Arboreal Galois Representations

Rafe Jones

Carleton college

November 9, 2014
UNC-Greensboro

Outline

I. (Dynamical) Arboreal Galois Representations: introduction
II. Image: examples and conjectures
III. Ramification
IV. Image: number of orbits.

Arboreal Galois representations

Let K be a number field with absolute Galois group G_K.

An *arboreal Galois representation* is a continuous homomorphism

$$\rho : G_K \to \mathrm{Aut}(T),$$

where T is a locally finite rooted tree, and $\mathrm{Aut}(T)$ is the group of tree automorphisms of T.

Arboreal Galois representations from dynamics

Let $\phi \in K(z)$ have degree $d \geq 2$, let $b \in \mathbb{P}^1(K)$, and denote by ϕ^n the n-fold composition of ϕ with itself. Put

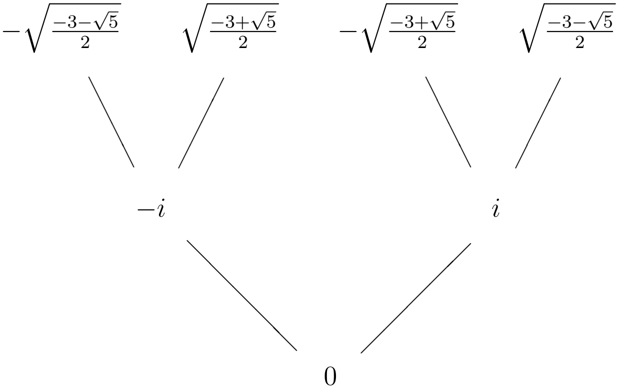
$$\phi^{-i}(b) = \{\beta \in \overline{\mathbb{Q}} : \phi^i(\beta) = b\}.$$

The *preimage tree* of ϕ with root b is

$$T_\infty := \bigsqcup_{i \geq 0} \phi^{-i}(b),$$

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

Denote the truncation of T_∞ to the nth level by T_n.



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

Then G_K acts naturally on T_∞ as tree automorphisms (since ϕ is defined over K), giving

$$\rho_{\phi,b} : G_K \to \mathrm{Aut}(T_\infty).$$

Denote the image of $\rho_{\phi,b}$ by G_∞, and note that

$$G_\infty = \varprojlim G_n,$$

where $G_n = \mathrm{Gal}(K(\phi^{-n}(b))/K)$.

Put $K_n = K(\phi^{-n}(b))$ and $K_\infty = \bigcup_{n \geq 1} K_n$.

Example 1: Lattès maps

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

Let $\phi = \phi_{E,\ell}$ and $b = \infty$. Then $\phi_{E,\ell}^{-n}(\infty) = x(E[\ell^n])$.

Hence G_n is a subgroup of index at most two in $\mathrm{Gal}(K(E[\ell^n])/K)$.

Thus the arboreal and ℓ-adic representations have nearly identical image.

Example 2: A map with no special structure at all

Let $K = \mathbb{Q}, \phi(x) = x^2 + 1$, and $b = 0$.

In the 80s, Odoni conjectured that $G_\infty = \mathrm{Aut}(T_\infty)$, or equivalently $G_n \cong \mathrm{Aut}(T_n)$ for all $n \geq 1$.

He showed that $G_n \cong \mathrm{Aut}(T_n)$ provided that in the sequence $\phi^2(0), \phi^3(0), \ldots, \phi^n(0)$, each term has a primitive prime divisor appearing to odd multiplicity.

In 1990, Cremona used this to show $G_n \cong \mathrm{Aut}(T_n)$ for $n = 5 \cdot 10^7$.

$$\log_2 |\mathrm{Aut}(T_{5 \cdot 10^7})| = 32^{10000000} - 1.$$

In 1992, Stoll used an ingenious trick to prove Odoni's conjecture.

Example 3: A map with a small critical orbit

Let $K = \mathbb{Q}, \phi(x) = (x+1)^2 - 2$, and $b = 0$.

Then K_∞ contains $\mathbb{Q}(\zeta_{2^\infty})$, and $\mathrm{Gal}(K_\infty/\mathbb{Q}(\zeta_{2^\infty}))$ is generated by two elements.

Reason: the orbit under f of the critical point is $-1 \to -2 \to -1 \to \cdots$. Thus ϕ is *post-critically finite* (PCF)

One can show $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$.

Conjecture (Boston-RJ): $\frac{\log_2(\# G_n)}{\log_2(\# \mathrm{Aut}(T_n))} \to 2/3$.

Example 4: A map with a non-trivial automorphism

Let $K = \mathbb{Q}, \phi(x) = \frac{x^2+1}{x}$, and $b = 0$.

Then $\mu : x \to -x$ commutes with ϕ, and $\mu(b) = b$.

Thus G_∞ commutes with the action of μ on T_∞, and we have

$$G_\infty \leq C,$$

where C is the centralizer in $\mathrm{Aut}(T_\infty)$ of the action of μ.

$[\mathrm{Aut}(T_\infty) : C] = \infty$, but C contains an index-two subgroup isomorphic to $\mathrm{Aut}(T_\infty)$.

Theorem (RJ-Manes 2014]): $G_\infty = C$.

Open image conjecture for quadratics

Conjecture (RJ 2013)

Let $\phi \in K(x)$ have degree two and critical points $\gamma_1, \gamma_2 \in \mathbb{P}^1(K)$. Then $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$ iff one of the following holds:

1. There is a non-trivial Möbius transformation that commutes with ϕ and fixes b.
2. ϕ is post-critically finite (this includes Lattés maps).
3. γ_1 and γ_2 of ϕ have a relation of the form $\phi^{r+1}(\gamma_1) = \phi^{r+1}(\gamma_2)$ for some $r \geq 1$.
4. The root b of T_∞ is periodic under ϕ.

What is known

- If any of conditions 1-4 hold, then $[\mathrm{Aut}(T_\infty) : G_\infty(\phi)] = \infty$ (Pink, RJ-Manes).
- Conjecture holds for $\phi(x) = x^2 - kx + k, k \in \mathbb{Z} \setminus \{0, 2\}$ and $\phi(x) = x^2 - kx + 1, k \in \mathbb{Z} \setminus \{0, 2\}$ (RJ 2008).
- If $\phi(x) = x^2 + c$ with $c \neq 2$, $-c$ not a square, then ABC implies $\rho_{\phi,b}$ is surjective (Gratton-Nguyen-Tucker 2013).

If ϕ satisfies one of conditions 1-4, then there is an over-group in which G_∞ ought to have finite index. This group is well-understood (RJ-Manes, Pink, Swaminathan).

More of what is known

Theorem (Hindes 2014)

Replace K by $K(t)$. Let $\phi(x) = x^2 + c \in K(t)[x]$ with c a non-constant polynomial in t. Then

$$[\mathrm{Aut}(T_\infty) : G_\infty] \leq 2^{65519}.$$

Application: prime divisors of recurrence sequences

Let $\phi(x) \in K[x]$ and $a_0 \in K$. Let

$$P(\phi, a_0) = \{\mathfrak{p} : \mathfrak{p} \mid \phi^n(a_0) \text{ for at least one } n \geq 1\}.$$

Suppose that $b = 0$ and

$$\lim_{n\to\infty} \frac{\#\{g \in G_n : g \text{ fixes at least one element of } \phi^{-n}(0)\}}{\# G_n} = 0.$$

Then the natural density of $P(\phi, a_0)$ is zero (independent of a_0).

Odoni showed that if $G_\infty = \mathrm{Aut}(T_\infty)$, the limit on the previous slide is indeed zero.

Problem: give conditions on a subgroup $G \leq \mathrm{Aut}(T_\infty)$ that ensure this limit is zero.

Some well-known orbits:

- $\phi(x) = (x-1)^2 + 1$, $a_0 = 3$: $3, 5, 17, 257, 65537, \ldots$
- $\phi(x) = x^2 - x + 1, a_0 = 2$: $2, 3, 7, 43, 1807, \ldots$
- $\phi(x) = x^2 - 2, a_0 = 4$: $4, 14, 194, 37634, \ldots$
  Lucas-Lehmer test: M_p is prime iff $M_p \mid \phi^{p-2}(a_0)$.

Frobenius conjugacy classes

Problem: given a prime $\mathfrak{p}$ of K, associate a meaningful invariant to the image of the Frobenius conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ in G_∞.

One idea (Boston-RJ): study the cycle type of the action of $\mathrm{Frob}_{\mathfrak{p}}$ on $\phi^{-n}(b)$, and let $n \to \infty$.

Consider the set of "ends" $E := \varprojlim (\phi^{-n}(b))$ of T_∞, which has a natural probability measure that is the inverse limit of the uniform probability measure on $\phi^{-n}(b)$ for each $n \geq 1$.

We conjecture that every orbit of the action of $\mathrm{Frob}_{\mathfrak{p}}$ on E has positive measure, giving a (possibly infinite) partition of 1.

Ramification

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.

Finitely ramified representations

Recall that ϕ is *post-critically finite* (PCF) if for every critical point γ of ϕ, the orbit $\{\gamma, \phi(\gamma), \phi^2(\gamma), \ldots\}$ is finite.

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

Let K be a number field and $\phi \in K(x)$. 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.

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)
$\#G_7 = 2^{86}$ (J. Klüners, M. Watkins)
$\#G_8 = 2^{171}$?

Observation: If $\phi(x) = x^2 + c (c \in \overline{\mathbb{Q}})$ is PCF, then taking $K = \mathbb{Q}(c)$, we have that K_∞/K is unramified away from primes over 2.

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

Theorem (Benedetto-Ingram-RJ-Levy, 2014)

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 (Manes-Lukas-Yap, 2014)

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

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

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

Definitions

Definition

Let $\phi \in K(x), b \in K$ and write $\phi^n(x) = p_n(x)/q_n(x)$ with $(p_n, q_n) = 1$. The pair (ϕ, b) is *stable* if $p_n(x) - bq_n(x)$ is irreducible over K for all $n \geq 1$, and *eventually stable* if the number of irreducible factors of $p_n(x) - bq_n(x)$ remains bounded as n grows.

Equivalently, (ϕ, b) is stable (resp. eventually stable) if G_K acts on E with a single orbit (resp finitely many orbits).

If ϕ is a polynomial, we say ϕ is stable if $(\phi, 0)$ is stable, i.e. all iterates of ϕ are irreducible.

Some results on stability

Fun exercise: if $\phi \in \mathbb{Z}[x]$ is Eisenstein, then so is $\phi^n(x)$ for all $n \geq 1$, and hence ϕ is stable.

Theorem (Fein-Danielson 2001)

Let $\phi(x) = x^d - b \in \mathbb{Z}[x]$. If ϕ is irreducible, then ϕ is stable.

Theorem (RJ 2012)

Let $\phi(x) \in \mathbb{Z}[x]$ be quadratic with critical point $\gamma \in \mathbb{Z}$. If $\phi(x)$ is irreducible and $\phi(\gamma)$ is odd, then ϕ is stable.

Main tool: fact that if none of $\phi^2(\gamma), \phi^3(\gamma), \ldots \phi^n(\gamma)$ is a square, then $\phi^n(x)$ is irreducible.

Cautionary examples

1. $\phi(x) = x^2 + 10x + 17$ is irreducible over $\mathbb{Q}$. But
$$\phi^2(x) = (x^2 + 8x + 14)(x^2 + 12x + 34).$$
2. $\phi(x) = x^2 - x - 1$ is irreducible, and so is $\phi^2(x)$. But
$$\phi^3(x) = (x^4 - 3x^3 + 4x - 1)(x^4 - x^3 - 3x^2 + x + 1)$$
3. $\phi(x) = x^2 - \frac{16}{9}$ has
$$\phi^3(x) = \left(x^2 - 2x + \frac{2}{9}\right)\left(x^2 + 2x + \frac{2}{9}\right)\left(x^2 - \frac{22}{9}\right)\left(x^2 - \frac{10}{9}\right).$$

Eventual stability conjecture

Conjecture (RJ-Levy 2014)

Let K be a number field. If $\phi \in K(x)$ and $b \in K$ is not periodic under ϕ, then (ϕ, b) is eventually stable.

A few results

Theorem (Ingram 2013)

Let $\phi \in K[x]$ be monic polynomial of degree $d \geq 2$. If there is a prime $\mathfrak{p}$ of K with $\mathfrak{p} \nmid d$ and $|\phi^n(b)|_{\mathfrak{p}} \to \infty$ as $n \to \infty$. Then (ϕ, b) is eventually stable.

Theorem (Hamblen-RJ-Madhu 2014)

Let $\phi(x) = x^d + c \in K[x]$ with $c \neq 0$. If there is a prime $\mathfrak{p}$ of K with $|c|_{\mathfrak{p}} < 1$, then $(\phi, 0)$ is eventually stable over K.

Using similar ideas, can show that if $\phi(x) \in \mathbb{Z}[x]$ and $\phi(x) \equiv x^d \bmod p$ for some p, then $(\phi, 0)$ is eventually stable.

Question: let $\phi(x) = x^2 + 1/k$ for $k \in \mathbb{Z} \setminus \{0\}$. Is $(\phi, 0)$ eventually stable?