Galois actions on preimage trees

Rafe Jones

College of the Holy Cross

July 23, 2009

Motivating problem: prime divisors of polynomial orbits

Let $f \in \mathbb{Z}[x]$, and denote the nth iterate of f by f^n.

Let $O_f(a) = \{f^n(a) : n = 0, 1, 2, \ldots\}$ denote the orbit of $a \in \mathbb{Z}$ under f. The orbits of f can hold great number-theoretic interest.

Examples:

- $f(x) = (x-1)^2 + 1 = x^2 - 2x + 2.$

  $O_f(3) = \{3, 5, 17, 257, 65537, \ldots\}$.
  Fermat numbers ($F_n = 2^{2^n} + 1$).

- $f(x) = x^2 - x + 1.$

  $O_f(2) = \{2, 3, 7, 43, 1807, \ldots\}$
  Sylvester's sequence ($s_0 = 2, s_n = s_0 \cdots s_{n-1} + 1$).

Problem of recurrent interest: show various sequences have infinitely many prime terms.

Dirichlet: $(cn + d)_{n \geq 1}$ contains infinitely many primes (provided $(c, d) = 1$).

Open problems: show $(n^2 + 1)_{n \geq 1}$ contains infinitely many primes. Show the Fibonacci sequence contains infinitely many primes.

Conjecture (Fermat)

F_n is prime for all n

Slightly Revised Conjecture

F_n is composite for all $n \geq 5$.

Rather than investigate prime terms in polynomial orbits, we consider the set of all primes dividing at least one term of a given orbit:

$$P(O_f(a)) = \{p \text{ prime} : p \text{ divides some element of } O_f(a)\}$$

(Can extend to rational functions by considering p dividing the numerator of some element of the orbit.)

By the *natural upper density* of a set of primes $S \subset \mathbb{Z}$, we mean

$$D(S) = \limsup_{x \to \infty} \frac{\#\{p \in S : p \leq x\}}{\#\{p : p \leq x\}},$$

Our main affair is to determine $D(P(O_f(a)))$ in various cases.

Main Theorem (RJ, RJ-Manes)

The following $f \in \mathbb{Q}(x)$ satisfy $D(P(O_f(a))) = 0$ for all $a \in \mathbb{Z}$:

- $x^2 - kx + k$ for $k \in \mathbb{Z}$
- $x^2 - kx + 1$ for $k \in \mathbb{Z} \setminus \{0, 2\}$
- $x^2 + k$ for $k \in \mathbb{Z} \setminus \{-1\}$
- $\frac{k(x^2+1)}{x}$ for odd $k \in \mathbb{Z}$ having no prime factor $\equiv 1 \bmod 4$

Connections with Galois theory

Lemma

Fix $n \geq 1$ and $f \in \mathbb{Z}[x]$, and let

$$d_n = 1 - D(p : f^n(x) \equiv 0 \bmod p \text{ has no solution in } \mathbb{Z}).$$

Then for any $a \in \mathbb{Z}$, $D(P(O_f(a))) < d_n$.

Proof sketch: $f^n(x) \equiv 0 \bmod p$ has no solution implies $p \nmid f^m(a)$ for all $m \geq n$. There are only finitely many p for which $p \mid f^m(a)$ for some $m < n$.

Lemma

Let G_n be the Galois group of the splitting field of $f^n(x)$ over $\mathbb{Q}$, and recall G_n acts naturally on the roots of f^n. We have

$$d_n = \frac{1}{\#G_n}\#\{\sigma \in G_n : \sigma \text{ fixes at least one root of } f^n\}.$$

Proof: Classical application of the Chebotarev Density theorem.

Conclusion: $D(P(O_f(a)))$ is bounded above by

$$\frac{1}{\#G_n}\#\{\sigma \in G_n : \sigma \text{ fixes at least one root of } f\}.$$

Remark: A similar statement holds for $f \in \mathbb{Q}(x)$, provided that $f(\infty) = \infty$.

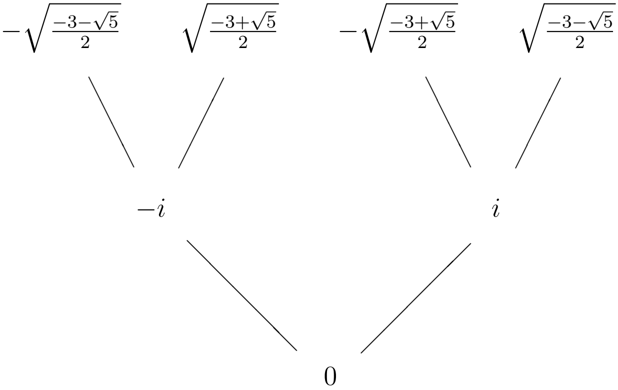
Arboreal representations

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

The *preimage tree* of f with root b has as vertices

$$\bigsqcup_{n \geq 1} f^{-n}(b),$$

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



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

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

Let T_∞ be the full preimage tree of f and T_n its truncation to the nth level. Since f has coefficients in K, G_n respects the connectivity relation in T_n, giving natural injections

$$G_n \hookrightarrow \mathrm{Aut}(T_n) \qquad G_\infty \hookrightarrow \mathrm{Aut}(T_\infty).$$

Remark: in the typical case that b avoids the orbits of all critical points of f, T_∞ is the complete $(\deg f)$-ary rooted tree, and $\mathrm{Aut}(T_\infty)$ is a well-understood group.

Example: Let T_2 be the complete binary rooted tree of height 2, and label the vertices at the top level of T_2 by $1, 2, 3, 4$. Then $\mathrm{Aut}(T_2) \cong$
$\{e, (12), (34), (12)(34), (1324), (1423), (13)(24), (14)(23)\} = D_4$.

In general for T_n the complete binary rooted tree of height n, $\mathrm{Aut}(T_n)$ is the n-fold iterated wreath product of $\mathbb{Z}/2\mathbb{Z}$.

Aside on conjugacy-invariance: the group G_∞ associated to (f, b) is the same as the group associated to $(\psi \circ f \circ \psi^{-1}, \psi(b))$, for any $\psi \in PGL_2(K)$. However, we often wish to keep b constant and let f vary, and in such a case we can only use ψ that fix b.

Generalizations

One can generalize this construction by replacing V by an algebraic variety and f by a finite morphism.

When $V = E$ is an elliptic curve, $f = [\ell]$ for a prime ℓ, and $b = O$, $G_\infty \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ is the image of the ℓ-adic linear Galois representation associated to E. Serre showed that if E does not have complex multiplication, then $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G_\infty]$ is finite.

When V is a commutative algebraic group and f is multiplication by n, determining G_∞ amounts to doing Kummer theory on V.

For remainder of the talk, we return to the case $V = \mathbb{P}^1$, and we let $b = 0$.

Questions: For which $f \in K(x)$ can one determine G_∞? When does G_∞ have finite index in $\mathrm{Aut}(T_\infty)$?

Results of Odoni

Theorem (Odoni 1985)

Let $f(x) \in K(t_0, \ldots, t_d)[x]$ be the generic polynomial of degree d over K. Then $G_\infty \cong \mathrm{Aut}(T_\infty)$.
In particular, if n is fixed then for all but a 'thin set' of degree d $f \in K[x]$ we have $G_n \cong \mathrm{Aut}(T_n)$.

Theorem (Odoni 1985)

Let $f(x) = x^2 - x + 1$. Then $G_\infty \cong \mathrm{Aut}(T_\infty)$

Quadratic polynomials

Theorem (RJ)

Let $f \in \mathbb{Z}[x]$ be monic and quadratic. Suppose all iterates of f are irreducible over $\mathbb{Q}$, f is not post-critically finite, and 0 is pre-periodic (but not periodic) under f. Then G_∞ has finite index in $\mathrm{Aut}(T_\infty)$.

The above theorem applies to $f(x) = x^2 - kx + k$ for all $k \in \mathbb{Z}$ except $-2, 0, 2$, and 4, for which G_∞ is either degenerate ($k = 0$) or explicitly computable and of infinite index in $\mathrm{Aut}(T_\infty)$.

It also applies to $f(x) = x^2 + kx - 1$ for all $k \in \mathbb{Z}$ except $-1, 0$, and 2. When $k = -1$, $f^3(x)$ is reducible, but nonetheless one can show G_∞ has finite index in $\mathrm{Aut}(T_\infty)$. For $k = 0$ and 2, G_∞ remains unknown, but appears to have infinite index in $\mathrm{Aut}(T_\infty)$.

Theorem (Stoll 1992)

Let $f = x^2 + k \in \mathbb{Z}[x]$ where $-k$ is not a square, and suppose that one of the following holds:

- $k > 0, k \equiv 1 \bmod 4$
- $k > 0, k \equiv 2 \bmod 4$
- $k < 0, k \equiv 0 \bmod 4$

Then $G_\infty \cong \mathrm{Aut}(T_\infty)$.

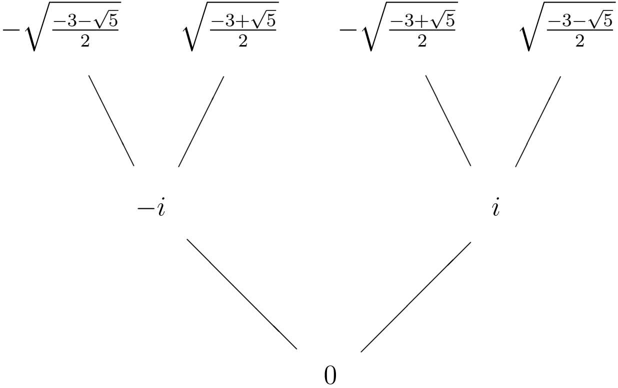
Remark: for $f = x^2 + 3$, $[\mathrm{Aut}(T_\infty) : G_\infty] \geq 2$. Not known to be finite.

Quadratic rational functions with non-trivial automorphisms

The case where $f \in K(x)$ commutes with a non-trivial $\psi \in \mathrm{PGL}_2(K)$, and a is a fixed point of ψ, is analogous to the case of an elliptic curve with complex multiplication.

In recent work with M. Manes, we study the family $f = \frac{k(x^2+1)}{x}$, $k \in \mathbb{Z}$, which has $\psi(x) = -x$ (recall our running assumption $b = 0$). Here, $G_\infty \hookrightarrow C_\infty$, where C_∞ is the subgroup of $\mathrm{Aut}(T_\infty)$ commuting with the action of ψ on T_∞.

For all n, C_n has a subgroup of index two isomorphic to $\mathrm{Aut}(T_{n-1})$.


$-\sqrt{\frac{-3-\sqrt{5}}{2}}$
$\sqrt{\frac{-3+\sqrt{5}}{2}}$
$-\sqrt{\frac{-3+\sqrt{5}}{2}}$
$\sqrt{\frac{-3-\sqrt{5}}{2}}$
$-i$
i
0

Theorem (RJ-Manes)

There is a density 0 set of primes $S \subset \mathbb{Z}$ such that if $k \in \mathbb{Z}$ is not divisible by any $s \in S$ and $f = \frac{k(x^2+1)}{x}$, then $G_\infty \cong C_\infty$.

Notes: S is the set of primes dividing the numerator of $f^n(1)$ for some $n \geq 1$, where $f = \frac{(x^2+1)}{x}$. All p in S are $\equiv 1 \pmod 4$.

Counting elements with fixed points

Recall: $D(P(O_f(a)))$ is bounded above by

$$d_n = \frac{1}{\#G_n} \#\{\sigma \in G_n : \sigma \text{ fixes at least one root of } f\}.$$

Suppose $G_\infty \cong \mathrm{Aut}(T_\infty)$.

$G_1 \cong \{e, (12)\}$. $d_1 = 1/2$
$G_2 \cong \{e, (12), (34), (12)(34), (1324), (1423), (13)(24), (14)(23)\}$.
$d_2 = 3/8$
$d_3 = 39/128$

Let $e_n = 1 - d_n$. Then one can show $e_n = \frac{1}{2}e_{n-1}^2 + \frac{1}{2}$.

It follows that $e_n \to 1$, and thus $d_n \to 0$. A similar argument can be used to show that $d_n \to 0$ when $G_\infty \cong C_\infty$. This proves the main theorem in the case $f = \frac{k(x^2+1)}{x}$ for certain k.

Let $f \in \mathbb{Z}[x]$ be quadratic with f^n irreducible, and let $H_n = \mathrm{Gal}(K_n/K_{n-1})$. Since $K_n = K_{n-1}(f^{-1}(\alpha))$ as α runs over $f^{-(n-1)}(b)$, we have $H_n \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}$. Call H_n *maximal* if this injection is an isomorphism.

Theorem (RJ)

Suppose that f is quadratic, f^n is irreducible for all n, and H_n is maximal for infinitely many n. Then $d_n \to 0$.

In particular, if f^n is irreducible for all n, and $[\mathrm{Aut}(T_\infty) : G_\infty] < \infty$, then the set of prime divisors of any orbit of f has density zero. This can be used to prove the Main Theorem in the cases $f = x^2 - kx + k$, $k \in \mathbb{Z}$, and $f = x^2 - kx + 1, k \in \mathbb{Z} \setminus \{0, 2\}$.

The hypothesis that H_n be maximal for infinitely many n is much weaker than $[\mathrm{Aut}(T_\infty) : G_\infty] < \infty$, and can be made to apply in cases where the latter is unknown.

For instance, $f(x) = x^2 + k \in \mathbb{Z}[x]$, where $-k$ is not a square, proving the main theorem in this case.

Also, $f(x) = x^2 + t \in \mathbb{F}_p(t)[x]$.

Further directions and open problems

Conjecture

Suppose that $f = x^2 + ax + b \in \mathbb{Z}[x]$ with critical point γ, and suppose that $O_f(\gamma)$ is infinite and f^n is irreducible for all n. Then for any $a \in \mathbb{Z}$,

$$D(P(O_f(a))) = 0.$$

Bad example: $f(x) = (x + 945)^2 - 945 + 3$, $\gamma = -945$.

$f(\gamma) = 2 \cdot 3 \cdot 157$
$f^2(\gamma) = 3 \cdot 311$
$f^3(\gamma) = 2 \cdot 3 \cdot 7 \cdot 19$
$f^4(\gamma) = 3 \cdot 83^2$
$f^5(\gamma) = 2 \cdot 3 \cdot 103 \cdot 755789$

The results showing G_∞ is a large subgroup of $\mathrm{Aut}(T_\infty)$ for quadratic $f \in \mathbb{Q}(x)$ rely on f not being post-critically finite. In the absence of this, the group G_∞ is often mysterious.

Polynomials conjugate to $x^2 - 1$ provide particularly interesting examples: in the case of $f(x) = (x+1)^2 - 2$, K_∞ is ramified over $\mathbb{Q}$ only at the prime 2.

Analogies with linear representations

In the case of a linear Galois representation $\rho : G_\infty \hookrightarrow GL_2(\mathbb{Z}_\ell)$, we may form an associated L-function via an Euler product where the local factors at the unramified primes p are

$$1 - \mathrm{tr}(\rho(\mathrm{Frob}_p))p^{-s} + p^{1-2s},$$

where $\mathrm{Frob}_p \subset G_\infty$ denotes the conjugacy class of Frobenius at p.

This prompts a search for conjugacy-invariants one can attach to Frob_p in the arboreal case.

For $f(x) \in \mathbb{Z}[x]$, $b = 0$, it is a classical fact that for all but finitely many p, the cycle structure of the image of Frob_p in G_n is given by the degrees of the irreducible factors of $f^n(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$.

Call $h \in \mathbb{Z}/p\mathbb{Z}[x]$ *f-stable* if $h \circ f^m$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ for all $m \geq 0$. Weight the irreducible factors of $f^n \in \mathbb{Z}/p\mathbb{Z}[x]$ by degree. If the proportion of the factorization occupied by f-stable factors goes to 1 as $n \to \infty$, call f *settled*.

To each settled element one can associate a partition of unity according to the weight occupied by each stable factor.
Example: $f(x) = (x+3)^2 - 3$, $p = 13$. $f(x) = (x+3)(x+4)$, and one can show both $(x+3)$ and $(x+4)$ are f-stable. The associated partition is thus $1/2 + 1/2$.

Conjecture

Let $f \in \mathbb{Z}/p\mathbb{Z}[x]$ be separable and quadratic. Then f is settled.