A Uniform Boundedness Theorem for Polynomials

Michael Zieve

(joint work with Alex Carney and Ruthi Hortsch)

University of Michigan

March 19, 2012

The theorem

Theorem (Carney–Hortsch–Z)

For any $f(X) \in \mathbb{Q}[X]$, the function $\mathbb{Q} \to \mathbb{Q}$ defined by $\alpha \mapsto f(\alpha)$ is at most 6-to-1 outside a finite set.

This result is best possible:

- The "finite set" cannot be avoided: there are polynomials inducing any prescribed function on any finite set (Lagrange).
- The "6" cannot be improved: for $f(X) := (X^3 - X)^2$,

$$f\left(\pm\frac{2t-1}{t^2-t+1}\right) = f\left(\pm\frac{t^2-1}{t^2-t+1}\right) = f\left(\pm\frac{t^2-2t}{t^2-t+1}\right)$$

for each $t \in \mathbb{Q}$.

Maps between elliptic curves

Theorem (Mazur, 1978): *Every elliptic curve over* $\mathbb{Q}$ *has at most* 16 *rational torsion points.*

Reformulation: *If* $f : C \to D$ *is a finite morphism between genus-*1 *curves over* $\mathbb{Q}$*, then the induced map* $C(\mathbb{Q}) \to D(\mathbb{Q})$ *is at most* 16*-to-*1*.*

Our result: *If* $f : \mathbb{A}^1 \to \mathbb{A}^1$ *is a finite morphism defined over* $\mathbb{Q}$*, then the induced map* $\mathbb{A}^1(\mathbb{Q}) \to \mathbb{A}^1(\mathbb{Q})$ *is at most* 6*-to-*1 *outside a finite set.*

Question: For any fixed d, is there a constant N such that any finite morphism $f : V \to W$ between d-dimensional varieties over $\mathbb{Q}$ induces a map $V(\mathbb{Q}) \to W(\mathbb{Q})$ which is at most N-to-1 outside a proper Zariski-closed subset of W?

Graph-theoretic dynamics

Associate to $f \in \mathbb{Q}[X]$ the directed graph $\mathcal{G}$ having vertices $\mathbb{Q}$ and having an edge from α to $f(\alpha)$.

- Our result: all but finitely many vertices of $\mathcal{G}$ have in-degree ≤ 6.
- The Morton–Silverman conjecture bounds the size (and number) of connected components of cycles in terms of $\deg(f)$.

Another theorem: *Suppose f cannot be written as $f = g \circ h \circ \mu$ where $g, h, \mu \in \mathbb{C}[X]$ satisfy $\deg(\mu) = 1 < \deg(h)$ and either $\deg(h) \leq 12$ or $h = X^a(X-1)^b$. Then all but finitely many components of $\mathcal{G}$ are rays, and every infinite component of $\mathcal{G}$ is a ray plus finitely many points.*

Many-to-one polynomials

Theorem: *Let K be a number field, and suppose that $f \in K[X]$ induces a map $f : K \to K$ such that*

$$S := \{\alpha \in K \colon \#f^{-1}(\alpha) \geq r\}$$

is infinite. If $r > 6$, then $f = g \circ h$ for some $g, h \in K[X]$ such that

1. *all but finitely many $\alpha \in S$ satisfy $\#h^{-1}(\alpha) \geq r$; and*
2. *there exist linear $\mu, \nu \in \overline{K}[X]$ such that $\mu \circ h \circ \nu$ is either X^n or $T_n(X)$.*

- Our 6-to-1 result follows from this result plus considerations of roots of unity.
- We have an "if and only if" version of this result, as well as similar (but lengthier) results for any $r > 1$.

Proof strategy

Suppose $f \in \mathbb{Q}[X]$ induces a map $f: \mathbb{Q} \to \mathbb{Q}$ which is (≥ 7)-to-1 over infinitely many points.

Then the scheme $V\colon\ f(X_1) = f(X_2) = \cdots = f(X_7)$ has an irreducible component containing infinitely many rational points that do not lie in any diagonal $X_i = X_j$ $(i \neq j)$.

Hence (Faltings) V has an irreducible component of genus 0 or 1.

Obstacle: it's difficult to use this fact, since we don't know how many components V can have, or any formula for the genus of these components.

We circumvent this issue by first classifying the f's which are (≥ 2)-to-1 infinitely often.

Infinitely non-injective polynomials

Theorem: *For $f(X) \in \mathbb{C}[X] \setminus \mathbb{C}$, if $H(X, Y)$ is an irreducible factor of $f(X) - f(Y)$ such that the curve $H(X, Y) = 0$ has genus ≤ 1, then $f = g \circ h \circ \ell$ for some $g, h, \ell \in \mathbb{C}[X]$ such that ℓ is linear, $H(X, Y) \mid [(h \circ \ell)(X) - (h \circ \ell)(Y)]$, and $h(X)$ is either*

- *a Chebyshev polynomial $T_n(X)$*
- $X^i(X+1)^j$
- $r(X)^n$ *where* $\deg(r) \leq 5$
- *or a polynomial of degree at most* 12.

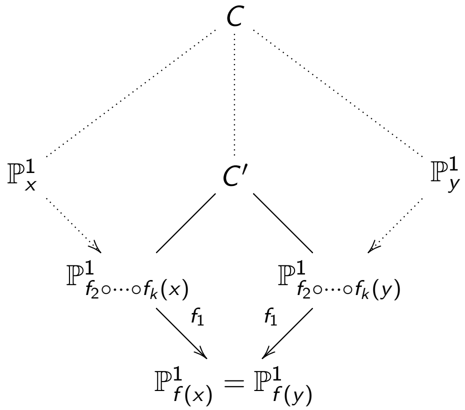
We deduce our (> 6)-to-1 result from this via

- Ritt's theory of functional decomposition of polynomials,
- Computations of Galois groups of $(h \circ \ell)(X) - t$ over $\mathbb{C}(t)$,
- etc.

The decomposable case

$$\text{What if } f = f_1 \circ f_2 \circ \cdots \circ f_k?$$

We get intermediate curves:



- The genus can only stay the same or increase as we progress up through intermediate curves
- Riemann-Hurwitz implies there can be no ramification between genus one curves.
- Ramification at infinity usually forces C to have genus greater than one.

Another tool for the decomposable case

We often used a generalization of the following result:

Theorem

For indecomposable $f, g \in \mathbb{C}[X]$, if $f(X) - g(Y)$ is reducible in $\mathbb{C}[X, Y]$ then f and g have the same critical values: that is,

$$\{f(a)\colon f'(a) = 0\} = \{g(b)\colon g'(b) = 0\}.$$

This result can be generalized to any pair of maps between curves which have the same target curve.