Applications of p-adic Dynamics

Robert L. Benedetto
Amherst College

Fields Institute
Mini-Workshop on p-adic Dynamics

Tuesday, October 28, 2008

Dynamics over Number Fields

K = global field, $N \geq 1$.

$\phi : \mathbb{P}^N(K) \to \mathbb{P}^N(K)$ morphism over K, degree $d \geq 2$.
($N = 1$: $\phi \in K(z)$ is a rational function.)

$\mathrm{Preper}(\phi, K) := \{\text{preperiodic points of } \phi \text{ in } \mathbb{P}^1(K)\}$.

Example. $\phi(z) = z^2 - \dfrac{133}{144}$, on $\mathbb{P}^1(\mathbb{Q})$.

$$0 \mapsto -\frac{133}{144} \mapsto -\frac{1463}{20736} \mapsto -\frac{394995503}{429981696} \mapsto \cdots$$

$$0 \mapsto -\frac{(*)}{2^4 \cdot 3^2} \mapsto \frac{(*)}{2^8 \cdot 3^4} \mapsto \frac{(*)}{2^{16} \cdot 3^8} \mapsto \cdots$$

$$\frac{17}{12} \mapsto \frac{13}{12} \mapsto \frac{1}{4} \mapsto -\frac{31}{36} \mapsto -\frac{59}{324} \mapsto \cdots$$

$$\frac{(*)}{2^2 \cdot 3} \mapsto \frac{(*)}{2^2 \cdot 3} \mapsto \frac{(*)}{2^2 \cdot 3^0} \mapsto \frac{(*)}{2^2 \cdot 3^2} \mapsto \frac{(*)}{2^2 \cdot 3^4} \mapsto \cdots$$

$$\frac{43}{12} \mapsto \frac{143}{12} \mapsto \frac{1693}{12} \mapsto \frac{238843}{12} \mapsto \frac{4753831543}{12} \mapsto \cdots$$

$$\phi(z) = z^2 - \frac{133}{144}.$$

$$\frac{1}{12} \mapsto -\frac{11}{12} \leftrightarrows -\frac{1}{12} \mapsto \frac{11}{12}$$

$$\frac{7}{12} \mapsto -\frac{7}{12} \mapsto -\frac{7}{12}$$

$$-\frac{19}{12} \mapsto \frac{19}{12} \mapsto \frac{19}{12}$$

$$\infty \mapsto \infty$$

$$\phi(z) = z^2 - \frac{29}{16}.$$

$$\begin{array}{ccccccc} & & -\frac{1}{4} & \longrightarrow & -\frac{7}{4} & \longrightarrow & \frac{5}{4} \longrightarrow -\frac{1}{4} \\ & & \uparrow & & \uparrow & & \uparrow \\ \pm\frac{3}{4} & \longrightarrow & -\frac{5}{4} & & \frac{1}{4} & & \frac{7}{4} \end{array}$$

$$\infty \mapsto \infty$$

Theorem (Northcott, 1950): Let K be a global field. Let $\phi : \mathbb{P}^N(K) \to \mathbb{P}^N(K)$ be a morphism, defined over K, of degree $d \geq 2$. Then

$$\#\text{Preper}(\phi, K) < \infty.$$

Dynamical Uniform Boundedness Conjecture (Morton & Silverman, 1994):
For any integers $d \geq 2$, $D \geq 1$, and $N \geq 1$, there is a constant $C = C(d, D, N)$ such that

- for any number field K with $[K : \mathbb{Q}] = D$, and
- for any morphism $\phi : \mathbb{P}^N(K) \to \mathbb{P}^N(K)$ defined over K and of degree d,

$$\#\text{Preper}(\phi, K) \leq C(d, D, N).$$

Conjecture (DUBC Lite):
There is a constant $C > 0$ so that for any **quadratic polynomial** $\phi \in \mathbb{Q}[z]$,

$$\#\text{Preper}(\phi, \mathbb{Q}) \leq C.$$

Refined DUBC Lite Conjecture (Poonen, 1998):
The DUBC Lite Constant is 9.

Recall:

Definition. Let K be a global field, $v \in M_K$ non-archimedean, and $\phi \in K(z)$ a rational function.

We say ϕ has **good reduction** at v if ϕ may be written in homogeneous coordinates as $[f, g]$, i.e.,

$$\phi\left(\frac{x}{y}\right) = \frac{f(x,y)}{g(x,y)}$$

for some $f, g \in \mathcal{O}_v[x, y]$ homogeneous of the same degree such that:

the reductions $\overline{f}$ and $\overline{g}$ have no common zeros besides $(0, 0)$.

Idea: ϕ still "makes sense" everywhere modulo v.

Theorem.
(Pezda, Morton & Silverman, Zieve, 1990s).
If $\phi \in K(z)$ with $\deg \phi = d$ has good reduction at v, then

$$\#\text{Preper}(\phi, K) \leq O(d^{N\mathfrak{p}_v^3}).$$

[$\mathfrak{p}_v$ is the prime ideal in K associated to v, and $N\mathfrak{p}_v$ is its norm.]

In fact, they proved a bound on the length of the longest periodic cycle.

Somewhat better bounds are possible if you know two good primes.

The proof works entirely in the local field K_v.

Theorem. (Call & Goldstine, 1997.) Let $c \in \mathbb{Q}$ and let $\phi(z) = z^2 + c$. Let s be the number of bad primes (i.e., one plus the number of **distinct** primes dividing the denominator of c).
Then

$$\#\text{Preper}(\phi, \mathbb{Q}) \leq 1 + 2^{s+2} = O(2^s)$$

except for $c = -2$, with $\#\text{Preper}(\phi, \mathbb{Q}) = 6$.

Idea of Proof:

1. (p-adic dynamics step):

Recall $\mathcal{K}_p =$ filled Julia set of ϕ at p.

Clearly $\text{Preper}(\phi, \mathbb{Q}_p) \setminus \{\infty\} \subseteq \mathcal{K}_p$.
(a.) For good primes p, prove that $\mathcal{K}_p$ sits inside a unit disk.

(b.) For bad primes p, prove that $\mathcal{K}_p$ sits inside a union of two unit disks.
(Slightly different for $p = 2, \infty$.)

2. (global step):

In each choice of one unit disk at each prime (or interval length 1 at $v = \infty$), there is only one rational number.

Theorem. (RB, 2004.) Let K be a global field, and let $\phi(z) \in K[z]$ be a polynomial of degree $d \geq 2$. Let s be the number of bad primes (i.e, **not potentially good**) of ϕ. Then

$$\#\text{Preper}(\phi, K) \leq O\left(\frac{d^2}{\log d} \cdot s \log s\right).$$

In fact, for s large enough, the bound is

$$(d^2 - 2d + 2)[t \log_d t + t \log_d \log_d t + 3t] + 1.$$

where

$$t = \begin{cases} s & \text{if there are no archimedean primes} \\ s + \dfrac{D \log d}{4 \log 2} & \text{otherwise,} \end{cases}$$

where $D = [K : \mathbb{Q}]$ in the number field case.

Recall:

Definition. Let $v \in M_K$, and let $\phi \in K[z]$ be a polynomial of degree $d \geq 2$. Let $\mathbb{C}_v$ be the completion of an algebraic closure of K_v.

The *filled Julia set* of ϕ at v is

$$\mathcal{K}_{\phi,v} = \{x \in \mathbb{C}_v : \{|\phi^n(x)|_v\}_{n\geq 0} \text{ is bounded}\}$$

Note:

(1) All preperiodic points (besides ∞) lie in $\mathcal{K}_{\phi,v}$.

(2) If ϕ is good at v, then $\mathcal{K}_{\phi,v} = \overline{D}(0,1)$.

(3) If ϕ is monic, then the smallest disk $\overline{D}(a,r)$ containing $\mathcal{K}_{\phi,v}$ has radius $r \geq 1$.

Lemma 1. Let K, v, ϕ, d be as above. Assume ϕ is monic, and let $r_{\phi,v}$ be the radius of the smallest disk in $\mathbb{C}_v$ containing $\mathcal{K}_{\phi,v}$.

Given $N \geq 2$, let $x_1, \ldots, x_N \in \mathcal{K}_{\phi,v}$. Then

$$\prod_{i \neq j} |x_i - x_j|_v \leq B_v(N) \cdot r_{\phi,v}^{(d-1)N \log_d N},$$

where

$$B_v(N) = \begin{cases} N^N & \text{if } v \text{ is archimedean,} \\ 1 & \text{if } v \text{ is non-archimedean.} \end{cases}$$

Note:

(1) If ϕ not monic, you get a correction factor of $|a_d|^{-N(N-1)/(d-1)}$ on the right.

(2) The N^N factors can probably be substantially reduced (but not eliminated).

(3) Otherwise, these bounds are sharp: $\phi(z) = z^d + c$.

Proof.

Let $\overline{D}(a, r_{\phi,v})$ be the smallest disk containing $\mathcal{K}_{\phi,v}$.

For any integer $j \geq 0$, write

$$j = c_0 + c_1 d + c_2 d^2 + \cdots + c_M d^M$$

in base d. $(0 \leq c_i \leq d-1.)$ Let

$$f_j(z) = \prod_{i=0}^{M} [\phi^i(z) - a]^{c_i},$$

so that f_j is a monic polynomial of degree j with

$$|f_j(x)|_v \leq r_{\phi,v}^{c_0+c_1+c_2+\cdots+c_M}$$

for $x \in \mathcal{K}_{\phi,v}$.

Meanwhile, $\prod_{i \neq j} (x_i - x_j) = \pm(\det V)^2$, where V is the Vandermonde matrix

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{N-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_N & x_N^2 & \dots & x_N^{N-1} \end{bmatrix}.$$

Since each f_j is monic, we can apply column operations (starting from the right) to obtain $\det V = \det A$, where

$$A = \begin{bmatrix} 1 & f_1(x_1) & f_2(x_1) & \dots & f_{N-1}(x_1) \\ 1 & f_1(x_2) & f_2(x_2) & \dots & f_{N-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & f_1(x_N) & f_2(x_N) & \dots & f_{N-1}(x_N) \end{bmatrix}.$$

By Hadamard's inequality, $|\det A|_v$ is bounded above by the product of the norms of the columns.
(Use the L^2-norm for archimedean v, and L^∞-norm for non-archimedean v.)

The f_j column has norm at most $\sqrt{N} \cdot r_{\phi,v}^{c_0+\cdots+c_M}$ if v is archimedean, or simply $r_{\phi,v}^{c_0+\cdots+c_M}$ if v is non-archimedean.

Hence

$$\prod_{i \neq j} |x_i - x_j|_v \leq B_v(N) \prod_{j=0}^{N-1} r_{\phi,v}^{2(c_0+\cdots+c_M)},$$

That is,

$$\prod_{i \neq j} |x_i - x_j|_v \leq B_v(N) \cdot r_{\phi,v}^{E(N,d)},$$

where

$$\begin{aligned} E(N,d) &= 2 \sum_{j=0}^{N-1} [c_0(j) + c_1(j) + \cdots + c_M(j)] \\ &= \text{ twice the sum of all base-}d\text{ coefficients} \\ &\quad \text{of all integers from 0 to } N-1. \end{aligned}$$

Finally, it is elementary to show that

$$E(N,d) \leq (d-1) N \log_d N.$$

Lemma 2. Let K, v, ϕ, d, and $r_{\phi,v}$ be as in Lemma 1. Assume that

$$r_{\phi,v} > \begin{cases} (4+\sqrt{3})(d-1) & \text{if } v \text{ is archimedean,} \\ 1 & \text{if } v \text{ is non-archimedean.} \end{cases}$$

Then there is an integer $1 \le m \le d-1$ and disjoint sets $V_1, V_2 \subseteq \mathbb{C}_v$ such that

- $\mathcal{K}_{\phi,v} = V_1 \cup V_2$,
- $\phi : V_1 \twoheadrightarrow \mathcal{K}_{\phi,v}$ is m-to-1,
- $\phi : V_2 \twoheadrightarrow \mathcal{K}_{\phi,v}$ is $(d-m)$-to-1, and
- For $x_1, \ldots, x_N \in V_1$,

$$\prod_{i \ne j} |x_i - x_j|_v \le B'_v(N) r_{\phi,v}^{(d-1)N[\log_d N - P_m(N)]},$$

where

$$P_m(N) = \frac{d-m}{m(d-1)} N - (1 - \log_d m).$$

and

$$B'_v(N) = \begin{cases} N^N (d-1)^{P_m(N)} & \text{if } v \text{ is archimedean,} \\ 1 & \text{if } v \text{ is non-archimedean.} \end{cases}$$

(Throw in the same correction factor if ϕ is not monic.)

Theorem: Sketch of Proof.
We can reduce to the case that ϕ monic.

For each $v \in M_K$, let $R_v = r_{\phi,v}^{n_v}$.

[Actually, adjust R_v slightly at archimedean v.]

Let $w \in M_K$ be the absolute value for which R_w is largest.

If V_1 contains N distinct rational preperiodic points

$$x_1, \ldots, x_N \in V_1 \subseteq \mathbb{C}_w,$$

then by the product formula,

$$1 = \prod_{i \neq j} \prod_{v \in M_K} |x_i - x_j|_v^{n_v} \leq \prod_{v \text{ bad}} \prod_{i \neq j} |x_i - x_j|_v^{n_v}$$

$$\leq \left[R_w^{-P_m(N)} \prod_{v \text{ bad}} R_v^{\log_d N} \right]^{(d-1)N} \cdot \prod_{v \text{ arch}} (B_v \text{ or } B_v')$$

$$\leq \left[R_w^{s \log_d N - P_m(N)} \right]^{(d-1)N} \cdot \prod_{v \text{ arch}} (B_v \text{ or } B_v')$$

Since $R_w > 1$, we only need to choose N large enough so that

$$s \log_d N - \frac{d-m}{m(d-1)} N + (1 - \log_d m) < 0$$

to get a contradiction.

Letting N be slightly bigger than

$$N_m = \frac{m(d-1)}{d-m} s \log_d s$$

does the trick.

Do the same for V_2. So if the **total** number of rational preperiodic points is at least $N_m + N_{d-m}$, we get a contradiction.

The worst case is $m = 1$, which gives a total number of points on the order of at most

$$[1 + (d-1)^2] s \log_d s = (d^2 - 2d + 2) s \log_d s.$$

Heights

The **standard height** on $\mathbb{P}^N(K)$ is

$$h([x_0, \ldots, x_N]) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{|x_0|_v, \ldots, |x_N|_v\}.$$

For $K = \mathbb{Q}$ and for $x_i \in \mathbb{Z}$ with $\gcd(x_0, \ldots, x_N) = 1$, we can write

$$h([x_0, \ldots, x_N]) = \log \max\{|x_0|_\infty, \ldots, |x_N|_\infty\}.$$

(Analogous definition for function fields.)

Key properties:

- If $\phi : \mathbb{P}^N \to \mathbb{P}^N$ is any morphism of degree d, then $h(\phi(x)) - d \cdot h(x)$ is a bounded function of x.
- (**Non-degeneracy**) For global fields K and any real number B, the set of K-points of height at most B is finite.

Canonical Heights

Given a morphism $\phi : \mathbb{P}^N \to \mathbb{P}^N$ defined over K of degree $d \geq 2$, the **canonical height** for ϕ on $\mathbb{P}^N(K)$ is

$$\hat{h}_\phi(x) = \lim_{n\to\infty} \frac{1}{d^n} h\left(\phi^n(x)\right).$$

We have:

- The limit converges.
- $\hat{h}_\phi - h$ is bounded.
- $\hat{h}_\phi(\phi(x)) = d \cdot \hat{h}_\phi(x)$.
- $\hat{h}_\phi(x) \geq 0$.
- For $N = 1$, ϕ a polynomial, and $x \neq \infty$:

  $$\hat{h}_\phi(x) = 0 \iff x \in \mathcal{K}_{\phi,v} \text{ for all } v \in M_K.$$

- If x is preperiodic, then $\hat{h}(x) = 0$.
- For global fields, if $\hat{h}(x) = 0$, then x is preperiodic.

Points of Small Canonical Height

a.k.a. "Almost" Preperiodic Points

Example. $\phi(z) = z^2 - \dfrac{181}{144}$

$$\frac{7}{12} \mapsto -\frac{11}{12} \quad \mapsto -\frac{5}{12} \quad \mapsto -\frac{13}{12} \quad \mapsto -\frac{1}{12}$$

$$\mapsto -\frac{5}{4} \quad \mapsto \frac{11}{36} \quad \mapsto -\frac{377}{324} \quad \mapsto \cdots$$

$\hat{h}_\phi(7/12) = 2^{-5}\log 3 = 0.03433\ldots$, vs.
$h(\phi) = h(181/144) = \log 181 = 5.198\ldots$
Ratio is $\hat{h}_\phi(7/12)/h(\phi) = 0.00660\ldots$

Example. $\phi(z) = z^2 - \dfrac{36989}{19600}$

$$\frac{153}{140} \mapsto -\frac{97}{140} \quad \mapsto -\frac{197}{140} \quad \mapsto \frac{13}{140} \quad \mapsto -\frac{263}{140}$$

$$\mapsto \frac{1609}{980} \quad \mapsto \frac{38821}{48020} \quad \mapsto \cdots$$

$\hat{h}_\phi(153/140) = 2^{-10}\log 5 + 2^{-4}\log 7 = 0.12319\ldots$, vs.
$h(\phi) = h(36989/19600) = \log 36989 = 10.518\ldots$
Ratio is $\hat{h}_\phi(153/140)/h(\phi) = 0.0117\ldots$

Another Point of Small Canonical Height

Example. $\phi(z) = -\frac{1}{24}z^3 + \frac{97}{24}z + 5$

$$-7 \quad \mapsto 19 \quad \mapsto -1 \quad \mapsto 1 \quad \mapsto 9$$

$$\mapsto 11 \quad \mapsto -6 \quad \mapsto -\frac{41}{4} \quad \mapsto \frac{4323}{512} \quad \mapsto \cdots$$

$\hat{h}_\phi(-7) = 0.0011\ldots$, vs.

$h(\phi) = \log(97) = 4.57\ldots$

Ratio is $\hat{h}_\phi(-7)/h(\phi) = 0.00025\ldots$

Conjecture. (Silverman)
Let K be a number field and $d \geq 2$.
There is a constant $C = C(K, d)$ such that if $\phi \in K(z)$ with $\deg \phi = d$, then for any non-preperiodic $P \in \mathbb{P}^1(K)$,

$$\hat{h}_\phi(P) \geq Ch(\phi).$$

Function Fields over Arbitrary Fields

Over a global field K, we have: $x \in \mathbb{P}^N(K)$ is preperiodic **iff** $\hat{h}_\phi(x) = 0$.

Idea of Proof: Preperiodic $\Longrightarrow$ height zero is easy.

The converse follows from non-degeneracy.

But for general function fields K (e.g. over $\mathbb{C}$), we don't have non-degeneracy.

Example.
$K = \mathbb{C}(T)$, and $\phi(z) = z^2$.
Then ϕ has countably many preperiodic points and uncountably many points of canonical height zero.

But, if there is at least one bad prime, then the same argument as the main Theorem still works:

Theorem. (RB, 2005.)
Let K be a function field over an arbitrary field $\mathbb{F}$, and let $\phi \in K[z]$ with $\deg \phi \geq 2$. Suppose that ϕ is not isotrivial, even after a K-rational change of coordinates. Then

$$x \in \mathbb{P}^1(K) \text{ is preperiodic } \textbf{iff } \hat{h}_\phi(x) = 0.$$

In fact, there are at most $O(s \log s)$ such points, where s is the number of bad primes

---

Extended:

- by Baker (2006) to rational functions on $\mathbb{P}^1$
- by Chatzidakis and Hrushovski (2007) to $\mathbb{P}^N$
- Cf. also Petsche, Szpiro, Tepper (2008) for $\mathbb{P}^N$

Dynamical Mordell Lang

Conjecture.
(Dynamical Mordell-Lang Conjecture; posed by Ghioca and Tucker, 2007)

Given:

- X, a quasiprojective variety over $\mathbb{C}$
- $V \subseteq X$, a subvariety
- $\Phi : X \to X$, a morphism
- $P \in X(\mathbb{C})$

Then $\{n \geq 0 : \Phi^n(P) \in V\}$ is a union of finitely many arithmetic progressions and finitely many other integers.

(Essentially) equivalently, if $V(\mathbb{C}) \cap \{\Phi^n(P) : n \geq 0\}$ is infinite, then there is a subvariety $W \subseteq V$ and an integer $m \geq 1$ such that $\Phi^m(W) \subseteq W$.

Theorem. (RB, Ghioca, Kurlberg, Tucker, 2007)
Suppose $X = (\mathbb{P}^1)^g$ and $\Phi = (\phi, \ldots, \phi)$, where

- $\phi \in \overline{\mathbb{Q}}(z)$,
- $V \subseteq X$ is a subvariety defined over $\overline{\mathbb{Q}}$,
- and $P \in X(\overline{\mathbb{Q}})$.

If V is a curve and ϕ has no non-exceptional periodic critical points,
OR
if V, P and ϕ are defined over $\mathbb{Q}$, and ϕ is a quadratic polynomial,

then $\{n \geq 0 : \Phi^n(P) \in V\}$ is a union of finitely many arithmetic progressions and finitely many other integers.

Idea of Proof:

- Find p at which everything has good reduction.
- The residue classes are the periodic points of $\overline{\phi}$.
- Use Rivera-Letelier's analysis of dynamics on periodic components to construct an integer k and power series

  $$F_{\ell,1}(z), \ldots, F_{\ell,g}(z) \in \mathbb{Z}_p[[z]]$$

  for all $\ell = 0, \ldots, k-1$ so that for all $n \geq 0$ large enough,

  $$\Phi^{\ell+nk}(P) = (F_{\ell,1}(n), \ldots, F_{\ell,g}(n)).$$

- Let $I(V) = \langle H_1, \ldots, H_m \rangle$ be the ideal of V.

  Let $G_{\ell,j} = H_j \circ (F_{\ell,1}, \ldots, F_{\ell,g}) \in \mathbb{Z}_p[[z]]$.

  For any n large enough,

  $$\Phi^{\ell+nk}(P) \in V \iff G_{\ell,j}(n) = 0 \text{ for all } j = 1, \ldots, m$$

- But a nontrivial power series in $\mathbb{Z}_p[[z]]$ can only have finitely many zeros in $\mathbb{Z}_p$.