Minimality criteria for rational maps with good reduction on the projective line over $\mathbb{Q}_p$

Sangtae Jeong

Department of Mathematics

Inha University

stj@inha.ac.kr

p-adic Mathematical Physics and its Applications
Web Conference May 17-28, 2021

May 25, 2021

Outline

1. Introduction
2. Two systems on the p-adic setting
3. Minimal criterion for series over $\mathbb{Z}_p$
4. Minimality criterion for rational maps with good reduction on $\mathbb{P}^1(\mathbb{Q}_p)$

Goal of the Talk

• In this talk, we provide the minimality criterion for a rational map of degree at least 2 with good reduction on the projective line $\mathbb{P}^1(\mathbb{Q}_p)$ over $\mathbb{Q}_p$. This criterion enables us to obtain a complete description of minimal conditions for such a map on $\mathbb{P}^1(\mathbb{Q}_p)$ in terms of its coefficients for $p = 2$ or 3. For an arbitrary prime $p \geq 5$, we present a method of characterizing minimal rational maps ϕ of degree ≥ 2 on $\mathbb{P}^1(\mathbb{Q}_p)$, provided that the prescribed conditions for the reduction of ϕ on $\mathbb{P}^1(\mathbb{F}_p)$ to be transitive are known.
As a prerequisite we characterize the minimality criterion for a convergent power series f on $\mathbb{Z}_p$ in terms of its coefficients for an arbitrary prime p.

• This is a joint work with Dohyun Ko, Yongjae Kwon and Youngwoo Kwon.

p-adic measurable dynamical systems on $\mathbb{Z}_p$

What are p-adic dynamical systems?

(1) p-adic measurable dynamical system on $\mathbb{Z}_p$:
It is made up of a triple $(\mathbb{Z}_p, f, \mu)$ where
$-\mathbb{Z}_p$ is the ring of p-adic integers equipped with the p-adic absolute value $|x| := |x|_p = p^{-v_p(x)}$ where $v_p(x)$ is the p-adic valutation on $\mathbb{Z}_p$. Denote by $\mathbb{Q}_p$ the quotient field of $\mathbb{Z}_p$.
$-f$: a measurable(continuous) function $f : \mathbb{Z}_p \to \mathbb{Z}_p$.
$-\mu$: a normalized measure on $\mathbb{Z}_p$ so that $\mu(\mathbb{Z}_p) = 1$.
Note that the measure of a ball of the form $a + p^n\mathbb{Z}_p$ is defined as its radius: $\mu_p(a + p^n\mathbb{Z}_p) = 1/p^n$.

p-adic topological dynamical systems on $\mathbb{P}^1(\mathbb{Q}_p)$:

(2) p-adic topological dynamical systems on $\mathbb{P}^1(\mathbb{Q}_p)$:
It consists of $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ where
-$\mathbb{P}^1(\mathbb{Q}_p)$ is the projective line over $\mathbb{Q}_p$ equipped with the p-adic chordal metric ρ defined as follows: for $P = [x_0, x_1]$ and $Q = [y_0, y_1] \in \mathbb{P}^1(\mathbb{Q}_p) = \mathbb{Q}_p \cup \{\infty\}$,

$$\rho(P, Q) = \frac{|x_0 y_1 - x_1 y_0|}{\max\{|x_0|, |x_1|\}\max\{|y_0|, |y_1|\}}.$$

Note that for $z_0, z_1 \in \mathbb{Z}_p, \rho(z_0, z_1) = |z_0 - z_1|$.
- ϕ is a rational map in $\mathbb{Q}_p(z)$.

1-Lipschitz functions

Definition

(1) A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be 1-Lipschitz continuous if $|f(x) - f(y)| \leq |x - y|$ for all $x, y \in \mathbb{Z}_p$.
(2) A map $\phi : \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{P}^1(\mathbb{Q}_p)$ is said to be 1-Lipschitz continuous if
$\rho(\phi(P), \phi(Q)) \leq \rho(P, Q)$ holds for all $P, Q \in \mathbb{P}^1(\mathbb{Q}_p)$.

Then, every 1-Lipschitz function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ induces a sequence of reduced functions, f_n $(n \geq 1)$, on quotient rings defined by
$f_n : \mathbb{Z}_p/p^n\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$, $x + p^n\mathbb{Z}_p \mapsto f(x) + p^n\mathbb{Z}_p$.

- Examples of 1-Lipschitz functions on $\mathbb{Z}_p$.

$$\mathbb{Z}[x] \subset \mathbb{Z}_p[x] \subset \mathbb{Z}_p\langle\langle z\rangle\rangle \subset \mathbf{B}(\mathbb{Z}_p) \subset Lip_1(\mathbb{Z}_p),$$

where $\mathbb{Z}_p\langle\langle z\rangle\rangle :=$ the set of analytic functions on $\mathbb{Z}_p$ in $\mathbb{Z}_p[[x]]$,
$\mathbf{B}(\mathbb{Z}_p) := \{f(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m} : \frac{a_m}{m!} \in \mathbb{Z}_p, \quad m = 0, 1, \cdots\}$.

Reduced functions of a 1-Lipschitz function on $\mathbb{P}^1(\mathbb{Q}_p)$

$\mathbb{P}^1(\mathbb{Q}_p)$ consists of the set of $(p+1)p^n$ disjoint balls $B_n(x)$ of radius p^{-n} defined by

$$B_n(x) := \left\{z \in \mathbb{P}^1(\mathbb{Q}_p) \,\middle|\, \rho(z,x) \le p^{-n}\right\}.$$

$\mathfrak{B}_n$ denotes the set of such balls.
Note that as $\mathbb{P}^1(\mathbb{Q}_p)$ is an infinite tree, for each n, there is a one-to-one correspondence between the set $\mathfrak{B}_n$ and the set of vertices of the tree at level n.
Every 1-Lipschitz continuous map $\phi : \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{P}^1(\mathbb{Q}_p)$ induces a sequence of reduced transformations $\phi_n : \mathfrak{B}_n \to \mathfrak{B}_n$ defined by:

$$\phi_n(B_n(x)) = B_n(\phi(x)) \text{ for all } x \in \mathbb{P}^1(\mathbb{Q}_p).$$

Basic properties of convergent series in $\mathbb{Z}_p\langle\langle z\rangle\rangle$

The basic properties for $\mathbb{Z}_p\langle\langle z\rangle\rangle$ can be summarized in the following proposition.

1. Each series in $\mathbb{Z}_p\langle\langle z\rangle\rangle$ is a 1-Lipchitz function on $\mathbb{Z}_p$.
2. $\mathbb{Z}_p\langle\langle z\rangle\rangle$ is closed under addition, multiplication, differentiation, and composition.
3. Each $f \in \mathbb{Z}_p\langle\langle z\rangle\rangle$ has a Taylor expansion at any $x \in \mathbb{Z}_p$; i.e.,

$$f(x+z) = \sum_{m=0}^{\infty} \frac{f^{(m)}(x)}{m!} z^m,$$

   where $\frac{f^{(m)}(x)}{m!}$ is a p-adic integer for all $m \geq 0$.
4. $\mathbf{Q}_p\langle\langle z\rangle\rangle$ is a complete normed space with respect to the sup-norm $\|\cdot\|$.
5. p-adic division algorithm for $Z_p\langle\langle z\rangle\rangle$ works.
6. p-adic Weierstrass preparation theorem for $Z_p\langle\langle z\rangle\rangle$ holds.

Terminologies in p-adic dynamical systems

[Definition] Let $(\mathbb{Z}_p, f, \mu_p)$ be a p-adic dynamical system on $\mathbb{Z}_p$.
(1) A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be measure-preserving if $\mu_p(f^{-1}(M)) = \mu_p(M)$ for each measurable subset $M \subset \mathbb{Z}_p$.

(2) A measure-preserving function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be ergodic if it has no proper invariant subsets (i.e., either $\mu_p(M) = 1$ or $\mu_p(M) = 0$ holds for any measurable subset, $M \subset \mathbb{Z}_p$, such that $f^{-1}(M) = M$).

[Definition] Let $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ be a topological dynamical system. Let E be a ϕ-invariant set (i.e. $\phi(E) \subset E$). The subsystem (E, ϕ) is said to be minimal if the orbit of x under ϕ is dense in E for all $x \in E$.

Basic facts in p-adic dynamical systems

Proposition 1. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function. Then, the following are equivalent:
(1) $(\mathbb{Z}_p, f)$ is minimal;
(2) $(\mathbb{Z}_p/p^n\mathbb{Z}_p, f_n)$ is minimal for all integers, $n \geq 1$;
(3) f is ergodic.

In particular, if f is a convergent series in $\mathbb{Z}_p[[x]]$, then $(\mathbb{Z}_p, f)$ is minimal if and only if $(\mathbb{Z}_p/p^\mu\mathbb{Z}_p, f_\mu)$ is minimal where $\mu = \mu(p) = 3$ if $p = 2, 3$ and $\mu = 2$ if $p \geq 5$.

Proposition 1'[Fan-Fan-Liao-Wang, 2017]
Let $\phi : \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{P}^1(\mathbb{Q}_p)$ be a 1-Lipschitz continuous map. Then $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ is minimal if and only if the finite system $(\mathfrak{B}_n, \phi_n)$ is minimal for all integers $n \geq 1$.

In particular, if ϕ is a rational map on $\mathbb{P}^1(\mathbb{Q}_p)$ with good reduction, then $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ is minimal if and only if $(\mathfrak{B}_\mu, \phi_\mu)$ is minimal where μ is as in the above.

Basic facts in p-adic dynamical systems

An efficient minimality criterion for a convergent series in $\mathbb{Z}_p\langle\langle x\rangle\rangle$ is known.

Proposition 2. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a convergent series in $\mathbb{Z}_p\langle\langle x\rangle\rangle$ satisfying that $(\mathbb{Z}_p/p^n\mathbb{Z}_p, f_n)$ is minimal for $n \geq 1$. Then, the followings are equivalent:
(1) $\left(\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p, f_{n+1}\right)$ is minimal;
(2) For all $x \in \mathbb{Z}_p$, we have that $f^{p^n}(x) - x \notin p^{n+1}\mathbb{Z}_p$ and $\left(f^{p^n}\right)'(x) \in 1 + p\mathbb{Z}_p$; and
(3) There exists $x \in \mathbb{Z}_p$ such that $f^{p^n}(x) - x \notin p^{n+1}\mathbb{Z}_p$, and $\left(f^{p^n}\right)'(x) \in 1 + p\mathbb{Z}_p$.

This is the case where the cycle σ of length p^n that arises from f_n, grows in the well known linearization arguments for minimality. The analogue for a rational map with good reduction on $\mathbb{P}^1(\mathbb{Q}_p)$ also works.

Another minimality criterion for p-adic series in $\mathbb{Z}_p\langle\langle z\rangle\rangle$

For a prime p, we set

$$\mu := \mu(p) = 3 \ \text{ if } p \in \{2,3\}; 2 \text{ otherwise.}$$

$$\delta(z) := \delta_p(z) = \begin{cases} \binom{z}{p^2} & \text{if } p \in \{2,3\}; \\ \binom{z}{2p} & \text{if } \ p \geq 5. \end{cases}$$

Theorem

Let $f(z) \in \mathbb{Z}_p\langle\langle z\rangle\rangle$ be a convergent series. Then f is minimal on $\mathbb{Z}_p$ if and only if the reduction of $f(z)$ modulo $\delta(z)$ is minimal on $\mathbb{Z}_p$.

Proof. Use the p-adic division algorithm for convergent series in $\mathbb{Z}_p\langle\langle z\rangle\rangle$ to write $f(z) = (\deg\delta)!q(z)\,\delta(z) + r(z)$.
It follows from Proposition 1 by observing that $p^\mu|(\deg\delta)!$.

Complete minimality criterion for various functions over $\mathbb{Z}_2$

Theorem.(Larin) A polynomial,
$f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbb{Z}_2[x]$, is minimal if and only if the system of the following relations is fulfilled:

$$\begin{aligned} a_0 &\equiv 1 \pmod 2; \\ a_1 &\equiv 1 \pmod 2; \\ A_1 - a_1 &\equiv 2a_2 \pmod 4; \textit{ and} \\ A_0 &\equiv a_1 + 2a_2 - 1 \pmod 4. \end{aligned}$$

⇔

f_3 is minimal
⇕
- $f(0) \equiv 1$ (2)
- $f(1) \equiv 0$ (2)
- $(f^2)'(0) \equiv 1$ (2)
- $f^2(0) \in 2\mathbb{Z}_2 \setminus 4\mathbb{Z}_2$
- $f^4(0) \in 4\mathbb{Z}_2 \setminus 8\mathbb{Z}_2$

• Durand and Paccaut presented a minimal criterion for polynomials over $\mathbb{Z}_2$, equivalent to that of Larin.
• Anashin characterized the minimality for convergent series over $\mathbb{Z}_p$. In general, he gave a complete minimal criterion for 1-Lipschitz functions in terms of the Mahler expansion coefficients.

Complete minimality criterion for convergent series over $\mathbb{Z}_3$

• Durand and Paccaut presented a minimal criterion for polynomials f over $\mathbb{Z}_3$, under the assumption that $f(0) = 1$.

For a convergent series, $f(z) = \sum a_n z^n \in \mathbb{Z}_3\langle\langle z\rangle\rangle$, set

$$A_0 := \sum_{i \equiv 0 \pmod 2, i>0} a_i, \; A_1 := \sum_{i \equiv 1 \pmod 2} a_i;$$

$$D_0 := \sum_{i \equiv 0 \pmod 2, i>0} i a_i, \; D_1 := \sum_{i \equiv 1 \pmod 2} i a_i.$$

Set $D_1' = D_0 + D_1, D_2' = -D_0 + D_1$.

Minimality criterion for convergent series over $\mathbb{Z}_3$

Theorem

A convergent series $f(z) = \sum a_n z^n \in \mathbb{Z}_3\langle\langle z \rangle\rangle$, is minimal if and only if f fulfills one of the conditions (i)–(viii):
Setting $[a_0, A_1, A_0, a_1, D_1', D_2'] \bmod 3 = [\cdot, \cdot, \cdots, \cdot]$,

(i) $[1, 1, 0, 1, 1, 1]$,
$A_0 + 6 \not\equiv 0\ [9],\ A_0 + 6 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+2}\ [9]$;

(ii) $[1, 1, 0, 1, 2, 2]$,
$A_1 + a_0 + 4 \not\equiv 0\ [9],\ A_1 + a_0 + 4 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+5}\ [9]$;

(iii) $[1, 1, 0, 2, 1, 2]$,
$A_1 + 2a_0 + 3 \not\equiv 0\ [9],\ A_1 + 2a_0 + 3 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+5}\ [9]$;

(iv) $[1, 1, 0, 2, 2, 1]$,
$A_0 + 2a_0 + 4 \equiv 0\ [9],\ A_0 + 2a_0 + 4 \not\equiv 3a_2 + 6\sum_{j\geq 0} a_{6j+2}\ [9]$;

Minimality criterion for convergent series over $\mathbb{Z}_3$

(Continued) There are 4 more cases.

Theorem

(v) $[2, 1, 0, 1, 1, 1]$,
$A_0 + 3 \not\equiv 0\ [9],\ A_0 + 3 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+2}\ [9]$;

(vi) $[2, 1, 0, 1, 2, 2]$,
$A_1 + 2a_0 + 7 \not\equiv 0\ [9],\ A_1 + 2a_0 + 7 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+5}\ [9]$;

(vii) $[2, 1, 0, 2, 1, 2]$,
$A_0 + 2a_0 + 5\ \not\equiv 0\ [9],\ A_0 + 2a_0 + 5 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+2}\ [9]$;

(viii) $[2, 1, 0, 2, 2, 1]$,
$A_1 + a_0 + 6 \not\equiv 0\ [9],\ A_1 + a_0 + 6 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+5}\ [9]$.

• There are terms of higher powers of a_0 in the DP's criterion for a polynomial f with $f(0) \neq 1$ because $g(x) = \frac{f(a_0x)}{a_0}$.

Idea of proof for the case $p = 3$ and general cases

Lemma A. Let f be a convergent series over $\mathbb{Z}_3$. Then, f is minimal if and only if the following conditions are satisfied:

(M1) $f_{/1}$ is transitive (i.e., f is transitive modulo 3);
(M2) $(f^3)'(0) \equiv 1 \pmod 3$;
(M3) $f^3(0) \in 3\mathbb{Z}_3 \setminus 9\mathbb{Z}_3$; and
(M4) $3(f^3)''(0) - 2f^3(0) \not\equiv 0 \pmod 9$.

• Use the arguments in Linear Algebra to decompose f into a sum of the form $f(x) = r(x) + 3h(x)$.

Remark. p-adic Weierstrass preparation theorem enables us to adapt this method to the general primes $p \geq 5$, along with the following

Lemma B. A convergent series, $f \in \mathbb{Z}_p\langle\langle z \rangle\rangle$, is minimal if and only if the following conditions are satisfied:
(E1) f is transitive modulo p;
(E2) $(f^p)'(0) \equiv 1 \pmod p$; *and*
(E3) $f^p(0) \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$.

Minimality criterion for convergent series over $\mathbb{Z}_p$ for $p \geq 5$

Theorem

Let $f \in \mathbb{Z}_p\langle\langle z\rangle\rangle$ be a convergent series of the form $f(z) = g(z) + ph(z)$, of widegree N, and of norm 1. Then f is minimal on $\mathbb{Z}_p$ if and only if the following conditions are satisfied:

1. *$g(x)$ is a transitive polynomial modulo p of degree N, of which the full cycle is given by $(\xi_0, \xi_1, \cdots, \xi_{p-1})$ where $\{\xi_0 := 0, \xi_1, \cdots, \xi_{p-1}\} = \mathbb{F}_p$;*
2. $$\prod_{i=0}^{p-1} g'(i) \equiv 1 \pmod{p};$$ *and*
3. $$\sum_{i=1}^{p}(g(\xi_{i-1}) - \xi_i)w_i + p\sum_{i=1}^{p} h(\xi_{i-1})w_i \not\equiv 0 \pmod{p^2},$$ *where* $w_i = \prod_{j=i}^{p-1} g'(\xi_j)$ for $1 \leq i \leq p-1$, $w_p = 1$ and $\xi_p = 0$.

Several corollaries

Corollary (For later use, referred to as Corollary 1)

The dynamical system $(p\mathbb{Z}_p, \phi^{p+1} = \sum_{i=0}^{\infty} \lambda_i z^i)$ *is minimal if and only if* $(\mathbb{Z}_p, \chi = \sum_{i=0}^{\infty} u_i z^i)$ *is minimal, where* $u_i = p^{i-1}\lambda_i$ *for all* $i \geq 0$. *(Note that* $(p\mathbb{Z}_p, \phi^{p+1})$ *is conjugate to* $(\mathbb{Z}_p, \chi = \sum_{i=0}^{\infty} u_i z^i)$ *by the transformation* $\eta(z) = z/p$.*)*

(i) for $p = 2$,

$u_0 \equiv 1 (\bmod p), u_1 \equiv 1 \pmod p, u_3 \equiv 2u_2 \pmod{p^2}$.

$\Leftrightarrow \lambda_0/p \equiv 1 \pmod p, \lambda_1 \equiv 1 \pmod p, \lambda_1 + 2\lambda_2 \equiv 1 \pmod{p^2}$.

(ii) for $p = 3$,

$u_0 \not\equiv 0 \pmod p, \quad u_1 \equiv 1 \pmod p, \quad u_2/p \not\equiv u_0 \pmod p$.

$\Leftrightarrow \lambda_0/p \not\equiv 0 \pmod p, \quad \lambda_1 \equiv 1 \pmod p \quad \lambda_2 \not\equiv \lambda_0/p \pmod p$.

(iii) for $p \geq 5$,

$u_0 \not\equiv 0 \pmod p, \quad u_1 \equiv 1 \pmod p$.

$\Leftrightarrow \lambda_0/p \not\equiv 0 \pmod p, \quad \lambda_1 \equiv 1 \pmod p$.

Several corollaries

Corollary

Let $f(z) = \sum_{n\geq 0} a_n z^n \in \mathbb{Z}_p\langle\langle z\rangle\rangle$ be a convergent series that satisfies the following system of relations:

$$\begin{cases} a_0 \not\equiv 0 \pmod{p}; \\ a_1 \equiv 1 \pmod{p}; \\ a_i \equiv 0 \pmod{p} \text{ for } i \geq 2; \text{ and} \\ \displaystyle\sum_{\substack{i\in(p-1)\mathbb{Z} \\ i\neq 0}} a_i \not\equiv pa_0 \pmod{p^2}. \end{cases}$$

Then, f is minimal on $\mathbb{Z}_p$.

This is a generalization of minimal conditions for polynomials in $\mathbb{Z}_p[z]$ that was proved by M. Javaheri and G. Rusak whose proof is based on the power sum involving the Bernoulli numbers.

Rational maps with good reduction

Any rational map ϕ on $\mathbb{P}^1(\mathbb{Q}_p)$ of degree $d \geq 2$ is expressed as a quotient of two polynomials f and g in $\mathbb{Z}_p[z]$ with no common roots, such that at least one coefficient of f or g is a unit in $\mathbb{Z}_p$.
[**Definition**] A rational map ϕ has good reduction if $\deg(\phi) = \deg(\bar{\phi})$, where the reduced rational function $\bar{\phi}$ is defined as $\bar{\phi} = \frac{\bar{f}}{\bar{g}}$, where $\bar{h} \in \mathbb{F}_p[z]$ is the reduced polynomial of $h \in \mathbb{Z}_p[z]$ modulo p.

Proposition

If ϕ is a rational map with good reduction on $\mathbb{P}^1(\mathbb{Q}_p)$, then it is 1-Lipschitz continuous , that is, ϕ satisfies the following inequality with a Lipschitz constant 1, for all $P, Q \in \mathbb{P}^1(\mathbb{Q}_p)$,
$\rho(\phi(P), \phi(Q)) \leq \rho(P, Q)$.

For a proof see [Theorem 2.17] in Silverman's book, the arithmetic of dynamical systems.

Minimal criteria for rational maps with good reduction

If a rational map $\phi \in \mathbb{Q}_p(z)$ has good reduction, then the reduced rational map $\bar{\phi} \in \mathbb{F}_p(z)$ induces a map on $\mathbb{P}^1(\mathbb{F}_p)$, the projective line over $\mathbb{F}_p$.

Theorem (Fan-Fan-Liao-Wang, 2017)

Let $\phi \in \mathbb{Q}_p(z)$ be a rational map of $\deg \phi \geq 2$ with good reduction. Then the dynamical system $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ is minimal if and only if the following conditions are satisfied:

1. *the reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbb{F}_p)$;*
2. $(\phi^{p+1})'(0) \equiv 1 \pmod{p}$ *and* $|\phi^{p+1}(0)| = 1/p$; *and*
3. *additionally, for the cases of $p = 2$ or 3,*

$$|\phi^{(p+1)p}(0)| = 1/p^2.$$

Minimal criteria for rational maps with good reduction

Theorem (JKKK,2021)

Let $\phi \in \mathbb{Q}_p(z)$ be a rational map of $\deg \phi \geq 2$ with good reduction. Then the dynamical system $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ is minimal if and only if the following conditions are satisfied:

1. *the reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbb{F}_p)$;*
2. $(\phi^{(p+1)})'(0) \equiv 1 \pmod{p}$ *and* $|\phi^{(p+1)}(0)| = 1/p$; *and*
3. *additionally,*
   for $p = 2$, $(\phi^{(p+1)})'(0) + (\phi^{(p+1)})''(0) \equiv 1 \pmod{p^2}$;
   for $p = 3$, $\frac{1}{p}\phi^{(p+1)}(0) - \frac{1}{2}(\phi^{(p+1)})''(0) \not\equiv 0 \pmod{p}$.

Note that condition (3), $|\phi^{(p+1)p}(0)| = 1/p^2$, of the previous Theorem[FFLW] is replaced by a simper condition involving the first and second derivatives of $\phi^{(p+1)}(z)$ at $z = 0$.

Sketchy proof of the main result

For sufficiency, note that cond.(1) implies that $\phi^{p+1} = \sum_{i=0}^{\infty} \lambda_i z^i$ is 1-Lipschitz continuous on $p\mathbb{Z}_p$.
It suffices to show that the dynamical system $(p\mathbb{Z}_p, \phi^{p+1} = \sum_{i=0}^{\infty} \lambda_i z^i)$ is minimal. Equivalently, the system $(\mathbb{Z}_p, \chi = \sum_{i=0}^{\infty} u_i z^i)$ is minimal. From Corollary 1, by noting that $\lambda_0 = \phi^{p+1}(0), \lambda_1 = (\phi^{p+1})'(0), \lambda_2 = \frac{1}{2}(\phi^{p+1})''(0)$.
the minimal conditions for χ (hence ϕ^{p+1}) are,
for $p = 2, u_0 \equiv 1 (\mathrm{mod}\ p), u_1 \equiv 1\ (\mathrm{mod}\ p), u_3 \equiv 2u_2\ (\mathrm{mod}\ p^2)$.
$\Leftrightarrow$ $\boxed{\lambda_0/p \equiv 1\ (\mathrm{mod}\ p), \lambda_1 \equiv 1\ (\mathrm{mod}\ p)}$, $\boxed{\lambda_1 + 2\lambda_2 \equiv 1\ (\mathrm{mod}\ p^2)}$.
for $p = 3, u_0 \not\equiv 0\ (\mathrm{mod}\ p), u_1 \equiv 1\ (\mathrm{mod}\ p), u_2/p \not\equiv u_0\ (\mathrm{mod}\ p)$.
$\Leftrightarrow$ $\boxed{\lambda_0/p \not\equiv 0\ (\mathrm{mod}\ p), \quad \lambda_1 \equiv 1\ (\mathrm{mod}\ p)}$, $\boxed{\lambda_2 \not\equiv \lambda_0/p\ (\mathrm{mod}\ p)}$.
for $p \geq 5, u_0 \not\equiv 0\ (\mathrm{mod}\ p), \quad u_1 \equiv 1\ (\mathrm{mod}\ p)$.
$\Leftrightarrow$ $\boxed{\lambda_0/p \not\equiv 0\ (\mathrm{mod}\ p)}$. $\quad \boxed{\lambda_1 \equiv 1\ (\mathrm{mod}\ p)}$.

Sketchy proof of the main result

The necessity follows from the following fact of Fan et al.

Theorem [Fan-Fan-Liao-Wang, 2017]. Let $\phi : \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{P}^1(\mathbb{Q}_p)$ be a rational function with good reduction. Then
(i) $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ is minimal if and only if
(ii) $(\mathfrak{B}_\mu, \phi_\mu)$ is minimal where $\mu = \mu(p) = 3$ if $p = 2, 3$ and $\mu = 2$ if $p \geq 5$.

By (ii), the minimality of $(\mathfrak{B}_1, \phi_1)$ implies that the reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbb{F}_p)$, which is assertion(1). It also yields a convergent series $\phi^{p+1}(z) = \lambda_0 + \lambda_1 z + \lambda_2 z^2 + \lambda_3 z^3 + \cdots$.
The minimality of $(\mathfrak{B}_2, \phi_2)$ implies assertion (2).
For the cases where $p = 2$ or 3, the minimality of $(\mathfrak{B}_3, \phi_3)$ implies $|\phi^{(p+1)p}(0)| = 1/p^2$.
By doing some algebras, for $p = 2$, it is equivalent to $(\phi^3)'(0) + (\phi^3)''(0) \equiv 1 \pmod 4$ in assertion(3).
for $p = 3$, it is equivalent to $\frac{1}{3}\lambda_0 \not\equiv \lambda_2 \pmod 3$ in assertion(3)

Minimal conditions of rational maps for the case p=2 in terms of coefficients

Setup: Let ϕ be a rational map ϕ of degree $d \geq 2$ of the form

$$\phi(z) = \frac{A(z)}{B(z)} = \frac{a_0 + a_1 z + \cdots + a_{d-1} z^{d-1} + z^d}{b_1 z + \cdots + b_{d-1} z^{d-1} + z^d} \in \mathbb{Q}_2(z), \quad (1)$$

satisfying $\phi(0) = \infty$ and $\phi(\infty) = 1$ with $a_i, b_i \in \mathbb{Q}_2$.
This is possible by the linear fractional transformation g of the form,

$$g(z) = \frac{(z - z_0)(\phi^2(z_0) - \phi(z_0))}{(z - \phi(z_0))(\phi^2(z_0) - z_0)}.$$

Set $A_\phi = \sum_{i \geq 0} a_i, B_\phi = \sum_{i \geq 1} b_i,$
$A_{\phi,1} = \sum_{i \geq 0} a_{2i+1}, A_{\phi,2} = \sum_{i \geq 0} a_{4i+1}, A_{\phi,3} = \sum_{i \geq 0} a_{4i+3}.$

Minimal conditions for rational maps for the case p=2

Theorem (Fan-Fan-Liao-Wang, 2017)

If ϕ in (1) has good reduction and is minimal on $\mathbb{P}^1(\mathbb{Q}_2)$, then:

$$\begin{cases} (C1)\ a_i, b_i \in \mathbb{Z}_2,\ \textit{for } 0 \le i \le d-1, \\ (C2)\ a_0 \equiv 1 \pmod 2, (C3)\ B_\phi \equiv 1 \pmod 2, \\ (C4)\ A_\phi \equiv 2 \pmod 4, (C5)\ A_{\phi,1} \equiv 1 \pmod 2, \\ (C6)\ b_1 \equiv 1 \pmod 2, (C7)\ a_{d-1} - b_{d-1} \equiv 1 \pmod 2, \\ (C8)\ a_0 b_1 (a_{d-1} - b_{d-1})(A_{\phi,2} - A_{\phi,3}) B_\phi + \\ \qquad 2(b_2 - a_1 + a_{d-2} - b_{d-2} + b_{d-1} + A_{\phi,3}) \equiv 1 \pmod 4. \end{cases} \tag{2}$$

Conversely, these conditions imply that ϕ is 1-Lipschitz continuous and minimal on $\mathbb{P}^1(\mathbb{Q}_2)$.

Equivalent minimal conditions for $p = 2$

Theorem (JKKK,2021)

If ϕ in (1) has good reduction and is minimal on $\mathbb{P}^1(\mathbb{Q}_2)$, then conditions (C1)-(C8) in Theorem FFLW are satisfied with (C8) replaced by the following condition:

$$(C8')\, A_{\phi,1} + B_\phi + a_{d-1} + b_{d-1} + a_0 + b_1 +$$

$$2\,(b_2 - a_1 + a_{d-2} - b_{d-2}) \equiv 1 \pmod 4.$$

Conversely, the conditions (C1)-(C7) and (C8′) imply that ϕ is 1-Lipschitz continuous and minimal on $\mathbb{P}^1(\mathbb{Q}_2)$.

Note that two conditions $(C8)$ and $(C8')$ are equivalent to each other because for five odd elements $x_i (1 \le i \le 5)$ in $\mathbb{Z}_2$, we have $\prod_{i=1}^5 x_i \equiv \sum_{i=1}^5 x_i \pmod 4$, and the relation $A_{\phi,1} = A_{\phi,2} + A_{\phi,3}$.

Equivalent minimal conditions for $p = 2$

Sketchy proof of the case $p = 2$

(1) Use the minimal conditions of $(\mathbb{P}^1(\mathbb{Q}_2), \phi)$:

(i) the reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbb{F}_2)$;

(ii) $|\lambda_0 = \phi^3(0)| = 1/2$ and $\lambda_1 = (\phi^3)'(0) \equiv 1 \pmod{p}$; and

(iii) $\lambda_1 + \lambda_2/2 = (\phi^3)'(0) + (\phi^3)''(0) \equiv 1 \pmod{2^2}$

(2) Find the coefficients $\lambda_0, \lambda_1, \lambda_2$ of a convergent series $\phi^3(z) = \lambda_0 + \lambda_1 z + \lambda_2 z^2 + O(z^3)$ by decomposing ϕ^3 into a composition of simper convergent series of the form

$$\phi^3 = \varphi_3 \circ \varphi_2 \circ \varphi_1,$$

where, for $\rho(z) = 1/z$, and $T_a(z) = z + a$,

$$\begin{cases} \varphi_1 = \rho \circ \phi = t_{11} z + t_{12} z^2 + O(z^3), \\ \varphi_2 = T_{-1} \circ \phi \circ \rho = t_{21} z + t_{22} z^2 + O(z^3), \\ \varphi_3 = \phi \circ T_1 = t_{30} + t_{31} z + t_{32} z^2 + O(z^3). \end{cases}$$

The results follow from computing (ii) and (iii) involving t_{ij}.

Example for a minimal rational map for $p = 2$

It is known that there are no rational maps on $\mathbb{P}^1(\mathbb{Q}_2)$ of degrees 2, 3, or 4 with good reduction, so we illustrate a rational map on $\mathbb{P}^1(\mathbb{Q}_2)$ of degree 5 with good reduction.

Example

Let $\phi(z) = \dfrac{1 + 2z + 2z^4 + z^5}{3z + 2z^2 - 3z^4 + z^5}$ be a rational map of degree 5 on $\mathbb{P}^1(\mathbb{Q}_2)$. Then the reduction modulo 2 of ϕ is

$$\bar{\phi} = \frac{(z+1)(z^4 + z^3 + z^2 + z + 1)}{z(z^4 + z^3 + 1)}.$$

Therefore, ϕ has good reduction. By the minimal conditions, $(\mathbb{P}^1(\mathbb{Q}_2), \phi)$ is minimal, of which periodic orbit of the induced system of ϕ at level 3 is given by:
$0 \to \infty \to 1 \to 2 \to \tilde{6} \to 3 \to 4 \to \tilde{4} \to 5 \to 6 \to \tilde{2} \to 7,$

Minimal conditions of rational maps for $p = 3$

Let ϕ be a rational map of the form

$$\phi(z) = \frac{A(z)}{B(z)} = \frac{a_0 + a_1 z + \cdots + a_{d-1} z^{d-1} + z^d}{b_1 z + \cdots + b_{d-1} z^{d-1} + z^d} \in \mathbb{Q}_3(z), \quad (3)$$

which satisfies $\phi(0) = \infty$ and $\phi(\infty) = 1$ with $a_i, b_i \in \mathbb{Q}_3$.
Set: $A_\phi = \sum_{i \geq 0} a_i, \quad B_\phi = \sum_{i \geq 1} b_i, \quad A_{\phi,k,l} = \sum_{i \geq 0} a_{ki+l}, \quad B_{\phi,k,l} = \sum_{i \geq 0} b_{ki+l}$ for $0 \leq l \leq k$.
Set the following rational maps $\{\psi_i\}_{1 \leq i \leq 4}$ to decompose $\phi^4 = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$ of $\phi^3(z) = \lambda_0 + \lambda_1 z + \lambda_2 z^2 + O(z^3)$:

$$\begin{cases} \psi_1 = \rho \circ \phi = s_{11} z + s_{12} z^2 + O(z^3), \\ \psi_2 = T_{-1} \circ \phi \circ \rho = s_{21} z + s_{22} z^2 + O(z^3), \\ \psi_3 = T_{-\phi(1)} \circ \phi \circ T_1 = s_{31} z + s_{32} z^2 + O(z^3), \\ \psi_4 = \phi \circ T_{\phi(1)} = s_{40} + s_{41} z + s_{42} z^2 + O(z^3) \end{cases}$$

The results follow from computing the relations $\lambda_0/3 \not\equiv 0\,[3], \lambda_1 \equiv 1\,[3], \lambda_2 \not\equiv \lambda_0/3\,[3]$ involving s_{ij}.

Minimal conditions of rational maps for the case p=3

Theorem (JKKK,2021)

If ϕ has good reduction and is minimal on $\mathbb{P}^1(\mathbb{Q}_3)$, then ϕ satisfies the following conditions:
(a)

$$\begin{cases} a_i, b_i \in \mathbb{Z}_3, \ \textit{for } 0 \le i \le d-1, \\ a_0 \not\equiv 0 \pmod 3, \\ A(1) \equiv 2B(1) \pmod 3 \textit{ and } B(1) \not\equiv 0 \pmod 3, \\ A(2) \equiv 0 \pmod 3 \textit{ and } B(2) \not\equiv 0 \pmod 3. \end{cases}$$

The above conditions correspond to the fact that the reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbb{F}_3)$.

Minimal conditions of rational maps for the case p=3

Theorem (JKKK,2021)

(b) Additionally, ϕ satisfies one of the conditions, (i)-(viii):

Set $u_0 := \left(\frac{A(2)}{3}B(2) + \frac{(A(1)-2B(1))}{3}B(1)B(2)A'(2)\right) \bmod 3;$

$[s_{11}, s_{21}, s_{31}, s_{41}] \bmod 3 = [\cdot,\cdot,\cdot,\cdot]$.

- (i) $[1,1,1,1]$, $u_0 \not\equiv 0[3], s_{12}+s_{22}+s_{32}+s_{42} \not\equiv u_0[3]$;
- (ii) $[1,1,2,2]$, $u_0 \not\equiv 0[3], s_{12}+s_{22}-s_{32}+s_{42} \not\equiv u_0[3]$;
- (iii) $[1,2,1,2]$, $u_0 \not\equiv 0[3], s_{12}-s_{22}-s_{32}+s_{42} \not\equiv u_0[3]$;
- (iv) $[1,2,2,1]$, $u_0 \not\equiv 0[3], s_{12}-s_{22}+s_{32}+s_{42} \not\equiv u_0[3]$;
- (v) $[2,1,1,2]$, $u_0 \not\equiv 0[3], -s_{12}-s_{22}-s_{32}+s_{42} \not\equiv u_0[3]$;
- (vi) $[2,1,2,1]$, $u_0 \not\equiv 0[3], -s_{12}-s_{22}+s_{32}+s_{42} \not\equiv u_0[3]$;
- (vii) $[2,2,1,1]$, $u_0 \not\equiv 0[3], -s_{12}+s_{22}+s_{32}+s_{42} \not\equiv u_0[3]$; *and*
- (viii) $[2,2,2,2]$, $u_0 \not\equiv 0[3], -s_{12}+s_{22}-s_{32}+s_{42} \not\equiv u_0[3]$.

Conversely, the conditions above imply ϕ is minimal on $\mathbb{P}^1(\mathbb{Q}_3)$.

Example for a minimal rational map for $p = 3$

Example

Let $\phi(z) = \dfrac{2+z+z^2+2z^4+z^5}{2z+2z^3+z^5}$ be a rational map of degree 5 on $\mathbb{P}^1(\mathbb{Q}_3)$. Then the reduction modulo 3 of ϕ is $\bar{\phi} = \frac{(z+1)(z^4+z^3+2z^2+2z+2)}{z(z^4+2z^2+2)}$. Thus, ϕ has good reduction. By checking $[s_{11}, s_{21}, s_{31}, s_{41}] \bmod 3 = [1,2,1,2]$ in case (iii), $[s_{12}, s_{22}, s_{32}, s_{42}] \bmod 3 = [1,1,1,1]$, and $[\frac{\lambda_0}{3}, \lambda_2] \bmod 3 = [2,0]$, the periodic orbit of a minimal ϕ at level 3 is given by:

$$0 \to \infty \to 1 \to 23 \to 15 \to \tilde{24} \to 4 \to 8 \to 12 \to \tilde{21} \to 25 \to 2 \to 18 \to \tilde{18} \to 10 \to 5 \to 6 \to \tilde{15} \to 13 \to 17 \to 3 \to\to \tilde{12} \to 7 \to 11 \to 9 \to \tilde{9} \to 19 \to 14 \to 24 \to \tilde{6} \to 22 \to 26 \to 21 \to \tilde{3} \to 16 \to 20.$$

Minimal conditions for a rational map for the case $p \geq 5$

Theorem (JKKK,2021)

Let p be a prime ≥ 5 and $\phi(z) = \frac{A(z)}{B(z)} \in \mathbb{Q}_p(z)$ be a rational map of $\deg \phi \geq 2$ with good reduction. If the dynamical system $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ is minimal, then the following conditions are satisfied:

(1) The reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbb{F}_p)$, of which the full cycle is given by $(0, \infty, \xi_1, \cdots, \xi_{p-1})$ where $\{\xi_1 := 1, \xi_2, \cdots, \xi_{p-1}\} = \mathbb{F}_p^*$.

(2) $\displaystyle \frac{b_1}{a_0}(a_{d-1} - b_{d-1}) \prod_{i=1}^{p-1} \frac{A'(i)B(i) - A(i)B'(i)}{B^2(i)} \equiv 1 \pmod{p}.$

(3) $\phi(\xi_{p-1}) + (\phi(\xi_{p-2}) - \xi_{p-1})w_{p-1} + \cdots + (\phi(\xi_1) - \xi_2)w_2 \not\equiv 0 \pmod{p^2}$ *for* $2 \leq i \leq p-1$, $w_i = \prod_{j=i}^{p-1} \phi'(\xi_j)$.

Conversely, if the above conditions are satisfied, then ϕ is a 1-Lipschitz continuous minimal map on $\mathbb{P}^1(\mathbb{Q}_p)$.

Minimal conditions for $p \geq 5$

Using the decomposition of $\phi^{p+1} = \eta_{p+1} \circ \eta_p \cdots \eta_2 \circ \eta_1$ consisting of the following convergent series:

$$\begin{cases} \eta_1 = \rho \circ \phi = b_1/a_0 z + O(z^2), \\ \eta_2 = T_{-\phi^2(0)} \circ \phi \circ \rho = (a_{d-1} - b_{d-1})z + O(z^2), \\ \eta_i = T_{-\phi^i(0)} \circ \phi \circ T_{\phi^{i-1}(0)} = \phi'(\phi^{i-1}(0))z + O(z^2) \ (3 \leq i \leq p), \text{ and} \\ \eta_{p+1} = \phi \circ T_{\phi^p(0)} = \phi^{p+1}(0) + \phi'(\phi^p(0))z + O(z^2), \end{cases} \tag{4}$$

we find the constant term and the term of degree 1 so that

$$\phi^{p+1}(z) = \boxed{\phi^{p+1}(0)} + \boxed{\frac{b_1}{a_0}(a_{d-1} - b_{d-1})\phi'(\phi^2(0)) \cdots \phi'(\phi^p(0))} z + O(z^2).$$

$\Downarrow$ cond.(3) $\qquad\qquad$ $\Downarrow$ cond. (2)

Example for a minimal rational map for primes $p \geq 5$

Example

Let $\phi(z) = \dfrac{5 + 4z + 3z^2 + 4z^4 + z^5}{4z + 7z^2 + 3z^4 + z^5}$ be a rational map of degree 5 on $\mathbb{P}^1(\mathbb{Q}_7)$. Then the reduction modulo 7 of ϕ is

$$\bar{\phi} = \frac{(z+1)(z^4 + 3z^3 + 4z^2 + 6z + 5)}{z(z^4 + 3z^3 + 4)}.$$

Therefore, ϕ has good reduction. Since the full cycle of $\bar{\phi}$ is given by $(0, \infty, \xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6) = (0, \infty, 1, 3, 2, 4, 5, 6)$, the reduction ϕ is transitive on $\mathbb{P}^1(\mathbb{F}_7)$. By checking that $[r_\infty, r_0, r_1, \cdots, r_6] = [5, 1, 3, 2, 2, 5, 2, 3]$ and $[w_2, w_3, w_4, w_5, w_6] = [1, 4, 2, 6, 3]$, conditions (2) and (3) of the previous Theorem are satisfied as $\lambda_0 \equiv 28 \bmod 49$, so the dynamical system $(\mathbb{P}^1(\mathbb{Q}_7), \phi)$ is minimal.

Example for a minimal rational map for primes $p \geq 5$

The periodic orbit of minimal length 56 of the induced system of ϕ at level 2 is given by:

$$0 \to \infty \to 1 \to 24 \to 23 \to 46 \to 26 \to 34 \to 28 \to \tilde{42} \to 43$$
$$\to 3 \to 30 \to 11 \to 47 \to 27 \to 7 \to \tilde{35} \to 36 \to 31 \to 37$$
$$\to 25 \to 19 \to 20 \to 35 \to \tilde{28} \to 29 \to 10 \to 44 \to 39x \to 40$$
$$\to 13 \to 14 \to \tilde{21} \to 22 \to 38 \to 2 \to 4 \to 12 \to 6 \to 42$$
$$\to \tilde{14} \to 15 \to 17 \to 9 \to 18 \to 33 \to 48 \to 21 \to \tilde{7} \to 8$$
$$\to 45 \to 16 \to 32 \to 5 \to 41.$$

Some remarks

1. Without a change of coordinates we obtain the following crucial relation:

$$\phi'(0)\phi'(\infty) = \frac{b_1}{a_0}(a_{d-1} - b_{d-1}).$$

2. It is of great interest to characterize a minimal rational function $f(z) \in \mathbb{F}_p(z)$ satisfying $f(0) = \infty$ and $f(\infty) = 1$ in terms of its coefficients , as in permutation polynomials over finite fields.

Thank you for your attention !!!