, -13, \ldots]$ $[0, 4, -2, 6, 1, 3, 7, -1, 5, -421, \ldots]$

$[0, 4, 10, -1, 5, 9, -5, 1, 3, 41, \ldots]$ $[0, 6, -2, -6, -4, -9, -3, 1, 3, 5, \ldots]$

$[0, 6, 3, -1, 5, -4, 8, 2, -6, -5, \ldots]$ $[0, 7, -4, 5, 6, 10, 3, 4, 1, -180, \ldots]$

$[0, 7, 4, -5, 2, -3, 9, 1, -2, 265, \ldots]$ $[0, 8, -5, 3, -2, 9, -4, 7, -6, -539, \ldots]$

$[0, 8, 2, 3, -1, 5, -2, 7, 1, 6, \ldots]$ $[0, 9, -7, 5, -10, -1, -2, -9, 1, -969, \ldots]$

$[0, 9, 3, -6, -1, 4, -3, 1, 39, -56, \ldots]$ $[0, 9, 6, 7, 4, 10, -2, -5, 40, 37, \ldots]$

Below are (the distinct $\mathrm{PGL}_2(\mathbb{Z})$-conjugates of) the maps found by search for roots

of the numerator of the corresponding rational map

$[0, 2, -5, 11, 3, -1, 1, 4, -4, 328, \ldots]$ $[0, 4, 14, -4, 2, 5, -1, 3, 7, 35, \ldots]$

$[0, 5, 3, 6, 4, 13, 11, 12, 10, -3, \ldots]$ $[0, 5, 10, 9, 14, 7, 8, 4, 6, 11, \ldots]$

$[0, 6, 1, 8, 2, 14, -1, 5, 11, 149, \ldots]$ $[0, 6, 11, 2, 5, 16, 7, 10, 9, 18, \ldots]$

$[0, 7, 14, 5, 2, 4, -1, 6, 1, -34, \ldots]$ $[0, 8, 7, 3, 9, 11, 5, 6, 10, 2, \ldots]$

$[0, 9, 6, 14, 18, 12, 3, 7, 13, -1148, \ldots]$ $[0, 9, 15, 10, 18, 6, 16, 8, 11, 20, \ldots]$

$[0, 11, 3, 15, 21, 6, 12, 9, 16, 275, \ldots]$ $[0, 11, 10, 5, 14, 17, 12, 7, 6, -87, \ldots]$

$[0, 12, 8, 16, 20, 10, 13, 6, 15, -12, \ldots]$ $[0, 12, 18, 4, 6, 3, 9, 11, 15, -33, \ldots]$

$[0, 13, 15, 8, 10, 18, 14, 16, 9, -19, \ldots]$ $[0, 14, 7, 21, 18, 15, 9, 12, 6, 63, \ldots]$

$[0, 17, 13, 19, 20, 14, 21, 15, 16, -15, \ldots]$ $[0, 20, 15, 17, 21, 14, 16, 18, 11, -255, \ldots]$

$[0, 20, 18, 15, 12, 30, 21, 27, 22, 33, \ldots]$ $[0, 24, 27, 18, 30, 20, 21, 25, 19, 62, \ldots]$

$[0, 24, 33, 23, 27, 15, 18, 22, 25, -361, \ldots]$ $[0, 28, 30, 33, 36, 18, 27, 21, 26, 15, \ldots]$

We also have the orbits corresponding to degree three minimal maps with at least 9 integers and a non-integral value between them,

$$[0, 1, -1, -9, -5, -4, -3, 3, \infty, -6, \ldots]$$
$$[0, 1, 8, 5, 4, 3, 2, -2, \infty, 7, \ldots]$$
$$[0, 2, 5, -3, 9, -2, 7, 1, \infty, -24, \ldots]$$
$$[0, 6, 1, 3, 7, -1, 8, 2, \infty, -35, \ldots]$$
$$[0, 7, 3, 9, 10, 5, 8, 4, 20, 28/5, -160, \ldots]$$
$$[0, 9, -10, -4, 3, 8, 5, 10, \infty, -157, \ldots]$$