Dynamical methods in Algebra, Geometry and Topology

Scarcity of periodic points for rational functions over a number field (joint work with S. Vishkautsan)

Jung Kyu CANCI

5.07.2018

University of Basel and Lucerne University for Applied Science and Arts

Periodic and Preperiodic Points

We consider an endomorphism $\phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ defined over a field K. We denote by

$$\mathrm{Per}(\phi, K) = \{P \in \mathbb{P}_1(K) \mid \exists n > 0, \phi^n(P) = P\}$$

the set of *periodic points* of ϕ defined over K (ϕ^n denotes the n–th iterate of ϕ).

The minimal n verifying the above equality is called *minimal period* or *periodicity* of P.

We denote by

$$\mathrm{PrePer}(\phi, K) = \{P \in \mathbb{P}_1(K) \mid \exists n > 0, m \geq 0, \phi^{n+m}(P) = \phi^m(P)\}$$

the set of *preperiodic points* of ϕ defined over K ($\phi^0 = \mathrm{id}$).

Periodic and Preperiodic Points

Any endomorphism of $\mathbb{P}_1$ has an affine model given by a rational function of the form $\phi(z) = f(z)/g(z)$ where $f, g \in K[z]$. The degree of such a ϕ is given by $\deg \phi = \max\{\deg f, \deg g\}$, if f and g have no common (irreducible) factors.

- If K is an algebraic closed field and $\deg \phi > 1$, then the set $\mathrm{Per}(\phi, K)$ is infinite.
- But if K is a number field, and $\deg \phi > 1$, then the whole set $\mathrm{PrePer}(\phi, K)$ is finite.

Periodic and Preperiodic Points

Unif. Bound. Conj. (Morton and Silverman–1994)

Let $d \geq 2$ and $D \geq 1$ be given integers. There exists a number $B(d, D)$ such that for all morphism $\phi : \mathbb{P}_1 \to \mathbb{P}_1$ of degree d, defined over a number field K with $[K : \mathbb{Q}]$ at most D we have

$$\#\mathrm{PrePer}(\phi, K) \leq B(d, D).$$

Being a preperiodic point is an algebraic condition, so the above bound should depend on D. Also the dependence on the degree d is clear, e.g. consider

$$\phi(z) = \prod_{i=1}^{d}(z - i) + z.$$

We are far to know if the U.B.C. is true.

Preperiodic Points and Torsion Points

Let E be an elliptic curve (for example defined over $\mathbb{C}$). We consider the multiplication by 2-map $[2] : E \to E$. Assume that E is given by a planar model in a (x, y)–plane by an equation $y^2 = p(x)$. There exists an endomorphism ϕ of degree 4 that makes the following diagram commutative

$$\begin{array}{ccc} E & \xrightarrow{[2]} & E \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}_1 & \xrightarrow{\phi} & \mathbb{P}_1 \end{array}$$

The map π is the projection $\pi(x, y) = [x : 1], \pi(\mathcal{O}) = [1 : 0]$. The morphism ϕ is an example of Lattès map.

We have

$$\mathrm{PrePer}(\phi, \mathbb{C}) = \pi(E(\mathbb{C})_{\mathsf{Tors}}).$$

Preperiodic Points and Torsion Points

In general, by considering K-rational points with K number field, we have

$$\pi(E(K)_{\mathsf{Tors}}) \subset \mathrm{PrePer}(\phi, K).$$

Theorem (Mazur-Kamienny-Merel)

For all integers $D > 1$ there is a number $B(D)$ such that for all number field $K/\mathbb{Q}$ of degree at most D and all elliptic curve E/K we have

$$\#E(K)_{Tors} \leq B(D).$$

By using some elementary (but non-completely trivial) arguments one shows that the above theorem implies the Uniform Boundedness Conjecture for Lattès Maps.

Preperiodic Points for certain Polynomials

Let $\phi \in \mathbb{Z}[z]$ be monic of degree $d \geq 2$. Then

- If $P \in \mathbb{Q}$ is a periodic point of ϕ, then its periodicity is ≤ 2.
- Proposition due to Gerd Baron 80's

$$\#\mathrm{Per}(\phi, \mathbb{Q}) \leq d + 1$$

E.g. consider $\phi(z) = \prod_{i=1}^{d}(z - i) + z$. The unique zeros of the polynomial equation

$$\phi^n(z) - z = 0$$

are $1, \ldots, d$ for all $n \geq 1$.

-

$$\#\mathrm{PrePer}(\phi, \mathbb{Q}) \leq 3(d^4 - 1)$$

Bounds in terms of good reduction

Let $\mathfrak{p}$ be a nonzero prime of the algebraic integer R of a number field K. Let $R_\mathfrak{p}$ be the local ring of K at $\mathfrak{p}$. A rational map $\phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ defined over K is said to have *good reduction* at $\mathfrak{p}$ if ϕ can be written as $\phi = [F(X,Y) : G(X,Y)]$ where $F, G \in R_\mathfrak{p}[X,Y]$ are homogeneous polynomials, such that the resultant of F and G is a $\mathfrak{p}$-unit. For a given finite set S of primes of K, we say that ϕ has good reduction outside S if it has good reduction at each prime $\mathfrak{p} \notin S$.

Bounds in terms of good reduction

Equivalently, let $\phi = [F(X,Y) : G(X,Y)]$ be written in $\mathfrak{p}$–reduced form, that is $F, G \in R_\mathfrak{p}[X,Y]$ do not have irreducible common factors in $R_\mathfrak{p}(X,Y)$. We say that ϕ has good reduction at $\mathfrak{p}$, if the reduced map $\phi_\mathfrak{p} = [F_\mathfrak{p}(X,Y) : G_\mathfrak{p}(X,Y)]$ obtained by reducing the coefficients of F and G modulo $\mathfrak{p}$ is such that

$$\deg \phi = \deg \phi_\mathfrak{p}.$$

Bounds in terms of good reduction

Example. A polynomial $\phi \in \mathbb{Q}[z]$ (endomorphism of $\mathbb{P}_1$ with a totally ramified fixed point) has good reduction at any place iff it is monic with integer coefficients.

Let $n \geq 1$ and

$$\phi(z) = \frac{a_n z^n + \ldots + a_1 z + a_0}{b}$$

with $a_n, \ldots, a_1, a_0, b \in \mathbb{Z}$ coprime. Projective model for $\phi(z)$:

$$\phi([X : Y]) = [a_n X^n + \ldots + a_1 X Y^{n-1} + a_0 Y^n : b Y^n]$$

The map ϕ has good reduction at any prime $\mathfrak{p}$ that does not divide $a_n \cdot b$.

Theorem (C., S. Vishkautsan – On Transaction of AMS ≥2018)

Let K be a number field and S be a finite set of primes of K. Let $\phi, \psi \colon \mathbb{P}_1 \to \mathbb{P}_1$ be rational maps defined over K, where the degree d_ϕ of ϕ is ≥ 2. Assume that both maps have good reduction outside S. Then

$$|Per(\psi \circ \phi, K)| \leq \kappa d_\phi + \lambda$$

for some positive integers κ and λ depending only on the cardinality of S and $[K : \mathbb{Q}]$, that can be effectively computed.

κ and λ are exponential in $|S|$ and $[K : \mathbb{Q}]$.

S–unit equation theorem

Theorem (Evertse, Schlickewei, Schmidt 2002)

Let $n \geq 2$, $a_1, \ldots, a_n \in \mathbb{C}^*$ and Γ be a finitely generated subgroup of $\mathbb{C}^*$ of rank r. Then the equation

$$a_1 x_1 + \ldots + a_n x_n = 1$$

admits at most $e^{(6n)^{3n}(nr+1)}$ non-degenerate solutions $(x_1, \ldots, x_n) \in \Gamma^n$.

Non–degenerate solution means $\sum_{i \in A} a_i x_i \neq 0$ for each A nonempty subset of $\{1, \ldots, n\}$. (To avoid $u + (-u) + 1 = 1$ with $u \in \Gamma$)

E.g. (with $S = \{2, 3, 5\}$) the equation $2^a + 3^b = 5^c$ has only finitley many solutions in $a, b, c \in \mathbb{Z}$.

Some corollaries of our Theorem

Corollary

Let K be a number field and let $I = \langle f_1, \ldots, f_n \rangle$ be a finitely generated semigroup, with respect to composition, of rational maps $f_i \colon \mathbb{P}_1 \to \mathbb{P}_1$ of degree ≥ 2 defined over K. Then there exists a uniform bound B, depending on I, such that any $\phi \in I$ has at most B periodic points in $\mathbb{P}_1(K)$.

Example

Consider

$$I = \left\langle x^2 + 4, \frac{(x+1)^2}{x^2}, \frac{x^2 + x + 1}{x + 1}, x^2 + 3x + 1 \right\rangle$$

Then $\#\mathrm{Per}(\phi, \mathbb{Q}) \leq 7$ for all $\phi \in I$.

Some corollaries of our Theorem

WHLOG (With Huge Loss of Generality) we are able to prove the following:

Corollary

Let $n > 1$. The following polynomial equation

$$x^{2n} + a_{n-1}x^{2n-2} + a_{n-2}x^{2n-4} + \ldots + a_1 x^2 - x = a_0$$

admits at most 6 roots in $\mathbb{Q}$, for any choice of $a_{n-1}, a_{n-2}, \ldots, a_1, a_0 \in \mathbb{Z}$

Consider $\phi(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z - a_0$. The above zeros are fixed points of the map $\phi(x^2)$.

Thank you for your attention