Polynomial and rational dynamical systems on the field of $p$-adic numbers and its projective line

Lingmin LIAO (Université Paris-Est Créteil)
(worked with Ai-Hua Fan, Shi-Lei Fan, Yue-Fei Wang, Dan Zhou)

Inha University

Incheon, Korea, August 13th 2018
1. Introduction

2. Polynomials on $\mathbb{Z}_p$

3. Rational maps of degree 1 on $\mathbb{P}^1(\mathbb{Q}_p)$

4. $p$-adic repellers in $\mathbb{Q}_p$
Introduction
I. The \( p \)-adic numbers

- \( p \geq 2 \) a prime number:
  \[
  \forall n \in \mathbb{N}, \ n = \sum_{i=0}^{N} a_i p^i \ (a_i = 0, 1, \ldots, p-1).
  \]

- Ring \( \mathbb{Z}_p \) of \( p \)-adic integers:
  \[
  \mathbb{Z}_p \ni x = \sum_{i=0}^{\infty} a_i p^i.
  \]

- Field \( \mathbb{Q}_p \) of \( p \)-adic numbers: fraction field of \( \mathbb{Z}_p \):
  \[
  \mathbb{Q}_p \ni x = \sum_{i=v(x)}^{\infty} a_i p^i, \ (\exists v(x) \in \mathbb{Z}).
  \]

Absolute value: \( |x|_p = p^{-v(x)} \), metric: \( d(x, y) = |x - y|_p \).

- ultrametric inequality: \( d(x, z) \leq \max\{d(x, y), d(y, z)\} \).
- a fact: \( \overline{\mathbb{N}} = \mathbb{Z}_p \).
II. Arithmetic in $\mathbb{Q}_p$

Addition and multiplication: similar to the decimal way. "Carrying" from left to right.

Example: $x = (p - 1) + (p - 1) \times p + (p - 1) \times p^2 + \cdots$, then

- $x + 1 = 0$. So,

$$-1 = (p - 1) + (p - 1) \times p + (p - 1) \times p^2 + \cdots.$$ 

- $2x = (p - 2) + (p - 1) \times p + (p - 1) \times p^2 + \cdots$.

We also have subtraction and division.

Then we can define polynomials and rational maps.
III. $p$-adic dynamical systems

A $p$-adic dynamical system is a couple $(X, f)$ where $X$ is a $p$-adic space and $f : X \to X$ is a transformation on $X$.

The beginning:
Oselies-Zieschang 1975: automorphisms of $\mathbb{Z}_p$,
Herman-Yoccoz 1983: complex $p$-adic dynamical systems,
Volovich 1987: $p$-adic string theory.

We are interested in the **polynomials** and **rational maps** considered as dynamical systems on $\mathbb{Z}_p$ or $\mathbb{Q}_p$.

There are two important families of dynamical systems:

1. **Lipschitz** dynamical systems and **expanding** dynamical systems.

**Typical examples**:

- $f(x) = x + 1$ on $\mathbb{Z}_p$ is minimal (every orbit is dense).
- $f(x) = \frac{x^p - x}{p}$ on $\mathbb{Z}_p$ is conjugate to the shift on $\{0, 1, \ldots, p - 1\}^\mathbb{N}$.

Remark: shift $\sigma$ is defined as

$$x = x_0 x_1 x_2 \cdots \xrightarrow{\sigma} \sigma x = x_1 x_2 \cdots.$$
IV. 1-Lipschitz $p$-adic dynamical systems

Let $f \in \mathbb{Z}_p[x]$ be a polynomial. Then it defines a dynamical systems on $\mathbb{Z}_p$, denoted by $(\mathbb{Z}_p, f)$.

It is 1-Lipschitz and then equicontinuous.

The system $(X, T)$ is equicontinuous if

$$\forall \epsilon > 0, \exists \delta > 0 \text{ s. t. } d(T^n x, T^n y) < \epsilon \ (\forall n \geq 1, \forall d(x, y) < \delta).$$

**Theorem**

Let $X$ be a compact metric space and $T : X \to X$ be an equicontinuous transformation. Then the following statements are equivalent:

1. $T$ is minimal (every orbit is dense).
2. $T$ is uniquely ergodic (there is a unique invariant measure).
3. $T$ is ergodic for any/some invariant measure with $X$ as its support.
V. Researches on $1$-Lipschitz dynamical systems on $\mathbb{Z}_p$

For $1$-Lipschitz continuous maps $f : \mathbb{Z}_p \to \mathbb{Z}_p$, the dynamical systems $(\mathbb{Z}_p, f)$ are extensively studied. For example:

- **Polynomials**
  - Coelho-Parry 2001: $ax$ and distribution of Fibonacci numbers
  - S. Fan-Liao 2016: minimal decomp. of $x^2$, Chebyshev polynomials.

- **Mahler Series**

- **van der Put Series**

**Applications**: pseudo-randomnumber generator, frequency of prime divisors of a sequence, etc.
VI. Expanding dynamical systems on $\mathbb{Q}_p$

- $f : X(\subset \mathbb{Q}_p) \to \mathbb{Q}_p$ is \textbf{continuously differentiable} at $a \in X$ if the following exists:

$$\lim_{(x,y) \to (a,a), x \neq y} \frac{f(x) - f(y)}{x - y}.$$ 

\textbf{Lemma (Local rigidity lemma)}

Let $U$ be a clopen (close and open) set and $a \in U$. Suppose

$$f : U \to \mathbb{Q}_p \text{ is continuously differentiable, } f'(a) \neq 0.$$ 

Then there exists $r > 0$ such that $B_r(a) \subset U$ and

$$\forall x, y \in B_r(a), \quad |f(x) - f(y)|_p = |f'(a)|_p |x - y|_p.$$ 

\textbf{Remark} : if $|f'(a)|_p > 1$, then $f$ is \textbf{expanding} on a neighborhood of $a$. 
VII. Researches on expanding dynamical systems on $\mathbb{Q}_p$

- Woodcock and Smart 1998 : $\frac{x^p - x}{p}$ on $\mathbb{Z}_p$.
- Mukhamedov and Mendes 2007 : some cubic polynomials.

Applications : vastness of the set of $p$-adic Gibbs measures.
Polynomials on $\mathbb{Z}_p$
I. Polynomial dynamical systems on $\mathbb{Z}_p$

- Let $f \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$.
- Polynomial dynamical systems: $f : \mathbb{Z}_p \to \mathbb{Z}_p$, noted as $(\mathbb{Z}_p, f)$.

**Theorem (Ai-Hua Fan, L; 2011) minimal decomposition**

Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. The space $\mathbb{Z}_p$ can be decomposed into three parts:

$$\mathbb{Z}_p = \mathcal{P} \sqcup \mathcal{M} \sqcup \mathcal{B},$$

where

- $\mathcal{P}$ is the finite set consisting of all periodic orbits;
- $\mathcal{M} := \bigsqcup_{i \in I} \mathcal{M}_i$ ($I$ finite or countable)
  - $\mathcal{M}_i$ : finite union of balls,
  - $f : \mathcal{M}_i \to \mathcal{M}_i$ is minimal;
- $\mathcal{B}$ is attracted into $\mathcal{P} \sqcup \mathcal{M}$. 

II. Minimality on the whole space $\mathbb{Z}_p$

**Theorem (Larin 2002), General polynomials, only for $p = 2$**

Let $p = 2$ and let $f(x) = \sum_{k \geq 0} a_k x^k \in \mathbb{Z}_2[X]$ be a polynomial. Then $(\mathbb{Z}_p, f)$ is minimal iff

\[
\begin{align*}
a_0 &\equiv 1 \pmod{2}, \\
a_1 &\equiv 1 \pmod{2}, \\
2a_2 &\equiv a_3 + a_5 + \cdots \pmod{4}, \\
a_2 + a_1 - 1 &\equiv a_4 + a_6 + \cdots \pmod{4}.
\end{align*}
\]

General polynomials for $p = 3$ : **Durand-Paccaut 2009**.

Quadratic polynomials for all $p$ : **Larin 2002 + Knuth 1969**.
III. Minimal decomposition of affine polynomials on $\mathbb{Z}_p$

Let $T_{a,b}x = ax + b \ (a, b \in \mathbb{Z}_p)$. Denote

$$
U = \{z \in \mathbb{Z}_p : |z| = 1\}, \quad V = \{z \in U : \exists m \geq 1, \text{s.t. } z^m = 1\}.
$$

**Easy cases :**

1. $a \in \mathbb{Z}_p \setminus U \Rightarrow$ one attracting fixed point $b/(1 - a)$.
2. $a = 1, b = 0 \Rightarrow$ every point is fixed.
3. $a \in V \setminus \{1\} \Rightarrow$ every point is on a $\ell$-periodic orbit, with $\ell$ the smallest integer $\geq 1$ such that $a^\ell = 1$.

**Theorem (AH. Fan, MT. Li, JY. Yao, D. Zhou 2007) Case $p \geq 3$ :**

4. $a \in (U \setminus V) \cup \{1\}, \ v_p(b) < v_p(1 - a) \Rightarrow p^{v_p(b)}$ minimal parts.
5. $a \in U \setminus V, \ v_p(b) \geq v_p(1 - a) \Rightarrow (\mathbb{Z}_p, T_{a,b})$ is conjugate to $(\mathbb{Z}_p, ax)$.

Decomposition : $\mathbb{Z}_p = \{0\} \sqcup \sqcup_{n \geq 1} p^n U$.

(1) One fixed point $\{0\}$.

(2) All $(p^n U, ax)(n \geq 0)$ are conjugate to $(U, ax)$.

For $(U, T_{a,0}) : p^{v_p(a^\ell - 1)}(p - 1)/\ell$ minimal parts, with $\ell$ the smallest integer $\geq 1$ such that $a^\ell \equiv 1(\mod p)$. 
Two typical decompositions of $\mathbb{Z}_p$:

- $Tx = x + 3$, $p = 3$
- $Tx = 6x$, $p = 7$
IV. Min. decomp. of quadratic polynomials on $\mathbb{Z}_2$

Theorem (A. Fan-L, 2011)

For $(\mathbb{Z}_2, x^2 + x)$,

1. The ball $1 + 2\mathbb{Z}_2$ is mapped into $2\mathbb{Z}_2$.
2. The ball $2\mathbb{Z}_2$ can be decomposed as:

$$2\mathbb{Z}_2 = \{0\} \bigsqcup \left( \bigsqcup_{n \geq 2} 2^{n-1} + 2^n \mathbb{Z}_2 \right),$$

and for each $n \geq 2$, $2^{n-1} + 2^n \mathbb{Z}_2$ is decomposed as $2^{n-2}$ minimal component:

$$2^{n-1} + t2^n + 2^{2n-2} \mathbb{Z}_2, \quad t = 0, \ldots, 2^{n-2} - 1.$$
→ decomposition of $x^2 + x$

1 → 0 (mod 2)

0 → 2 (mod $2^2$)

0 → 4 (mod $2^3$)

0 → 12 (mod $2^4$)

0 → 24 (mod $2^5$)

0 → 56 (mod $2^6$)
Rational maps of degree 1 on $\mathbb{P}^1(Q_p)$
1. Projective line over $\mathbb{Q}_p$
For $(x_1, y_1), (x_2, y_2) \in \mathbb{Q}_p^2 \setminus \{(0, 0)\}$, we say that $(x_1, y_1) \sim (x_2, y_2)$ if there exists $\lambda \in \mathbb{Q}_p^*$ such that $x_1 = \lambda x_2$ and $y_1 = \lambda y_2$.

Projective line over $\mathbb{Q}_p$:

$$\mathbb{P}^1(\mathbb{Q}_p) := (\mathbb{Q}_p^2 \setminus \{(0, 0)\}) / \sim$$

Spherical metric: for $P = [x_1, y_1], Q = [x_2, y_2] \in \mathbb{P}^1(\mathbb{Q}_p)$, define

$$\rho(P, Q) = \frac{|x_1 y_2 - x_2 y_1|_p}{\max\{|x_1|_p, |y_1|_p\} \max\{|x_2|_p, |y_2|_p\}}.$$ 

Viewing $\mathbb{P}^1(\mathbb{Q}_p)$ as $\mathbb{Q}_p \cup \{\infty\}$, for $z_1, z_2 \in \mathbb{Q}_p \cup \{\infty\}$ we define

$$\rho(z_1, z_2) = \frac{|z_1 - z_2|_p}{\max\{|z_1|_p, 1\} \max\{|z_2|_p, 1\}}$$

if $z_1, z_2 \in \mathbb{Q}_p$, and

$$\rho(z, \infty) = \begin{cases} 1, & \text{if } |z|_p \leq 1; \\ 1/|z|_p, & \text{if } |z|_p > 1. \end{cases}$$
Geometric representations of $\mathbb{P}^1(\mathbb{Q}_2)$ and $\mathbb{P}^1(\mathbb{Q}_3)$
II. Homographic maps

Let

$$\phi(x) = \frac{ax + b}{cx + d} \quad \text{with} \quad a, b, c, d \in \mathbb{Q}_p, \quad ad - bc \neq 0,$$

which induces an 1-to-1 map $\phi : \mathbb{P}^1(\mathbb{Q}_p) \mapsto \mathbb{P}^1(\mathbb{Q}_p)$.

The dynamics of $\phi$ depends on its fixed points which are the solution of

$$\frac{ax + b}{cx + d} = x \iff cx^2 + (d - a)x - b = 0.$$

Discriminant : $\Delta = (d - a)^2 + 4bc$.

- If $\Delta = 0$, then $\phi$ has only one fixed point $x_0$ in $\mathbb{Q}_p$ and $\phi(x)$ is conjugate to a translation $\psi(x) = x + \alpha$ for some $\alpha \in \mathbb{Q}_p$ by $g(x) = \frac{1}{x - x_0}$.

- If $\Delta \neq 0$ and $\sqrt{\Delta} \in \mathbb{Q}_p$, then $\phi$ has two fixed points $x_1, x_2 \in \mathbb{Q}_p$ and $\phi$ is conjugate to a multiplication $x \mapsto \beta x$ for some $\beta \in \mathbb{Q}_p$ by $g(x) = \frac{x - x_2}{x - x_1}$.

- If $\Delta \neq 0$ and $\sqrt{\Delta} \notin \mathbb{Q}_p$, then $\phi$ has no fixed point in $\mathbb{Q}_p$. But $\phi$ has two fixed points $x_1, x_2 \in \mathbb{Q}_p(\sqrt{\Delta})$. So we will study the dynamics of $\phi$ on $\mathbb{P}^1(\mathbb{Q}_p(\sqrt{\Delta}))$ then its restriction on $\mathbb{P}^1(\mathbb{Q}_p)$. 

Lingmin LIAO University Paris-East Créteil

Polynomial and rational dynamical systems on $\mathbb{Q}_p$ and $\mathbb{P}^1(\mathbb{Q}_p)$
III. Minimal decomposition ($\phi$ admits no fixed point)

Theorem (AH. Fan, SL. Fan, L, YF. Wang; 2014)

Suppose that $\phi$ has no fixed points in $\mathbb{P}^1(\mathbb{Q}_p)$ and $\phi^n \neq id$ for each integer $n > 0$. Then

1. the system $(\mathbb{P}^1(\mathbb{Q}_p), \phi)$ is decomposed as a finite number of minimal subsystems;
2. these minimal subsystems are topologically conjugate to each other;
3. the number of minimal subsystems is determined by the number

$$\lambda := \frac{(a + d) + \sqrt{\Delta}}{(a + d) - \sqrt{\Delta}}.$$

Remark: We have also obtained the minimal criterion for a degree one rational map to be minimal on the whole space $\mathbb{P}^1(\mathbb{Q}_p)$. 
IV. Ideas and methods

  
  Let $X \subset \mathbb{Z}_p$ be a compact set.
  
  $f : X \to X$ is minimal $\iff$ $f_n : X/p^n\mathbb{Z}_p \to X/p^n\mathbb{Z}_p$ is minimal $\forall n \geq 1$.

- **Desjardins and Zieve 1994, Ph.D thesis of Zieve 1996**: induction from level $n$ to level $n + 1$.

Predicting the behavior of $f_{n+1}$ by the structure of $f_n$.

- Consider the cycle $(x_1, \ldots, x_k)$ in $X/p^n\mathbb{Z}_p$,
- Each $x_i$ is lift to be $p$ points $\{x_i + tp^n : 0 \leq t < p\}$ in $X/p^{n+1}\mathbb{Z}_p$.

**Linearization**:

$g := f^k$,

$$g(x_1 + tp^n) \equiv x_1 + (a_n t + b_n)p^n \pmod{p^{n+1}}$$

with $a_n = g'(x_1)$, $b_n = \frac{g(x_1) - x_1}{p^n}$.

**Linear maps** $\Phi : \Phi(t) = a_n t + b_n$. 


V. Ideas and methods (continued)

Lifts of the cycle \((x_1, \ldots, x_k)\):

Let \(X_{n+1} = \{x_i + tp^n : 0 \leq t < p\}\)

- \(a_n \equiv 1, b_n \not\equiv 0 \mod p\) : \(f_{n+1}|_{X_{n+1}}\) has 1 cycle of length \(pk\).
  We say \(\sigma\) grows.

- \(a_n \equiv 1, b_n \equiv 0 \mod p\) : \(f_{n+1}|_{X_{n+1}}\) has \(p\) cycles of length \(k\).
  We say \(\sigma\) splits.

- \(a_n \equiv 0 \mod p\) : \(f_{n+1}|_{X_{n+1}}\) has a single cycle of length \(k\) and the remaining points of \(X\) are mapped into this cycle by \(f^k\).
  We say \(\sigma\) grows tails.

- \(a_n \not\equiv 0, 1 \mod p\) : \(f_{n+1}|_{X_{n+1}}\) has a single cycle of length \(k\) and \((p - 1)/\ell\) cycles of length \(k\ell\).
  We say \(\sigma\) partially splits.
Behavior of $f_{n+1}$

Case 1

Case 2

Case 3

Case 4
$p$-adic repellers in $\mathbb{Q}_p$
I. Settings

- \( f : X \to \mathbb{Q}_p, \ X \subset \mathbb{Q}_p \) compact open.
- Assume that
  1. \( f^{-1}(X) \subset X \);
  2. \( X = \bigsqcup_{i \in I} B_{p^{-\tau}}(c_i) \) (with some \( \tau \in \mathbb{Z} \)), \( \forall i \in I, \exists \tau_i \in \mathbb{Z} \) s.t.
     \[
     |f(x) - f(y)|_p = p^{\tau_i} |x - y|_p \quad (\forall x, y \in B_{p^{-\tau}}(c_i)).
     \]  
(1)
- Define **Julia set**: 
  \[
  J_f = \bigcap_{n=0}^{\infty} f^{-n}(X).
  \]
  We have \( f(J_f) \subset J_f \). \((X, J_f, f)\) is called
  \( \rightarrow \) a **\( p \)-adic weak repeller** if all \( \tau_i \geq 0 \) in (1), but at least one \( > 0 \).
  \( \rightarrow \) a **\( p \)-adic repeller** if all \( \tau_i > 0 \) in (1).
II. Results

- For any $i \in I$, let
  \[ I_i := \{ j \in I : B_j \cap f(B_i) \neq \emptyset \} = \{ j \in I : B_j \subset f(B_i) \}. \]
- Define $A = (A_{i,j})_{I \times I}$:
  \[ A_{ij} = 1 \text{ if } j \in I_i; \quad A_{ij} = 0 \text{ otherwise.} \]
- If $A$ is irreducible, we say that $(X, J_f, f)$ is **transitive**.
- Let $(\Sigma_A, \sigma)$ be the corresponding subshift.


Let $(X, J_f, f)$ be a transitive $p$-adic weak repeller with matrix $A$. Then the dynamics $(J_f, f)$ is topologically conjugate to the shift dynamics $(\Sigma_A, \sigma)$. 
III. Examples

→ Example 1

Let \( c = \frac{c_0}{p^\tau} \in \mathbb{Q}_p \) with \( |c_0|_p = 1 \) and \( \tau \geq 1 \).
Define \textit{\( p \)-adic logistic map} \( f_c : \mathbb{Q}_p \rightarrow \mathbb{Q}_p \)

\[
f_c(x) = cx(x - 1).
\]

- \( X = p^\tau \mathbb{Z}_p \sqcup (1 + p^\tau \mathbb{Z}_p) \),
- \( J_c = \bigcap_{n=0}^\infty f_c^{-n}(X) \).


\( (J_c, f_c) \) is conjugate to \( (\{0, 1\}^\mathbb{N}, \sigma) \).
Example 2

Let \( a \in \mathbb{Z}_p \), \( a \equiv 1 \pmod{p} \) and \( m \geq 1 \) be an integer. Consider \( f_{m,a} : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p \):

\[
f_{m,a}(x) = \frac{x^p - ax}{p^m}.
\]

\[
I_{m,a} = \{0 \leq k < p^m : k^p - ak \equiv 0 \pmod{p^m}\}
\]

\[
X_{m,a} = \bigcup_{k \in I_{m,a}} (k + p^m \mathbb{Z}_p), \quad J = \bigcap_{n=0}^{\infty} f_{m,-n}^{-n}(X).
\]

Theorem (A. Fan-L-Wang-Zhou, 2007)

\((J, f_{m,a})\) is conjugate to \((\{0, \ldots, p - 1\}^\mathbb{N}, \sigma)\).

Theorem (Woodcock and Smart 1998)

\((J, f_{1,1})\) is conjugate to \((\{0, \ldots, p - 1\}^\mathbb{N}, \sigma)\).