Post-critically finite rational functions over number fields

Rafe Jones

Carleton college

September 26, 2013
Laboratoire de mathématiques de Besançon

Outline

I. Post-critically finite (PCF) maps: definitions and examples
II. Galois representations and finite ramification
III. A finiteness theorem for PCF maps over number fields:

Theorem (R. Benedetto, P. Ingram, RJ, A. Levy, 2013)

Let $d, B \in \mathbb{Z}$ with $d \geq 2$ and $B \geq 1$. Up to conjugacy, there are only finitely many PCF rational functions of degree d defined over a number field of degree at most B, except for flexible Lattès maps.

Setup

Let $\phi \in \mathbb{C}(z)$ be a rational function of degree $d \geq 2$.

Denote by ϕ^n the n-fold composition of ϕ with itself.

We say ϕ and ψ are *conjugate* if there is a Möbius transformation $f \in \mathrm{PGL}_2(\mathbb{C})$ with $f \circ \phi \circ f^{-1} = \psi$.

Setup, continued

Riemann-Hurwitz: counting multiplicity, ϕ has $2d-2$ critical points in $\mathbb{P}^1(\mathbb{C})$.

Definition

The *orbit* of $\alpha \in \mathbb{C}$ under ϕ is the set

$$O_\phi(\alpha) = \{\alpha, \phi(\alpha), \phi^2(\alpha), \ldots\}.$$

We say that ϕ is *post-critically finite* (PCF) if for every critical point γ of ϕ, the orbit $O_\phi(\gamma)$ is finite.

Every conjugate of a PCF map is PCF.

Examples

- $\phi(z) = z^d$. $\mathrm{Crit}_\phi = \{0, \infty\}$. $0 \mapsto 0$, $\infty \mapsto \infty$
- $\phi(z) = 1/z^2$. $\mathrm{Crit}_\phi = \{0, \infty\}$. $0 \mapsto \infty \mapsto 0$
- $\phi(z) = z^2 - 2$. $\mathrm{Crit}_\phi = \{0, \infty\}$. $0 \mapsto -2 \mapsto 2 \mapsto 2$, $\infty \mapsto \infty$
- $\phi(z) = z^2 - 1$. $\mathrm{Crit}_\phi = \{0, \infty\}$. $0 \mapsto -1 \mapsto 0$, $\infty \mapsto \infty$
- $\phi(z) = \frac{6z^2+16z+16}{-3z^2-4z-4}$. $\mathrm{Crit}_\phi = \{0, -2\}$.

$$0 \mapsto -4 \mapsto -4/3 \mapsto -4/3, \quad -2 \mapsto -1 \mapsto -2$$

- $\phi(z) = \frac{x^4+2x^2+1}{4x^3-4x}$. $\#\mathrm{Crit}_\phi = 6$.

Lattès maps

We say $\phi \in \mathbb{C}(z)$ is a *Lattès map* if there is an elliptic curve E, a morphism $\alpha : E \to E$, and a finite separable map π such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{\alpha} & E \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 & \xrightarrow[\phi]{} & \mathbb{P}^1 \end{array}$$

$$\begin{array}{ccc} E & \xrightarrow{\ \alpha\ } & E \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 & \xrightarrow[\ \phi\ ]{} & \mathbb{P}^1 \end{array}$$

Natural choices: let π be the double cover given by $\pi(P) = x(P)$, and let $\alpha = [m]$.

The resulting maps are called *flexible Lattès maps*.
If $\alpha = [m]$ for fixed m, and E varies, we obtain a family of non-conjugate maps.

$$\begin{array}{ccc} E & \xrightarrow{[m]} & E \\ \downarrow x & & \downarrow x \\ \mathbb{P}^1 & \xrightarrow[\phi_{E,m}]{} & \mathbb{P}^1 \end{array}$$

Claim: $\phi_{E,m}$ is PCF.

$[m]$ is unramified, so critical points of $\phi_{E,m}$ come from $P \neq Q$ with

$$x(P) = x(Q) \qquad \text{and} \qquad [m]P = [m]Q.$$

$x(P) = x(Q) \Rightarrow Q = -P$, so want $P \neq -P$ and $[m]P = [-m]P$

i. e., want $P \in E[2m] \setminus E[2]$

Thus $\mathrm{Crit}_{\phi_{E,m}} = \{x(P) : P \in E[2m] \setminus E[2]\}$.

For $n \geq 1$,

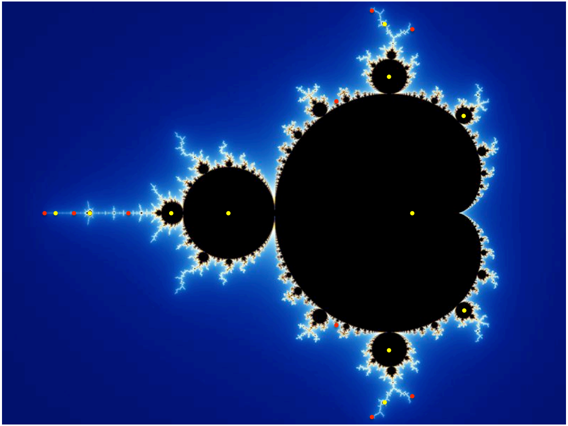
$$\phi_{E,m}^n(x(P)) = x([m^n]P).$$

If $P \in E[2m] \setminus E[2]$, then $[m^n]P \in E[2]$ for $n \geq 1$.

Therefore $\phi_{E,m}$ is PCF, as desired.

Example: $E : y^2 = x^3 - x, \ m = 2. \ \phi_{E,m} = \frac{x^4+2x^2+1}{4x^3-4x}$.

PCF maps in dynamics



Arboreal Galois representations

Let K be a number field, $\phi \in K(z)$, and $b \in \mathbb{P}^1(K)$.

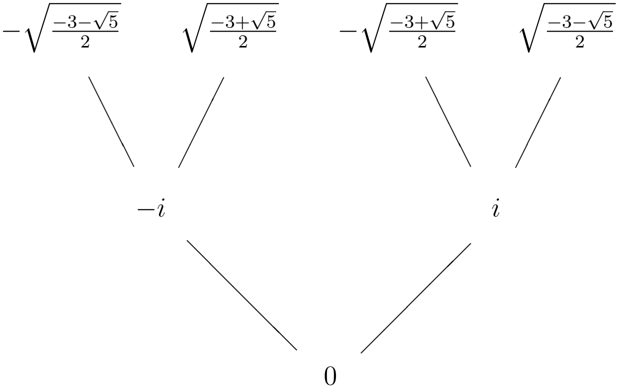
The *preimage tree* of ϕ with root b has vertex set

$$\bigsqcup_{i \geq 0} \phi^{-i}(b),$$

with two elements connected iff ϕ maps one to the other.

Denote this tree by T_∞, and its truncation to the nth level by T_n.

For simplicity, assume that T_∞ contains no critical points, so that it is a complete d-ary rooted tree.



First two levels of preimage tree of $f(x) = \frac{x^2+1}{x}$, $b = 0$.

Let $K_n = K(\phi^{-n}(b))$, and note $K_{n+1} \supseteq K_n$. Let $K_\infty = \bigcup K_n$.

Let $G_n = \mathrm{Gal}(K_n/K)$, and $G_\infty = \varprojlim G_n$. All these objects depend on ϕ and b, but to ease notation we don't make explicit reference to this dependence.

We have injections

$$G_n \hookrightarrow \mathrm{Aut}(T_n) \cong (S_d)^{\mathrm{wr(n)}} \qquad G_\infty \hookrightarrow \mathrm{Aut}(T_\infty).$$

The latter is the *arboreal Galois representation* associated to ϕ, b.

When $d = 2$, G_n is a 2-group, and G_∞ is a pro-2 group.

Lattès maps, once again

If $\phi_{E,m}$ is a flexible Lattès map and $b = \infty$, then

$$K_n = K(x(E[m^n])).$$

When $m = \ell$ is prime, then

$$G_\infty \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell),$$

and G_∞ is a subgroup of index at most 2 of the image of the ℓ-adic representation attached to E.

Finitely ramified representations

Theorem (Aitken-Hajir-Maire 2005, Hajir-Cullinan 2012)

Let K be a number field and $\phi \in K(z)$. If ϕ is PCF, then the extension K_∞/K is ramified over only finitely many primes of K.

Already known for Lattès maps $\phi_{E,\ell}$ with $b = \infty$: K_∞ can ramify only at ℓ and the primes of bad reduction for E.

Let $\phi(x) = p(x)/q(x)$ with p, q relatively prime.
Assume for simplicity that ∞ is not a critical point of ϕ and $b = 0$.
Then K_∞ can ramify only over primes of K dividing one of the following:

1. $\prod_\gamma \phi^i(\gamma)$, where the product is over the critical points γ of ϕ, and over i with $1 \leq i \leq n$.
2. The leading coefficient of $pq' - qp'$.
3. The leading coefficients of p and q.
4. The resultant of p and q.

When ϕ is a monic polynomial, (3) and (4) in the above list are both 1, and (2) is just the degree of ϕ.

Example Let $K = \mathbb{Q}$ and $\phi(x) = x^2 - 2$. $0 \mapsto -2 \mapsto 2 \mapsto 2$
K_∞ is ramified over $\mathbb{Q}$ only at the prime 2.

$K_n = \mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})$. So $G_n \cong \mathbb{Z}/2^n\mathbb{Z}$, $G_\infty \cong \mathbb{Z}_2$.

Example Let $K = \mathbb{Q}$ and $\phi(x) = (x+1)^2 - 2$. $-1 \mapsto -2 \mapsto -1$
K_∞ is ramified over $\mathbb{Q}$ only at 2 and ∞.

$\# G_2 = 2^3$
$\# G_3 = 2^6$
$\# G_4 = 2^{11}$
$\# G_5 = 2^{22}$
$\# G_6 = 2^{43}$ (J. Klüners)
$\# G_7 = 2^{86}$?
$\# G_8 = 2^{171}$?

Question: Does there exists a number field K and a PCF map $\phi \in K(x)$ of degree 2 such that K_∞ is unramified at 2?

An overgroup for G_∞

Return to an arbitrary number field K. Instead of $b = 0$, take $b = t$, where t is transcendental over K, and work over $K(t)$.

Let $\phi \in K(x)$ be post-critically finite, and put

$$K_{n,t} := K(t)(\phi^{-n}(t)) \qquad G_n^{K(t)} := \mathrm{Gal}(K_{n,t}/K(t)).$$

The isomorphism class of $G_\infty^{K(t)}$ is invariant under conjugation of ϕ. It contains G_∞ as a subgroup (specialization $t = b$).

We have an exact sequence

$$1 \to G_\infty^{\mathbb{C}(t)} \to G_\infty^{K(t)} \to \mathrm{Gal}(L/K) \to 1,$$

where $L = \overline{K} \cap K_{\infty,t}$.

The group $G_\infty^{\mathbb{C}(t)}$ is the *profinite iterated monodromy group* of $f(x)$.

It is a (topologically) finitely generated group satisfying a property known as self-similarity.

The action of its generators on T_∞ is given by an explicitly computable finite automaton, which can be calculated via a beautiful theory involving lifts of loops in $\mathbb{C}$. (V. Nekrashevych)

Example: $K = \mathbb{Q}$, $\phi(x) = x^2 - 2$. Then $G_\infty^{\mathbb{C}(t)}$ is the pro-2 completion of the infinite Dihedral group D_∞.

Example: $K = \mathbb{Q}$, $\phi(x) = x^2 - 1$. Then $G_\infty^{\mathbb{C}(t)}$ is the pro-2 completion of the *Basilica group* B. Note that $(x+1)^2 - 2$ is conjugate to $x^2 - 1$ by $x \mapsto x + 1$.

Recent work of R. Pink shows that $G_\infty^{K(t)}$ is also a self-similar group.

Moreover, if ϕ is a (PCF) quadratic polynomial whose finite critical point does not have a periodic orbit, then $G_\infty^{\mathbb{C}(t)}$ is isomorphic to a subgroup of $G_\infty^{K(t)}$ of index at most 4.

Theorem (R. Benedetto, P. Ingram, RJ, A. Levy, 2013)

Let $d, B \in \mathbb{Z}$ with $d \geq 2$ and $B \geq 1$. Up to conjugacy, there are only finitely many PCF rational functions of degree d defined over a number field of degree at most B, except for flexible Lattès maps.

Corollary (M. Manes, D. Yap, 2013)

Suppose that $\phi \in \mathbb{Q}(z)$ is quadratic and PCF. Then ϕ is conjugate to one of the following:

$$\begin{array}{cccc} z^2 & z^2 - 2 & z^2 - 1 & 1/z^2 \\ \frac{1}{(z-1)^2} & \frac{1}{2(z-1)^2} & \frac{2}{(z-1)^2} & \frac{-1}{4z^2-4z} \\ \frac{-4}{9z^2-12z} & \frac{2z+1}{4z-2z^2} & \frac{-2z}{2z^2-4z+1} & \frac{3z^2-4z+1}{1-4z} \end{array}$$

Moreover, none of these twelve is conjugate to any of the others.

Multipliers

Let K be a field, $\phi \in K(z)$.

Let $\gamma \in \mathbb{P}^1(K)$ be a fixed point of ϕ. The *multiplier* of γ is $\lambda := \phi'(\gamma) \in K$. The set of multipliers of the fixed points of ϕ is invariant under conjugation of ϕ.

Changing coordinates so $\gamma = 0$, we have

$$\phi(z) = \lambda z + \text{higher order terms}$$

in some neighborhood of zero.

We say γ is *attracting* with respect to an absolute value $|\cdot|$ on K if $|\lambda| < 1$.

Extend these definitions to n-periodic points of ϕ by considering them as fixed points of ϕ^n.

McMullen's theorem

For $\phi \in \mathbb{C}(z)$, denote by $M_n(\phi)$ the unordered set of multipliers of all n-periodic points of ϕ.

Theorem (McMullen, 1987)

For fixed $d \geq 2$, there exists $N_d \geq 1$ such that the set

$$\mathcal{M}(N_d) := M_1(\phi) \sqcup M_2(\phi) \sqcup \cdots \sqcup M_{N_d}(\phi)$$

determines the conjugacy class of ϕ up to finitely many choices, unless ϕ is a flexible Lattès map.

Special bonus (Milnor): $N_2 = 1$, and $\mathcal{M}(1)$ uniquely determines the conjugacy class of ϕ when ϕ is quadratic.

Proof strategy

By Thurston rigidity, the multipliers of a PCF map $\phi \in \mathbb{C}(z)$ all lie in $\overline{\mathbb{Q}}$. Thus if ϕ is PCF of degree d, then $\mathcal{M}(N_d) \subset (\overline{\mathbb{Q}})^k$ for some positive integer k.

- If ϕ is PCF of degree d, show that $\mathcal{M}(N_d)$ belongs to a set of bounded height.
- Observe that If ϕ is defined over a number field of degree at most B, then $\mathcal{M}(N_d)$ is defined over a number field of degree at most B'.
- By standard properties of height, there are only finitely many possibilities for $\mathcal{M}(N_d)$.
- From McMullen's theorem, conclude that ϕ belongs to a finite collection of conjugacy classes.

Definition

The *height* of $\alpha \in K$, where K is a finite extension of $\mathbb{Q}$, is defined by

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

where M_K denotes the set of absolute values of K, and K_v denotes the completion of K with respect to the absolute value v.

- $h(\alpha)$ is invariant under finite extensions of K, so $h : \overline{\mathbb{Q}} \to \mathbb{R}$ is well-defined.
- for $A, B \in \mathbb{Z}_{\geq 0}$, there are only finitely many $\alpha \in \overline{\mathbb{Q}}$ satisfying both

$$h(\alpha) \leq A \quad \text{and} \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq B.$$

A non-archimedean version of a theorem of Fatou

Theorem (Fatou, 1920)

Let $\phi \in \mathbb{C}(z)$. A cycle of ϕ whose multiplier satisfies $|\lambda| < 1$ strictly attracts a critical point of ϕ.

Key observation: a PCF rational function ϕ cannot have any critical points strictly attracted to a cycle. So every multiplier of ϕ satisfies $|\lambda| \geq 1$.

Hope: prove that if ϕ is defined over a number field K, in fact $|\lambda| \geq 1$ for every absolute value on K.

Example: $\phi(z) = z^p$. *Every* cycle is attracting with respect to the p-adic absolute value.

Example: $\phi(z) = z^2 - 4z$. The fixed point 0 has multiplier 4, and so is 2-adically attracting. But $2 \mapsto -4 \mapsto 0$, so 0 does not strictly attract a critical point.

Theorem (Benedetto-Ingram-J-Levy)

Let $\phi \in L(z)$, where L has characteristic zero, residue characteristic p, and is complete with respect to a non-archimedean absolute value $|\cdot|_p$. There exists $\epsilon_p \leq 1$ such that any cycle whose multiplier satisfies $|\lambda|_p < \epsilon_p$ strictly attracts a critical point. Moreover, if $p > d$, then $\epsilon_p = 1$.

More precisely, we can take

$$\epsilon_p = \min\{|m|_p^d : 1 \leq m \leq d\}.$$

Example: When $d = 2$, $\epsilon_2 = 1/4$ and $\epsilon_p = 1$ for $p \geq 3$. Note the bound of $1/4$ cannot be improved.

This shows that if λ is the multiplier of a fixed point of a quadratic rational map $\phi \in \mathbb{C}(z)$, then $h(\lambda) \leq \log 4$.