Monodromy Groups of Indecomposable Rational Functions

Franklyn H. Wang

Thomas Jefferson High School of Science and Technology

PRIMES conference, May 20th, 2017

Mentor: Michael E. Zieve, University of Michigan

A Motivating Theorem

- Let $\mathbb{Q}[X]$ be the set of polynomials with rational coefficients.

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Restate: $f : \mathbb{Q} \to \mathbb{Q}$ is (≤ 6)-to-1 over all but finitely many values.
- **Example:** $f(X) = X^2$. The only preimages of 4 are 2 and -2.
- **Surprise!** Six does not depend on the degree of the polynomial.

A Motivating Theorem

- Let $\mathbb{Q}[X]$ be the set of polynomials with rational coefficients.

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Restate: $f : \mathbb{Q} \to \mathbb{Q}$ is (≤ 6)-to-1 over all but finitely many values.

- **Example:** $f(X) = X^2$. The only preimages of 4 are 2 and -2.

- **Surprise!** Six does not depend on the degree of the polynomial.

A Motivating Theorem

- Let $\mathbb{Q}[X]$ be the set of polynomials with rational coefficients.

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Restate: $f : \mathbb{Q} \to \mathbb{Q}$ is (≤ 6)-to-1 over all but finitely many values.

- **Example:** $f(X) = X^2$. The only preimages of 4 are 2 and -2.

- **Surprise!** Six does not depend on the degree of the polynomial.

A Motivating Theorem

- Let $\mathbb{Q}[X]$ be the set of polynomials with rational coefficients.

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Restate: $f : \mathbb{Q} \to \mathbb{Q}$ is (≤ 6)-to-1 over all but finitely many values.
- **Example:** $f(X) = X^2$. The only preimages of 4 are 2 and -2.
- **Surprise!** Six does not depend on the degree of the polynomial.

A Motivating Theorem

- Let $\mathbb{Q}[X]$ be the set of polynomials with rational coefficients.

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Restate: $f : \mathbb{Q} \to \mathbb{Q}$ is (≤ 6)-to-1 over all but finitely many values.
- **Example:** $f(X) = X^2$. The only preimages of 4 are 2 and -2.
- **Surprise!** Six does not depend on the degree of the polynomial.

Generalization to rational functions

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Want analogue when $f(X)$ is a *rational function*.
- Polynomials are a special class of rational functions.
- A rational function version of this theorem would generalize Mazur's theorem on uniform boundedness of rational torsion on elliptic curves.

Generalization to rational functions

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Want analogue when $f(X)$ is a *rational function*.
- Polynomials are a special class of rational functions.
- A rational function version of this theorem would generalize Mazur's theorem on uniform boundedness of rational torsion on elliptic curves.

Generalization to rational functions

Theorem (Carney, Hortsch, Zieve)

For any $f(X) \in \mathbb{Q}[X]$, all but finitely many rational numbers have at most six rational preimages under f.

- Want analogue when $f(X)$ is a *rational function*.
- Polynomials are a special class of rational functions.
- A rational function version of this theorem would generalize Mazur's theorem on uniform boundedness of rational torsion on elliptic curves.

Indecomposable rational functions

Write $f = f_1(f_2(\ldots(f_k(X)))$ where each f_i is an *indecomposable* rational function (i.e., it is not the composition of lower-degree rational functions).

Example: X^5 is indecomposable, but X^6 is not.

Theorem (Neftin, Zieve)

If n is a sufficiently large integer which is not prime, square, or triangular, then every indecomposable $f(X) \in \mathbb{C}(X)$ of degree n behaves like a random degree-n rational function.

Indecomposable rational functions

Write $f = f_1(f_2(\ldots(f_k(X)))$ where each f_i is an *indecomposable* rational function (i.e., it is not the composition of lower-degree rational functions).

Example: X^5 is indecomposable, but X^6 is not.

Theorem (Neftin, Zieve)

If n is a sufficiently large integer which is not prime, square, or triangular, then every indecomposable $f(X) \in \mathbb{C}(X)$ of degree n behaves like a random degree-n rational function.

Indecomposable rational functions

Write $f = f_1(f_2(\ldots(f_k(X)))$ where each f_i is an *indecomposable* rational function (i.e., it is not the composition of lower-degree rational functions).

Example: X^5 is indecomposable, but X^6 is not.

Theorem (Neftin, Zieve)

If n is a sufficiently large integer which is not prime, square, or triangular, then every indecomposable $f(X) \in \mathbb{C}(X)$ of degree n behaves like a random degree-n rational function.

Monodromy groups

For $f(X) \in \mathbb{C}(X)$ of degree n, every point which is not a critical value will have n distinct preimages. Pick one such point p, and write $f^{-1}(p) = \{z_1, z_2, \ldots, z_n\}$.

Definition of a monodromy group

Consider a loop τ in $\mathbb{C}$ which starts and ends at p, and doesn't go through any critical values of $f(X)$. For each z_i, there is a unique path σ_i starting at z_i which maps to τ under f. Since τ starts and ends at p, the ending point of σ_i is some $z_j = z_{\pi(i)}$, where π is a permutation of $\{1, 2, \ldots, n\}$. The set of π's produced from all such loops τ forms a group of permutations of $\{1, 2, \ldots, n\}$, called the *monodromy group* of $f(X)$.

Monodromy groups of indecomposable rational functions

- "Random" degree-n rational function should have monodromy group A_n or S_n. We want to find all exceptions.
- Work of many mathematicians (Ritt, Zariski, Guralnick, Thompson, Aschbacher, ...)
- One of the hardest cases is when the monodromy group is A_d or S_d for some $d \neq \deg(f)$.
- Others have made progress, but we have resolved it completely.

Monodromy groups of indecomposable rational functions

- "Random" degree-n rational function should have monodromy group A_n or S_n. We want to find all exceptions.
- Work of many mathematicians (Ritt, Zariski, Guralnick, Thompson, Aschbacher, ...)
- One of the hardest cases is when the monodromy group is A_d or S_d for some $d \neq \deg(f)$.
- Others have made progress, but we have resolved it completely.

Monodromy groups of indecomposable rational functions

- "Random" degree-n rational function should have monodromy group A_n or S_n. We want to find all exceptions.
- Work of many mathematicians (Ritt, Zariski, Guralnick, Thompson, Aschbacher, ...)
- One of the hardest cases is when the monodromy group is A_d or S_d for some $d \neq \deg(f)$.
- Others have made progress, but we have resolved it completely.

Monodromy groups of indecomposable rational functions

- "Random" degree-n rational function should have monodromy group A_n or S_n. We want to find all exceptions.
- Work of many mathematicians (Ritt, Zariski, Guralnick, Thompson, Aschbacher, ...)
- One of the hardest cases is when the monodromy group is A_d or S_d for some $d \neq \deg(f)$.
- Others have made progress, but we have resolved it completely.

Tools

- Aschbacher–Scott classification of primitive permutation groups
- Classification of triply transitive permutation groups
- Representation theory of symmetric groups and wreath products
- Riemann–Hurwitz genus formula
- Riemann's existence theorem and facts about fundamental groups
- Various computer programs and other arguments involving combinatorics and Galois theory

Status of Project

Main Result

If $f(X) \in \mathbb{C}(X)$ is indecomposable of degree n, and the monodromy group G of $f(X)$ is A_d or S_d for some $d \neq n$, then either $n = d(d-1)/2$ or $d \leq 28$, where in either case we know all possibilities for the permutation action of G and for the ramification of $f(X)$.

- We are now working towards a similar result when $L^k \leq G \leq \mathrm{Aut}(L^k)$ for some nonabelian simple group L and some $k > 1$ (currently done when $k = 2$ or $k > 8$). A team of group theorists is doing the same when $k = 1$ and L is not alternating.
- Once these two projects are finished, we will know all indecomposable degree-n $f(X) \in \mathbb{C}(X)$ whose monodromy group is not A_n or S_n.

Status of Project

Main Result

If $f(X) \in \mathbb{C}(X)$ is indecomposable of degree n, and the monodromy group G of $f(X)$ is A_d or S_d for some $d \neq n$, then either $n = d(d-1)/2$ or $d \leq 28$, where in either case we know all possibilities for the permutation action of G and for the ramification of $f(X)$.

- We are now working towards a similar result when $L^k \leq G \leq \mathrm{Aut}(L^k)$ for some nonabelian simple group L and some $k > 1$ (currently done when $k = 2$ or $k > 8$). A team of group theorists is doing the same when $k = 1$ and L is not alternating.
- Once these two projects are finished, we will know all indecomposable degree-n $f(X) \in \mathbb{C}(X)$ whose monodromy group is not A_n or S_n.

Status of Project

Main Result

If $f(X) \in \mathbb{C}(X)$ is indecomposable of degree n, and the monodromy group G of $f(X)$ is A_d or S_d for some $d \neq n$, then either $n = d(d-1)/2$ or $d \leq 28$, where in either case we know all possibilities for the permutation action of G and for the ramification of $f(X)$.

- We are now working towards a similar result when $L^k \leq G \leq \mathrm{Aut}(L^k)$ for some nonabelian simple group L and some $k > 1$ (currently done when $k = 2$ or $k > 8$). A team of group theorists is doing the same when $k = 1$ and L is not alternating.
- Once these two projects are finished, we will know all indecomposable degree-n $f(X) \in \mathbb{C}(X)$ whose monodromy group is not A_n or S_n.

Acknowledgements

I would like to thank the following individuals, for without any of them none of this would have been possible.

- Dr. Michael Zieve, for suggesting this project and being my PRIMES mentor
- Dr. Danny Neftin, for checking some of the proofs in this paper, and for resolving the problem for sufficiently large n with Dr. Zieve
- the MIT Math Department
- the MIT-PRIMES program

Acknowledgements

I would like to thank the following individuals, for without any of them none of this would have been possible.

- Dr. Michael Zieve, for suggesting this project and being my PRIMES mentor
- Dr. Danny Neftin, for checking some of the proofs in this paper, and for resolving the problem for sufficiently large n with Dr. Zieve
- the MIT Math Department
- the MIT-PRIMES program

Acknowledgements

I would like to thank the following individuals, for without any of them none of this would have been possible.

- Dr. Michael Zieve, for suggesting this project and being my PRIMES mentor
- Dr. Danny Neftin, for checking some of the proofs in this paper, and for resolving the problem for sufficiently large n with Dr. Zieve
- the MIT Math Department
- the MIT-PRIMES program

Acknowledgements

I would like to thank the following individuals, for without any of them none of this would have been possible.

- Dr. Michael Zieve, for suggesting this project and being my PRIMES mentor
- Dr. Danny Neftin, for checking some of the proofs in this paper, and for resolving the problem for sufficiently large *n* with Dr. Zieve
- the MIT Math Department
- the MIT-PRIMES program

Acknowledgements

I would like to thank the following individuals, for without any of them none of this would have been possible.

- Dr. Michael Zieve, for suggesting this project and being my PRIMES mentor
- Dr. Danny Neftin, for checking some of the proofs in this paper, and for resolving the problem for sufficiently large n with Dr. Zieve
- the MIT Math Department
- the MIT-PRIMES program