REDUCTION IN ARITHMETIC DYNAMICS

ANGELINE PENG

Abstract. In this expository piece, we will introduce and examine the behaviors of the reduction of dynamical systems in $\mathbb{Q}_p$. The results in this paper may be generalized to any local field. We define reduction rigorously and provide a characterization of good reduction using resultants. We then prove, among others, two main results: the first, a statement on the possibilities of the exact period of a point given the exact period of its reductions (4.8); and the second, an algorithm for determining whether a rational function has potentially good reduction (5.3).

Contents

(ending marks in math mode)

1. Introduction

The p-adic numbers were first introduced by Kurt Hensel in an attempt to perform Taylor expansions around a prime in $\mathbb{Z}$ [Gou20, Section 1.1]. This allowed him to use techniques from analysis to prove number-theoretical facts. For example, one might see Hensel's lemma as an algebraic version of the implicit function theorem. We may then utilize these tools when working over the rational numbers once we take the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

One specific tool that we examine in this paper is reduction.

Definition 1.1. The *reduction modulo p map* is the map $\pi : \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. We will write $\overline{x}$ to denote the image of $x \in \mathbb{Z}_p$ under π.

Date: May 14, 2025.

An obvious advantage of considering the reduction of our system is that $\mathbb{F}_p$ is a finite field. There is some work done in understanding dynamical systems over finite fields, but it is still a relatively new area.

The goal of this paper is to introduce reduction and the relationship between dynamical systems before and after reduction. We will in section 2 by recalling some essential definitions and facts about the p-adics. We also include some definitions used in dynamical systems. We define good reduction in section 3 and give a criterion for good reduction. Next, in section 4, we look more in detail at the properties of reduction, the most important result of which is Theorem 4.8, which tells us how the period of a point after reduction relates to the period of the point before reduction. We then turn to bad reduction in section 5 and give an algorithm to find a change of basis into good reduction, if it exists.

2. Preliminary Notions

In this section, we shall recall some definitions that will be used throughout the remainder of the paper. In particular

2.1. p-adics.

In this section, we shall recall the constructions of $\mathbb{Q}_p$ and state some facts. We omit the proofs and defer the reader to [Gou20], which provides an in-depth treatment of the p-adic numbers.

Definition 2.1. Let $p \in \mathbb{Z}$ be a prime. The *p-adic valuation* is the map $v_p : \mathbb{Z} \to \mathbb{R}$ which maps $x \in \mathbb{Z}$ to the largest r such that p^r divides x. More precisely, let $x = ap^r$ for a, r integers such that $p \nmid a$. Then,

$$v(x) := r.$$

We denote $v(0) := \infty$.

We extend v_p to $\mathbb{Q}$ as follows: let $\frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$ relatively prime. Define

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b).$$

We may use the p-adic valuation to define a nonarchimedean absolute value. First, let us recall the definition of an absolute value.

Definition 2.2. An *absolute value* on K is a map $|\cdot| : K \to \mathbb{R}$ satisfying the following three properties for all $x, y \in K$:

(1) $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
(2) $|xy| = |x| \cdot |y|$, and
(3) (triangle inequality) $|x + y| \leq |x| + |y|$.

We say that $|\cdot|$ is *nonarchimedean* if it satisfies the following stronger version of the triangle inequality:

$$|x + y| \leq \max(x, y)$$

for all $x, y \in K$.

Definition 2.3. The *p-adic absolute value* is the map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ defined as follows: let $x \in \mathbb{Q}$. Then,

$$|x|_p := p^{-v_p(x)}.$$

Fact 2.4. [Gou20, Proposition 2.1.5] *The p-adic absolute value is a nonarchimedean absolute value.*

Definition 2.5. The *p-adic numbers*, $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ under the p-adic absolute value.

The *p-adic integers*, $\mathbb{Z}_p$, are the p-adic numbers with nonnegative valuation.

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_v \leq 1\}.$$

Fact 2.6. [Gou20, Proposition 4.4.2] *The p-adic integers form a local ring (a local ring is a ring with a unique maximal ideal) with maximal ideal*

$$p\mathbb{Z}_p := \{x \in \mathbb{Z}_p \mid |x|_v < 1\}.$$

Recall that in a local ring, an element is either in the maximal ideal or a unit. Thus,

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid |x|_v = 1\}.$$

2.2. **Dynamics.** The main function that we consider are rational functions, and the space over which it is acts on will be $\mathbb{P}^1$, which we shall define in the following section. Afterwards, we recall some definitions from dynamics.

Definition 2.7. Let K be a field. A *rational function* is an element $\phi \in K(z)$. The *degree* of ϕ is the maximum of the degrees of f and g as polynomials.

If we write a rational function $\phi = \frac{f}{g}$, $f, g \in K[z]$ coprime, it is a function $\phi : K \to K$ defined by $\phi(P) := \frac{f(P)}{g(P)}$. However, it is not defined at points at which g is zero. To remedy this, we extend the domain and target of rational functions to $\mathbb{P}^1(K) = K \cup \{\infty\}$, where ∞ is called *the point at infinity*, and say that if there is a $P \in \mathbb{P}^1(K)$ such that $g(P) = 0$ (necessarily, $f(P) \neq 0$), then we say $\phi(P) := \infty$.

Remark 2.8. If we extend ϕ to $\mathbb{P}^1(K)$, one might wonder how we evaluate $\phi(\infty)$. A working answer is $\phi(\infty) := \frac{1}{\phi(0)} = \frac{g(0)}{f(0)}$, which one might recognize as performing a change of variables to switch ∞ and 0. The "morally correct" answer is by homogenization. For more details, one may refer to chapter 5 of [Gal11], which gives a lovely exposition of projective space.

In this paper, we have a rational function ϕ be an element of $\mathbb{Q}_p(z)$ but a map $\phi : \mathbb{P}^1(\overline{\mathbb{Q}_p}) \to \mathbb{P}^1(\overline{\mathbb{Q}_p})$, where $\overline{\mathbb{Q}_p}$ is a fixed algebraic closure of $\mathbb{Q}_p$.

Remark 2.9. There are many other, deeper results relating algebra and geometry when working in $\mathbb{P}^1(\overline{K})$, which one may find in some commutative algebra textbook, such as [AM16]. In this paper, we only use the fact that every polynomial has a root in this field. However, the issue with working in $\mathbb{P}^1(\overline{\mathbb{Q}_p})$ with the topology induced by the p-adic metric is that it is totally disconnected. To remedy this, we may complete this into $\mathbb{C}_p := \overline{\mathbb{Q}_p}$ once again such that it is complete with respect to the p-adic metric. $\mathbb{P}^1(\mathbb{C}_p)$ is an instance of a Berkovich projective line. A reference for further details on dynamics over Berkovich spaces is [BR10]. We may generalize the results in this paper by having ϕ be a map on $\mathbb{P}^1(\mathbb{C}_p)$. For simplicity, we state the results for $\overline{\mathbb{Q}_p}$).

The following definitions will be used in 4.1 and may be deferred until then.

Definition 2.10. Given a rational function $\phi \in \mathbb{Q}_p(z)$, we say that $P \in \mathbb{P}^1$ is (ϕ-)*periodic* if there is some integer $n \geq 1$ such that $\phi^n(P) = P$. For a periodic point, the smallest such n is called the *exact period* of P.

We say that P is (ϕ-)*preperiodic* if its orbit is finite. Equivalently, P is preperiodic if there is some i, n integers where $n \geq 1$ such that $\phi^i(P) = \phi^{i+n}(P)$.

(move tihs or make a note that i'll only use this later)
The following definitions will not be used until in 4.2 and may be deferred until then.

DEFINITION 2.11. Let P be a periodic point of ϕ with exact period m. Define the *multiplier* of ϕ at P to be

$$\lambda_\phi(P) := (\phi^m)'(P)$$

For a periodic point P of a map ϕ, if

$\lvert\lambda_\phi(P)\rvert > 1$	P is *repelling*
$\lvert\lambda_\phi(P)\rvert = 1$	P is *indifferent*
$\lvert\lambda_\phi(P)\rvert < 1$	P is *attracting*
$\lvert\lambda_\phi(P)\rvert = 0$	P is a *critical point*

3. Reduction modulo a prime

We begin our discussion of reduction with precise definitions of the reduction of both points and maps modulo a prime. Since these objects are defined via equivalence classes, we must pick the correct representative so that our reduction is well-defined.

3.1. **Definitions.**

We know how to reduce using the map $\pi : \mathbb{Z}_p \to \mathbb{F}_p$. Let us extend this $P \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$, which will reduce to a point $\overline{P} \in \mathbb{P}^1(\overline{\mathbb{F}_p})$. We have to be a little careful, because $\frac{0}{0}$ is not a well-defined point.

DEFINITION 3.1. Let $P \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$. If $P = \infty$, then $\overline{P} = \infty$. Otherwise, we note that $\overline{\mathbb{Q}_p} = \mathrm{Frac}(\overline{\mathbb{Z}_p})$, where $\overline{\mathbb{Z}_p}$ is the integral closure of $\mathbb{Z}_p$ in $\overline{\mathbb{Q}_p}$, and so we may write $P = \frac{a}{b}$ for $a, b \in \overline{\mathbb{Z}_p}$ with $\max(|a|_p, |b|_p) = 1$. Then, $\overline{P} = \frac{\overline{a}}{\overline{b}}$. Note that one of $\overline{a}$ and $\overline{b}$ is nonzero. If $\overline{b} = 0$, then we say $\overline{P} = \infty$.

Remark 3.2. In the above definition, the reduction map is the natural extension of π to a map $\pi : \overline{\mathbb{Z}_p} \to \overline{\mathbb{Z}_p}/p\overline{\mathbb{Z}_p} \cong \overline{\mathbb{F}_p}$. We may also extend the p-adic valuation to $\overline{\mathbb{Z}_p}$, the details of which are in [Gou20].

Now let us move on to rational functions. In a similar fashion as with points, we must pick the correct representation of a rational function so the reduction does not become $\frac{0}{0}$.

DEFINITION 3.3. Let $\phi \in \mathbb{Q}_p(z)$ be a rational function. We may write $\phi = \frac{f}{g}$ for some $f, g \in \mathbb{Q}_p[z]$. We say that f and g are *normalized* if $f, g \in \mathbb{Z}_p[z]$ and at least one coefficient of f or g is not in $p\mathbb{Z}_p$. We call this representation the *normalized form* of ϕ.

If $\phi = \frac{f}{g}$ is in normalized form, we define the *reduction* of ϕ modulo p as $\overline{\phi} = \frac{\overline{f}}{\overline{g}}$, where $\overline{f}$ denotes the polynomial formed by reducing each coefficient modulo p.

Remark 3.4. It is always possible to write a rational function in normalized form.

EXAMPLE 3.5. Let $\phi = \frac{z^2-5z}{z^2-2z-3}$. Note that $\phi \in \mathbb{Q}(z)$, and since $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for any p, we may talk about its reduction in various primes.

- The reduction modulo 5 is $\overline{\phi} = \frac{z^2}{z^2+3z+2}$.

- The reduction modulo 3 is $\overline{\phi} = \frac{z^2+z}{z^2+z} = 1$

In the example above, we see that reducing modulo 3 results in a constant function, whose behavior differs drastically from our original degree 2 rational function. This motivates the following definition:

Definition 3.6. A rational map $\phi \in \mathbb{Q}_p(z)$ is said to have *good reduction* if $\deg \phi = \deg \overline{\phi}$. Otherwise, we say it has *bad reduction*.

As we'll see in Section 4, nice properties hold when ϕ has good reduction: reduction commutes with composition, and periodic points are sent to periodic points.

Our goal in the remainder of this section is to give a criterion for bad reduction. As we note in Example 3.5, while at first, the two polynomials f, g, have no common zeroes, they may pick them up after the reduction. It would then be helpful to utilize the following tool.

3.2. **Resultants.** The resultant is a commonly used tool in both number theory and algebraic geometry. It tells us exactly when two polynomials share a common divisor. It also interacts well with reduction, which allows us to use this tool in the first place.

Definition 3.7. Let A be a ring. Given two polynomials over A, $f = a_n x^n + \cdots + a_1 x + a_0$ and $g = b_m x^m + \cdots + b_1 x + b_0$ with $a_n b_m \neq 0$, the *resultant of f and g* is defined by

$$\mathrm{Res}(f,g) = \det \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & & & & \\ & a_n & a_{n-1} & \dots & a_0 & & & \\ & & \ddots & & & & & \\ & & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & & b_0 & & & \\ & \ddots & & & & & & \\ & & & b_m & b_{m-1} & & \dots & b_0 \end{vmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix} a \\ a \\ \ddots \\ a \end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix} b \\ \ddots \\ b \end{matrix}}\right\} n \end{array}$$

Proposition 3.8. [Lor96, Lemma 2.6] *Let A be a unique factorization domain and $f, g \in A[x]$. Then, f and g have a common divisor if and only if* $\mathrm{Res}(f,g) = 0$.

Proof. Suppose that $h \in A[x]$ is a common divisor of f and g, and we write $f = hu$ and $g = hv$ for some $u, v \in A[x]$. We write $u = c_{n-1}x^{n-1} + \cdots + c_0$ and $v = d_{m-1}x^{m-1} + \cdots + d_0$, where notably, c_{n-1}, d_{m-1} can be zero. Then, the equation $vf - ug = 0$ is the same as

$$\underbrace{\begin{pmatrix} a_n & & & -b_m & & \\ a_{n-1} & \ddots & & -b_{m-1} & \ddots & -b_m \\ \vdots & & a_n & \vdots & & -b_{m-1} \\ & & a_{n-1} & & & \vdots \\ a_0 & & \vdots & -b_0 & & \\ & \ddots & a_0 & & \ddots & -b_0 \end{pmatrix}}_{B} \begin{pmatrix} d_{m-1} \\ \vdots \\ d_0 \\ c_{n-1} \\ \vdots \\ c_0 \end{pmatrix} = \vec{0}$$

We can think of the resulting $n+m$-dimensional vector of the product as representing the coefficient of each x^i in the polynomial $vf - ug$, starting with x^{n+m} in the first entry.

Since we have exhibited a nontrivial vector in the matrix B's nullspace, we conclude that its determinant must be zero. Notice that we may obtain B by negating certain rows followed by the transpose of the matrix defining the resultant. These matrix transformations do not change the matrix determinant if it is zero, and so we conclude that $\operatorname{Res}(f, g) = 0$.

For the converse, we may reverse the steps above. In particular, we may find some vector in the nullspace and use it to construct u and v. Then, we may use polynomial division to find h. In particular, we may consider doing the division in $\operatorname{Frac}(A)[x]$, a Euclidean domain, and by Gauss's lemma, h is in $A[x]$, which gives us a common divisor. $\square$

We are now able to provide the promised characterization of when a rational map has good reduction with this property. The key fact is that the resultant behaves nicely after reduction.

PROPOSITION 3.9. [Sil07, Theorem 2.15] *Let $\phi \in \mathbb{Q}_p(z)$ with normalized form $\frac{f}{g}$. Then, ϕ has good reduction if and only if* $\operatorname{Res}(f, g) \in \mathbb{Z}_p^\times$

Proof. ϕ has bad reduction if and only $\overline{\phi}$ is equal to a rational function with smaller degree. This happens only when $\overline{f}$ and $\overline{g}$ have common roots. By Proposition 3.8, this is true if and only if $\operatorname{Res}(\overline{f}, \overline{g}) = 0$.

Note that the resultant is a sum of products of the coefficients of its input polynomials. Since the reduction map is a homomorphism, we see that $\operatorname{Res}(\overline{f}, \overline{g}) = \overline{\operatorname{Res}(f, g)}$. The reduction is zero if and only if $\operatorname{Res}(f, g) \in \mathbb{Z}_p^\times$. $\square$

This characterization immediately gives us the following corollary on primes of bad reduction. It also showcases the usefulness of considering the reduction of a rational function over $\mathbb{Q}$.

COROLLARY 3.10. *Let $\phi \in \mathbb{Q}(z)$ be a rational function. Then, ϕ has good reduction at all but finitely many primes.*

EXAMPLE 3.11. Continuing with $\phi = \frac{z^2-5z}{z^2-2z-3}$ from Example 3.5, let us compute its resultant.

$$\operatorname{Res}(z^2 - 5z, z^2 - 2z - 3) = \begin{vmatrix} 1 & -5 & 0 & \\ & 1 & -5 & 0 \\ 1 & -2 & -3 & \\ & 1 & -2 & -3 \end{vmatrix} = -36.$$

Thus, we see that ϕ has bad reduction at $p = 2, 3$ and good reduction elsewhere.

4. GOOD REDUCTIONS

In the following section, we consider the case of when ϕ has good reduction. We first consider the exact period of periodic points, and then move on to how a neighborhood of a periodic point, characterized by the multiplier, behaves after reduction.

First, let us establish the fact that dynamics does in fact behave nicely after a reduction.

Proposition 4.1. [Sil07, Theorem 2.18] *Let $\phi \in \mathbb{Q}_p(z)$ be a rational function with good reduction. Then,*

(1) $\overline{\phi}(\overline{P}) = \overline{\phi(P)}$ for all $P \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$
(2) Let $\psi \in \mathbb{Q}_p(z)$ be another rational function with good reduction. Then, $\phi \circ \psi$ has good reduction, and $\overline{\phi \circ \psi} = \overline{\phi} \circ \overline{\psi}$.

Proof. (1) Write $\phi = \frac{f}{g}$ normalized and let $P \in \overline{\mathbb{Q}_p}$. Since the reduction map is a homomorphism, $\overline{f}(\overline{P}) = \overline{f(P)}$ and similarly for g. ϕ has good reduction, so $\overline{f}$ and $\overline{g}$ do not share a common root. Thus, we cannot have $\overline{f(P)} = \overline{g(P)} = 0$, and so we conclude that

$$\overline{\phi(P)} = \frac{\overline{f(P)}}{\overline{g(P)}} = \frac{\overline{f}(\overline{P})}{\overline{g}(\overline{P})} = \overline{\phi}(\overline{P})$$

as desired.

(2) We notice that $\phi \circ \psi$ is already in normalized form. Thus, we can write $\overline{\phi \circ \psi} = \overline{\phi} \circ \overline{\psi}$ since the reduction map is a homomorphism.

The degree of the composition of rational functions is the sum of the degrees. If both ϕ and ψ has good reduction, then

$$\deg(\overline{\phi} \circ \overline{\psi}) = \deg \overline{\phi} + \deg \overline{\psi} = \deg \phi + \deg \psi = \deg(\phi \circ \psi)$$

□

Remark 4.2. The converse of Proposition 4.1(2) is not true. In particular, it might be true that the composition of two maps with bad reduction has good reduction. As an example, consider $\phi = p^2x^2$ and let $\psi = \frac{x^2}{p}$. We see that $\overline{\phi} = 0$ and $\overline{\psi} = \infty$, both constant functions. However, $\overline{\phi \circ \psi} = x^4$, a degree 4 rational function.

4.1. **Reduction of Periodic Points.** In this section, we will showcase some of the results that we may obtain from considering the reductions of the functions, starting from some more immediate results, which we omit the proof of.

Fact 4.3. [Sil07, Corollary 2.20] *Let $\phi \in \mathbb{Q}_p(z)$ be a rational map with good reduction. Periodic points of ϕ reduce to periodic points of $\overline{\phi}$, and preperiodic points of ϕ reduce to preperiodic points of $\overline{\phi}$.*

Fact 4.4. [Sil07, Corollary 2.20] *If P is a periodic point of ϕ with exact period n and its reduction $\overline{P}$ has exact period m for $\overline{\phi}$, then $m|n$.*

We can say something stronger than Fact 4.4 about the exact period of a point, as we'll see in the following theorem. Before we start, let us state without proof some useful lemmas about changing coordinates.

Lemma 4.5. [Sil07, Proposition 2.9] *Let $P, Q \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$ and $h \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$. Then,*

$$\overline{P} = \overline{Q} \iff \overline{h(P)} = \overline{h(Q)}$$

Then, we note that since

Definition 4.6. Let $\phi \in \mathbb{Q}_p(z)$ be a rational function, and let $h \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$ be a fractional linear transformation. Then, define

$$\phi^h := h^{-1} \circ \phi \circ h$$

Lemma 4.7. [Sil07, Proposition 2.11] *Let $P_1, P_2, P_3 \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$ be three distinct points with distinct reductions. Then, there exists a unique $h \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$ such that $h(P_1) = 0, h(P_2) = 1,$ and $h(P_3) = \infty$.*

These lemmas tell us respectively that changing the coordinates does not change the periodicity of the points and that in most cases, we allowed to find the change of coordinates that we are looking for.

The following theorem gives us an explicit relation between the exact period of a point and that of its reduction. Its proof is essentially a (potentially slow) algorithm to recover the exact period of a point given the exact period of its reduction, which is often much easier to find in the finite field $\mathbb{F}_p$.

Theorem 4.8. [Sil07, Theorem 2.21] *Let $\phi \in \mathbb{Q}_p(z)$ be a rational map of degree $d \geq 2$ with good reduction. Let $P \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$ be a periodic point of ϕ. Let m be the exact period of $\overline{P}$. Let r is the (multiplicative) order of $\lambda_{\overline{\phi}}(\overline{P})$ in $\mathbb{F}_p^{\times}$. Then, the exact period of P is one of*

$$m, \qquad mr, \qquad mrp^e$$

for some $e \in \mathbb{Z}, e \geq 1$.

Proof. We can reduce this to the case of P being a fixed point by letting $\psi_0 = \phi^m$. We may also perform a change of coordinates such that $P = 0$, and so we let $\psi = \psi_0^h$. This is helpful as the reduction of 0 is 0.

If $\phi(0) = 0$ then we are in the first case and we are done. Assume otherwise that $\phi(0) \neq 0$. Write $\phi(z) = \frac{a_0 z^d + \cdots + a_0}{b_d z^d + \cdots + b_0}$ where each $a_i, b_i \in \mathbb{Z}_p$.

We know that

$$\overline{\psi}(0) = 0 \implies \psi(0) = \frac{a_0}{b_0} \equiv 0 \mod p$$

Thus, $a_0 \in (p)$, and $b_0 \in \mathbb{Z}_p^{\times}$, otherwise, the reduction is identically zero, contradicting good reduction. Without loss of generality, we may assume $b_0 = 1$. Thus,

$$\psi(z) = \frac{a_0 + a_1 z + \cdots + a_d z^d}{1 + b_1 z + \cdots + b_d z^d}.$$

Consider the Taylor expansion of ϕ around $z = 0$,

$$\psi(z) = a_0 + \psi'(0)z + \frac{A(z)}{1 + zB(z)} z^2$$

where $A(z), B(z) \in \mathbb{Z}_p[x]$. Note that $\lambda_\psi(P) = \psi'(0)$. For ease of notation, let us write this as λ. Let's consider what happens when we iterate ψ twice.

$$\begin{aligned}
\psi^2(0) &= a_0 + \lambda\phi(0) + \frac{A(\phi(0))}{1 + \phi(0)B(\phi(0))}(\phi(0))^2 \\
&= a_0 + \lambda a_0 + \frac{A(a_0)}{1 + a_0 B(a_0)}(a_0)^2
\end{aligned}$$

We note that this is all divisible by $a_0 \in (p)$, so we can't just mod out by p. Let us consider modding out by a_0^2 instead.

$$\psi^2(0) \equiv a_0(1 + \overline{\lambda}) \mod a_0^2$$

Repeating this process until we get to n, we have

$$\psi^n(0) \equiv a_0(1 + \overline{\lambda} + \cdots + \overline{\lambda}^{n-1}) \mod a_0^2$$

Finally, we note that $\psi^n(P) = 0$ as n is the exact period of P. Plugging this in, we conclude that

$$\begin{aligned} 1 + \overline{\lambda} + \cdots + \overline{\lambda}^{n-1} &\equiv 0 \mod a_0 \\ \implies 1 + \overline{\lambda} + \cdots + \overline{\lambda}^{n-1} &\equiv 0 \mod p \end{aligned} \tag{$*$}$$

We thus see from $(*)$ that $\overline{\lambda}^n - 1 \equiv 0 \mod p$.

Case 1: $\overline{\lambda} \neq 1$. Then r, the order of $\overline{\lambda}$ in $\mathbb{F}_p$, divides n. If $n = r$, then we fall into the second case of the theorem and we are done. Otherwise, let us replace $\varphi = \psi^r$ and $n' = n/r$, so P has exact period n' under φ. We may continue doing this kind of substitution until $\overline{\lambda_\varphi(P)} = 1$. Then, we may address this in the following case.
Case 2: $\overline{\lambda} \equiv 1 \mod p$. Plugging $\overline{\lambda} = 1$ into the $(*)$ equation, we have

$$1 + 1 + \cdots + 1 = n \equiv 0 \mod p$$

so $p \mid n$. We then let $\varphi = \psi^p$, $n' = n/p$. We are done if $\varphi(P) = P$. Otherwise, continue iterating until $n' = 1$. Thus, there is some e such that $n = mrp^e$. □

4.2. **Multipliers Post Reductions.** Good reduction imposes pretty stringent conditions on the local behavior of a periodic point, as we shall explore in this section. The observations in this subsection will help us define conditions for when we are allowed to salvage a bad reduction through a change of coordinates.

Proposition 4.9. *If $\phi \in \mathbb{Q}_p(z)$ is a rational function with good reduction, then no periodic point of ϕ is repelling.*

Proof. Let P have exact period n. As before, we may replace ϕ^n with ϕ and assume that P is a fixed point. Then, let us make a change of variables such that $P = 0$. If $\phi = \frac{f}{g}$ in normalized form, then we note that $f(0) = 0$. We may write ϕ as

$$\phi(z) = \frac{f(z)}{g(z)} = \frac{a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

Computing the multiplier, we have

$$\lambda_\phi(P) = \frac{f'(0)g(0) - f(0)g'(0)}{(g(0))^2} = \frac{a_1 b_0}{b_0^2} = \frac{a_1}{b_0}$$

Since ϕ has good reduction, $b_0 \in \mathbb{Z}_p^\times$. Otherwise, z would be a common root of $\overline{f}$ and $\overline{g}$. Taking the absolute value, we have

$$|\lambda_\phi(P)|_v = \left|\frac{a_1}{b_0}\right|_v = |a_1|_v \leq 1$$

and thus no periodic points are repelling. □

Proposition 4.10. [Sil07, Corollary 2.23(a)] [Ben14, Lemma 2.2] *Let $\phi \in \mathbb{Q}_p(z)$ a rational map that has good reduction. If P an attracting fixed point, then for any other fixed point $Q \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$, they do not have the same reduction, i.e. $\overline{P} \neq \overline{Q}$.*

Proof. Perform a change of coordinates such that $P = 0$. Since 0 is a fixed point, we may write $\phi = \frac{f}{g}$ in the normalized form as before:

$$\phi(z) = \frac{f(z)}{g(z)} = \frac{a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

Suppose we have another fixed point x that reduces to 0. Note that the point at infinity cannot reduce to 0, and so we can assume x is an affine point. We must have $|x|_p < 1$. Consider then the absolute value of $\phi(x)$:

$$|\phi(x)|_p = \frac{|a_1 x + \cdots + a_d x^d|}{|b_0 + \cdots + b_d x^d|} = |x| \cdot \frac{|a_1 + \cdots + a_d x^{d-1}|}{|b_0 + \cdots + b_d x^d|}$$

Since ϕ is in normalized form, $|a_i|, |b_i| \leq 1$ for all i. Since ϕ has good reduction, $|b_0| \geq 1$, otherwise the linear term z will be a common factor of f and g. Thus, the absolute value of the denominator is

$$|b_0 + \cdots + b_d x^d| = \max(b_0, b_1 x, \ldots, b_d x^d) = 1$$

Since 0 is an attracting point,

$$1 > |\lambda_0(\phi)| = |\lambda_0(f)| = |a_1|$$

Thus, we conclude that

$$\frac{|a_1 + \cdots + a_d x^{d-1}|}{|b_0 + \cdots + b_d x^d|} = |a_1 + \cdots + a_d x^{d-1}| \leq |a_1| < 1$$

which implies that $|\phi(x)| = |x| < |x|$, a contradiction. ☐

The following, while a result about the local behavior of a periodic point, will be most useful as a lemma for the proof of Theorem 5.3.

Lemma 4.11. [Ben14, Lemma 2.3] *Let $\phi \in \mathbb{Q}_p(z)$ a rational function with good reduction and $\deg \phi \geq 2$. Let $P \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$ be an indifferent fixed point. Then,*

(1) $\phi^{-1}(P) \setminus \{P\}$ is nonempty, i.e. there exists at least one point $Q \in \mathbb{P}^1(\overline{\mathbb{Q}_p})$ such that $\phi(Q) = P$.
(2) for all $Q \in \phi^{-1}(P)$, $Q \neq P$, we have $\overline{Q} \neq \overline{P}$

Proof. (1) As before, perform a change of coordinates such that $P = 0$, then write $\phi = \frac{f}{g}$ in normalized form. We are looking for a point y such that $\phi(y) = 0$. Thus, y must be a root of f. Furthermore, since x is indifferent and thus not a critical point, the derivative of f at 0 must be nonzero. Thus, 0 is not a repeated root of f. Since the degree of f is at least 2, there must be another distinct root of f.

(2) We must show that f has no roots in $(p) \setminus \{0\}$. We note that we can write f as

$$f(z) = z(a_1 + \cdots + a_d z^{d-1})$$

If we have $f(z) = 0$ for some z, then we would expect the absolute value of the right hand side to be zero. However, from the proof of Proposition 4.9, we know that $|a_1| = 1$. Thus, $|a_1 + \cdots + a_d z^{d-1}| \geq 1 > 0$, a contradiction. ☐

5. Potentially good reductions

As we saw, good reduction is nice. Sometimes, bad reduction may be fixed simply by a change of coordinates. This is called potentially good reduction. In this section, we will look at an algorithm by [Ben14] which allows to determine when a rational function has potentially good reduction.

Definition 5.1. A rational function $\phi \in \mathbb{Q}_p(z)$ has *potentially good reduction* if there exists some $h \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$ such that ϕ^h has good reduction.

Before proving the theorem, let us quickly state and prove a lemma about the fixed points of a rational function.

LEMMA 5.2. *Let $\phi \in \mathbb{Q}_p(z)$ with degree d.*

(1) ϕ has $d+1$ fixed points, counted with multiplicity.
(2) the multiplicity of a fixed point x is more than 1 if and only if $\lambda_x(\phi) = 1$.

Proof. *(1)* Let $\phi = \frac{f}{g}$, $f, g \in \mathbb{Z}_p[x]$ polynomials of degree d. Then, the fixed points are simply the roots of the following polynomial:

$$f(x) - xg(x)$$

This is a degree $d+1$ polynomial. After dehomogenizing, we conclude that there are $d+1$ fixed points of ϕ, counted with multiplicity.

(2) Let $\Phi(z) = \phi(z) - z$. Then,

$$\Phi'(z) = \phi'(z) - 1.$$

x is a double root of $\Phi(z)$ if and only if it is the root of $\Phi'(z)$ as well. Thus, $\lambda_x(\phi) = 1 \iff x$ is a fixed point with multiplicity more than 1. □

It is easy to check whether a rational function has good reduction. The following theorem will provide with an algorithm that tells us how to check if a rational function has potentially good reduction by finding one, and only one, candidate conjugate to check for good reduction.

THEOREM 5.3. [Ben14, Main Theorem] *Let $\phi \in \mathbb{Q}_p(z)$ with degree greater than 2. Let its fixed points be $x_1, \dots, x_{d+1}$, repeated with multiplicity. Then,*

(1) if any of the x_i are repelling, then ϕ does not have potentially good reduction.
(2) if x_i is indifferent for some i, then we may pick $y_1 \in \phi^{-1}(x_i) \setminus \{x_i\}$ and $y_2 \in \phi^{-1}(y_1)$, and x_i, y_1, y_2 are distinct. By 4.7, we may let $h \in PGL_2(\overline{\mathbb{Q}_p})$ such that $h(x_i) = 0, h(y_1) = 1, h(y_2) = \infty$. Then, the map ϕ^h has good reduction if and only if ϕ has potentially good reduction.
(3) Otherwise, all fixed points are attracting points. We may pick three distinct points, without loss of generality say x_1, x_2, x_3. Let $h \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$ such that $h(x_1) = 0, h(x_2) = 1, h(x_3) = \infty$. Then, ϕ^h has good reduction if and only if ϕ has potentially good reduction.

Proof. *(1)* follows from Proposition 4.9. Otherwise, let $\lambda_i = \lambda_{x_i}(\phi)$ for each i.

In the case of *(2)*, that is, $|\lambda_i| = 1$ for some i, then we may apply Lemma 4.11(1) to pick $y_1 \in \phi^{-1}(x_i) \setminus \{x_i\}$. Let $y_2 \in \phi^{-1}(y_1)$. Note that $y_2 \neq y_1$, otherwise

$$y_1 = \phi(y_2) = \phi(y_1) = x$$

and we picked $y_1 \neq x$. Lastly, note that $y_2 \neq x_i$ either, by a similar argument.

Let h be defined as in the theorem statement. If ϕ^h has good reduction, then by definition, ϕ has potentially good reduction. On the other hand, if ϕ has potentially good reduction, then let $\tilde{h} \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$ such that $\phi^{\tilde{h}}$ has good reduction.

Since $\tilde{h}$ preserves fixed points and multipliers, $g(x_i)$ is also an indifferent fixed point of $\phi^{\tilde{h}}$, and $\tilde{h}(y_1) \in (\phi^{\tilde{h}})^{-1}(\tilde{h}(x_i))$. By Lemma 4.11(2), $\overline{\tilde{h}(x_i)} \neq \overline{\tilde{h}(y_1)}$. Then, since $\phi^{\tilde{h}}$ has good reduction,

$$\overline{\phi^{\tilde{h}}}(\overline{\tilde{h}(y_2)}) = \overline{\phi^{\tilde{h}}(\tilde{h}(y_2))} = \overline{\tilde{h} \circ \phi \circ \tilde{h}^{-1} \circ \tilde{h}(y_2)} = \overline{\tilde{h}(y_1)}$$

Thus, we may apply the same argument as before to show that the reductions of $\tilde{h}(x_i), \tilde{h}(y_1)$, and $\tilde{h}(y_2)$ are all distinct. Thus, there is some $r \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$ such that sends $\tilde{h}(x_i), \tilde{h}(y_1)$, and $\tilde{h}(y_2)$ to $0, 1, \infty$ respectively.

Since these transformations are unique, we must have $h = r \circ \tilde{h}$. Then, we may write $\phi^h = r \circ \phi^{\tilde{h}} \circ r^{-1}$. We note that since $\phi^{\tilde{h}}, r, r^{-1}$ has good reduction, ϕ^h has good reduction.

(3) Lastly, let us assume that no x_i are repelling or indifferent. They must then be all attracting, and so $|\lambda_i| < 1$. Then, by Lemma 5.2(2), none of the x_i's are repeated. Thus, x_1, x_2, x_3 are all distinct, and we may define h as outlined in the theorem statement.

If ϕ has potentially good reduction, let $\tilde{h}$ be such that $\phi^{\tilde{h}}$ has good reduction. Since conjugation does not change multipliers, $\tilde{h}(x_i)$ is still an attracting point for $i \in \{1, 2, 3\}$. We may then apply Proposition 4.10 to conclude that they do not have the same reduction.

Thus, there is some map $r \in \mathrm{PGL}_2(\overline{\mathbb{Q}_p})$ with good reduction that maps these points to $0, 1, \infty$ respectively. Then, we conclude that $h = r \circ \tilde{h}$ and so $\phi^h = r \circ \phi^{\tilde{h}} \circ r^{-1}$ has good reduction as well. $\square$

EXAMPLE 5.4. Let us check if $\phi = \frac{z^2-5z}{z^2-2z-3}$ has potentially good reduction at the prime 3. The polynomial

$$z^2 - 5z - z(z^2 - 2z - 3) = 0$$

has solutions $z = 0, 1, 2$. We then note that 0 is a repelling point:

$$\phi'(0) = \frac{3(0^2 - 2 \cdot 0 + 5)}{(0^2 - 2 \cdot 0 - 3)^2} = \frac{5}{3}$$

Since $|\frac{5}{3}|_3 = 3 > 1$.

References

[AM16] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[Ben14] Robert L. Benedetto. A criterion for potentially good reduction in nonarchimedean dynamics. *Acta Arith.*, 165(3):251–256, 2014.

[BR10] Matthew Baker and Robert Rumely. *Potential theory and dynamics on the Berkovich projective line*, volume 159 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2010.

[Gal11] Jean Gallier. *Geometric methods and applications*, volume 38 of *Texts in Applied Mathematics*. Springer, New York, second edition, 2011. For computer science and engineering.

[Gou20] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer, Cham, third edition, [2020] ©2020. An introduction.

[Lor96] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[Sil07] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Email address: pengs14@mit.edu