Critical Orbits in Dynamics

Rafe Jones

College of the Holy Cross

November 1, 2010

Definitions

Let K be a field and $f(x) \in K[x]$. Define f^n to be the nth iterate of f:

$$f^n := \underbrace{f \circ f \circ \cdots \circ f}_{n}.$$

Orbit of $\alpha \in K$ under f:

$$O_f(\alpha) := \{f^n(\alpha) : n = 1, 2, \ldots\}$$

Goal of dynamics: understand the orbits of f.

Complex dynamics

Let $f \in \mathbb{C}[z]$.

Typical goal is to understand topological properties of orbits of f

"The forward orbits of the critical points of a rational map determine the general features of the global dynamics of the map."
– Alan Beardon, *Iteration of Rational Functions*, p. 192.

Definition

We say that f is *chaotic* at $z \in \mathbb{C}$ if it exhibits sensitive dependence on initial conditions near z: there exists $\epsilon > 0$ such that in all neighborhoods U of z there exists $y \in U$ with

$$|f^n(z) - f^n(y)| > \epsilon.$$

for some $n \geq 1$.

The *Julia set* $J(f)$ is the set where f behaves chaotically.

Theorem

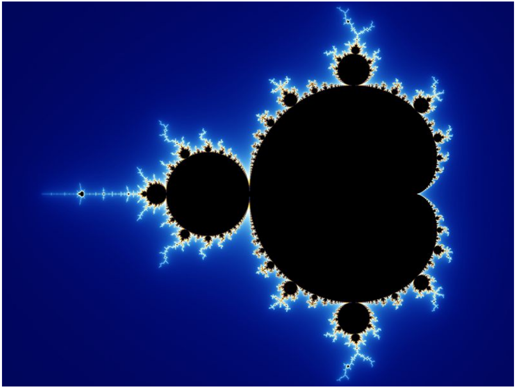
Let $f \in \mathbb{C}[z]$ be quadratic, with critical point γ. Then $J(f)$ is a Cantor set if the critical orbit $O_f(\gamma)$ is unbounded, and $J(f)$ is connected if $O_f(\gamma)$ is bounded.

We say f is conjugate to g if $f = m \circ g \circ m^{-1}$ for some complex Mobius transformation $m = (az + b)/(cz + d), ad - bc \neq 0$.

Conjugate maps have essentially the same dynamics, at least topologically. In particular, $J(f) = mJ(g)$.

Any quadratic $f \in \mathbb{C}[z]$ is conjugate to $f_c = z^2 + c$, and $\{c : O_{f_c} \text{ is bounded}\} \subset \mathbb{C}$ is called the Mandelbrot set.

The Mandelbrot set



Complex dynamics, continued

Conjecture (open): the hyperbolic components make up the full interior of the Mandelbrot set.

Real Dynamics

Any quadratic $f \in \mathbb{R}[x]$ is conjugate (over $\mathbb{R}$) to $f_c := x^2 + c$, $c \in \mathbb{R}$.

If $-2 \le c \le 1/4$ (i.e. if c belongs to the Mandelbrot set), then f_c maps $[-\beta, \beta]$ to itself, where

$$\beta = \frac{-1 - \sqrt{1 - 4c}}{2}.$$

Alternately, each such f_c is conjugate to $\mu x(1 - x)$ for $1 \le \mu \le 4$, and the invariant interval is $[0, 1]$.

Theorem

Suppose that f_c exhibits exponential expansion along the critical orbit: $|(f_c^n)'(f_c(0))|$ grows exponentially with n. Then f_c is chaotic at almost every $x \in [-\beta, \beta]$.

Note: $|(f_c^n)'(f_c(0))| = |\prod_{i=1}^n f_c'(f_c^i(0))|$.

Theorem (Avila-Moreira 2005)

For almost every $c \in [-2, 1/4]$, either the hypotheses of the previous theorem are satisfied or f_c is hyperbolic on $[0, 1]$.

Arithmetic Dynamics

Let $f(x) \in \mathbb{Z}[x]$ be monic and quadratic, with critical point γ.

Question: when is $f^n(x)$ irreducible over $\mathbb{Q}$?

Not always: if $f(x) = x^2 + 10x + 17$, then f is irreducible but f^2 factors as the product of two quadratics. $f^2(-5) = 1$.

If $f(x) = x^2 - x - 1$, then f and f^2 are both irreducible, but f^3 factors as the product of two quartics. $f^3(1/2) = 121/256$.

Theorem

f^n is irreducible if none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots, f^n(\gamma)$ is a square in $\mathbb{Q}$.

Proof: Write $f(x) = (x - \gamma)^2 + \gamma + m$, with $\gamma \in \frac{1}{2}\mathbb{Z}, m \in \frac{1}{4}\mathbb{Z}$.

For $n = 1$, f is irreducible if and only if $-f(\gamma)$ is a square in $\mathbb{Q}$.

Let $n \geq 2$ and suppose that none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots, f^n(\gamma)$ is a square in $\mathbb{Q}$.

By induction, we may assume f^{n-1} is irreducible.

Let β be a root of f^n, and note that $\alpha := f(\beta)$ is a root of f^{n-1}.

Thus $\mathbb{Q}(\beta) \supseteq \mathbb{Q}(\alpha)$.

Now

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^{n-1}[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)],$$

where the last equality follows since f^{n-1} is irreducible.

Thus f^n irreducible iff $[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] = 2$, i.e., if and only if $f(x) - \alpha$ is irreducible over $\mathbb{Q}(\alpha)$.

$f(x) - \alpha$ is irreducible over $\mathbb{Q}(\alpha)$ if and only if $-(\gamma + m - \alpha)$ is a square in $\mathbb{Q}(\alpha)$.

The Galois conjugates of $x \in \mathbb{Q}(\alpha)$ consist of the orbit of x under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

$N_{\mathbb{Q}(\alpha)/\mathbb{Q}} : \mathbb{Q}(\alpha) \to \mathbb{Q}$ is a multiplicative homomorphism mapping each element to the product of its Galois conjugates.

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma(-(\gamma + m - \alpha)) = -(\gamma + m - \sigma(\alpha))$

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(-(\gamma + m - \alpha)) = \prod_{\beta \text{ Gal. conj. of } \alpha} -(\gamma + m - \beta)).$$

$$\begin{aligned}
N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(-(\gamma + m - \alpha)) &= \prod_{f^{n-1}(\alpha)=0} -(\gamma + m - \alpha) \\
&= (-1)^{2^{n-1}} \prod_{f^{n-1}(\alpha)=0} (\gamma + m) - \alpha \\
&= (-1)^{2^{n-1}} f^{n-1}(\gamma + m) \\
&= f^{n-1}(f(\gamma)) \\
&= f^{n}(\gamma)
\end{aligned}$$

But the norm homomorphism maps squares to squares, and $f^n(\gamma)$ is not a square in $\mathbb{Q}$. QED

Remarks:

- Proof can be adapted to hold over any field of characteristic $\neq 2$.
- Hypotheses of theorem are not necessary, e.g. $f(x) = (x-1)^2 + 1$.
- When $\mathbb{Q}$ is replaced by a finite field, the result becomes if and only if.
- Conjugation does not preserve irreducibility, e.g. x^2 and $(x-2)^2 + 2$.

Example: $f_c(x) = x^2 + c, c \in \mathbb{Z}, -c$ not a square.
$f_c^n(0)$ is an increasing sequence of positive integers.

For $y \in \mathbb{Z}$, $y^2 + c$ cannot be a square if $|c| < 2|y| - 1$, i.e. if $|y| > (|c| + 1)/2$.

But $|f_c(0)| = |c| > (|c| + 1)/2$ provided $|c| > 1$.

For $c = 1$ we have $|f_c^2(0)| > (|c| + 1)/2$.

Another arithmetic application of the critical orbit

For $\alpha \in \mathbb{Z}$, let

$$P(O_f(\alpha)) := \{p \text{ prime} : p \mid f^n(\alpha) \text{ for at least one } n \geq 1\}.$$

Example: $f = x^2 + 1$, $\alpha = 3$, $O_f(\alpha)) = \{10, 101, 10202, \ldots\}$.
$\{2, 5, 101, 5101\} \subset P(O_f(\alpha))$.

27 out of the 1229 primes $\leq 10,000$ belong to $P(O_f(\alpha))$.

For S a set of primes, define its natural upper density $D^+(S)$ to be:

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

Theorem (RJ)

Let f have critical point γ, and let v_p be the p-adic valuation. Suppose that f^n is irreducible for all $n \geq 1$. Furthermore suppose that for infinitely many $n \geq 1$ the following holds:

$$\exists p \neq 2 \text{ with } v_p(f^n(\gamma)) \text{ odd and } v_p(f^m((\gamma)) = 0 \text{ for all } m < n.$$

Then $D^+(P(O_f(\alpha))) = 0$ for all $\alpha \in \mathbb{Z}$.

Loosely, this says that elements of orbits of f do not have many small prime factors.

The proof involves counting elements in $\mathrm{Gal}(f^n/\mathbb{Q})$ that fix at least one root of f^n, for $n \to \infty$. Uses probability theory (martingales), and facts about permutation groups.

Example: $f = x^2 + 3$. $\gamma = 0$.

$f(0) = 3$

$f^2(0) = 2^2 \cdot 3$

$f^3(0) = 3 \cdot 7^2$

$f^4(0) = 2^2 \cdot 3 \cdot 1801$

$f^5(0) = 3 \cdot 13 \cdot 3019 \cdot 3967$

$f^6(0) = 2^2 \cdot 3 \cdot 7^2 \cdot 40867 \cdot 9078827347$

$f^7(0) = 3 \cdot 79 \cdot 2008220222666722863337402398168 31$

The family $x^2 + c$, revisited

For $f(x) = x^2 + c$, $c \in \mathbb{Z} \setminus \{0, -1, -2\}$, the critical orbit has a property called *rigid divisibility*:

Let $\beta_n = f^n(0)$. Then for all $m \geq 1$,

1. $\beta_n | \beta_{nm}$ and
2. $v_p(\beta_n) = e > 0 \Rightarrow v_p(\beta_{nm}) = e$.

This property arises because of the lack of a linear term in f.

Example: $f = x^2 + 3$.

$\beta_1 = 3$
$\beta_2 = 2^2 \cdot 3$
$\beta_3 = 3 \cdot 7^2$
$\beta_4 = 2^2 \cdot 3 \cdot 1801$
$\beta_5 = 3 \cdot 13 \cdot 3019 \cdot 3967$
$\beta_6 = 2^2 \cdot 3 \cdot 7^2 \cdot 40867 \cdot 9078827347$
$\beta_7 = 3 \cdot 79 \cdot 2008220222666722863337402398168 31$

Note: when ℓ is prime, β_ℓ is divisible by β_1, and β_ℓ / β_1 is relatively prime to all β_m for $m < \ell$.

Theorem

Let $f = x^2 + c$, where $c \in \mathbb{Z} \setminus \{0, -1, -2\}$ and $-c$ not a square. Then for any $\alpha \in \mathbb{Z}$,

$$D^+(P(O_f(\alpha))) = 0.$$

Remark: The theorem can be extended to cover all $x^2 + c$ except for $c = -1$.

Proof: Since $-c$ is not a square, f^n is irreducible for all n.

By the previous theorem, it thus suffices to show that for infinitely many ℓ, β_ℓ/β_1 is not a square.

If $\beta_\ell/\beta_1 = y_0^2$ for $\ell \geq 3$, the curve

$$C : \beta_1 y^2 = f^3(x)$$

has the integral point $(\beta_{\ell-3}, y_0)$. Since f^3 has degree 8 and no repeated roots, C has genus 3, and thus by Siegel's Theorem only finitely many integral points.

Further Directions

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 $\alpha \in \mathbb{Z}$,

$$D^+(P(O_f(\alpha))) = 0.$$

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

$\beta_1 = 2 \cdot 3 \cdot 157$
$\beta_2 = 3 \cdot 311$
$\beta_3 = 2 \cdot 3 \cdot 7 \cdot 19$
$\beta_4 = 3 \cdot 83^2$
$\beta_5 = 2 \cdot 3 \cdot 103 \cdot 755789$