Ramification of Solutions of Functional Equations

Felix Wang
Mentor: Michael E. Zieve, University of Michigan

MIT-PRIMES

May 21, 2016

Historical Background

Ritt's Functional Equation

Which polynomials $f, \hat{f}, g, \hat{g} \in \mathbb{C}[X]$ satisfy $f \circ \hat{f} = g \circ \hat{g}$?

Note: $f(X) \circ \hat{f}(X) := f(\hat{f}(X))$

Historical Background

Ritt's Functional Equation

Which polynomials $f, \hat{f}, g, \hat{g} \in \mathbb{C}[X]$ satisfy $f \circ \hat{f} = g \circ \hat{g}$?

Note: $f(X) \circ \hat{f}(X) := f(\hat{f}(X))$

Example Solution: $X^3 \circ X^4 = X^{12} = X^6 \circ X^2$.

J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.

Ritt's Theorem

Theorem (Ritt's Theorem)

There are exactly two sources of solutions (up to simple methods for modifying solutions) for the functional equation $f \circ \hat{f} = g \circ \hat{g}$*, where* $f, \hat{f}, g, \hat{g} \in \mathbb{C}[X]$ *and have degree at least 2:*

1. $X^a \circ X^b h(X^a) = X^b h(X)^a \circ X^a$*, where* h *can be any function*
2. $T_a \circ T_b = T_b \circ T_a$

Note: T_a denotes the ath Chebyshev polynomial: the unique polynomial that satisfies $T_a(\cos(\theta)) = \cos(a\theta)$.

Applications of Ritt's Result

- D. Ghioca, T. J. Tucker and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell–Lang conjecture*, Invent. Math. **171** (2008), 463–483.
- F. Pakovich, *On polynomials sharing preimages of compact sets, and related questions*, Geom. Funct. Anal. **18** (2008), 163–183.
- M. Briskin, N. Roytvarf and Y. Yomdin, *Center conditions at infinity for Abel differential equations*, Annals of Math. (2) **172** (2010), 437–483.
- A. Medvedev and T. Scanlon, *Invariant varieties for polynomial dynamical systems*, Annals of Math. **179** (2014), 81–177.

Ritt's Strategy

Ritt first solved $f \circ \hat{f} = g \circ \hat{g}$ under the hypothesis that $f(X) - g(Y)$ was irreducible, and then deduced the case where $f(X) - g(Y)$ was reducible from the irreducible case.

Ritt's Strategy

Ritt first solved $f \circ \hat{f} = g \circ \hat{g}$ under the hypothesis that $f(X) - g(Y)$ was irreducible, and then deduced the case where $f(X) - g(Y)$ was reducible from the irreducible case.

Ritt wrote that "the analogous problem for fractional rational functions is much more difficult."

Ritt's Strategy

Ritt first solved $f \circ \hat{f} = g \circ \hat{g}$ under the hypothesis that $f(X) - g(Y)$ was irreducible, and then deduced the case where $f(X) - g(Y)$ was reducible from the irreducible case.

Ritt wrote that "the analogous problem for fractional rational functions is much more difficult."

Special cases of this "analogous problem" been studied extensively by Ritt 1923, Fried 1973, Bilu–Tichy 2000, Avanzi–Zannier 2001, and Pakovich 2010.

Fried's Question

Fried's Question

Which $f, \hat{f}, g, \hat{g} \in \mathbb{C}(X)$, where the numerator of $f(X) - g(Y)$ is irreducible, satisfy $f \circ \hat{f} = g \circ \hat{g}$?

Fried's Question

Fried's Question

Which $f, \hat{f}, g, \hat{g} \in \mathbb{C}(X)$, where the numerator of $f(X) - g(Y)$ is irreducible, satisfy $f \circ \hat{f} = g \circ \hat{g}$?

Theorem (Simplified Version)

If $f, \hat{f}, g, \hat{g} \in \mathbb{C}(X)$ satisfy $f \circ \hat{f} = g \circ \hat{g}$ and $f(X) - g(Y)$ has irreducible numerator, then one of the following holds:

1. *If $f(X) - g(Y)$ has sufficiently large degree, then we can explicitly write out the possibilities for either $f(X)$ or $g(X)$, and we can almost do the same for the other function.*
2. *If $f(X) - g(Y)$ does not have sufficiently large degree, then f and g both belong to a finite list of possible functions.*

AN INTERESTING CONSEQUENCE

Cahn, Jones, and Spear conjectured that for $f, g \in \mathbb{Q}(X)$ with degree at least 2 and $c \in \mathbb{Q}$, the set $\{n \in \mathbb{N} : g^n(c) \in f(\mathbb{Q})\}$ must be the union of finitely many numbers and finitely many infinite arithmetic sequences.

Note: $g^n(c)$ denotes the nth iterate of g evaluated at c. For example, $g^2(c) = g(g(c))$.

J. Cahn, R. Jones and J. Spear, *Powers in orbits of rational functions: cases of an arithmetic dynamical Mordell-Lang conjecture*, 2015, arXiv:1512.03085.

An Interesting Consequence

Cahn, Jones, and Spear conjectured that for $f, g \in \mathbb{Q}(X)$ with degree at least 2 and $c \in \mathbb{Q}$, the set $\{n \in \mathbb{N} : g^n(c) \in f(\mathbb{Q})\}$ must be the union of finitely many numbers and finitely many infinite arithmetic sequences.

Note: $g^n(c)$ denotes the nth iterate of g evaluated at c. For example, $g^2(c) = g(g(c))$.

J. Cahn, R. Jones and J. Spear, *Powers in orbits of rational functions: cases of an arithmetic dynamical Mordell-Lang conjecture*, 2015, arXiv:1512.03085.

This conjecture was recently proven by Hyde and Zieve.

An Interesting Consequence, Cont'd

Hyde and Zieve proved that for $f, g \in \mathbb{Q}(X)$ with degree at least 2 and $c \in \mathbb{Q}$, the set $\{n \in \mathbb{N} : g^n(c) \in f(\mathbb{Q})\}$ must be the union of finitely many numbers and finitely many infinite arithmetic sequences.

Using our results, we can say that each infinite arithmetic sequence must start with a number which is at most $4 + (\deg f)^2$. Hence if f is a degree-3 function, then each arithmetic sequence must start with a number no larger than 13.

An Interesting Consequence, Cont'd

Hyde and Zieve proved that for $f, g \in \mathbb{Q}(X)$ with degree at least 2 and $c \in \mathbb{Q}$, the set $\{n \in \mathbb{N} : g^n(c) \in f(\mathbb{Q})\}$ must be the union of finitely many numbers and finitely many infinite arithmetic sequences.

Using our results, we can say that each infinite arithmetic sequence must start with a number which is at most $4 + (\deg f)^2$. Hence if f is a degree-3 function, then each arithmetic sequence must start with a number no larger than 13.

Outline of Proof: For each fixed n, the equation $f(X) = g^n(Y)$ must have infinitely many rational solutions. By Faltings' Theorem, the curve of $f(X) - g^n(Y)$ must have a genus of 0 or 1. If the curve has genus 0, then there must exist nonconstant rational functions $\hat{f}$ and $\hat{g}$ for which $f \circ \hat{f} = g^n \circ \hat{g}$. We can then proceed inductively (downwards) on n.

Key Tool

Definition (Ramification)

The *ramification index* of a rational function $f(X)$ at a point $P \in \mathbb{C} \cup \{\infty\}$, denoted $e_f(P)$, is the multiplicity of P as a root of $f(X) - f(P)$. The *ramification multiset* of $f(X)$ over a point $Q \in \mathbb{C} \cup \{\infty\}$ is

$$E_f(Q) := \{e_f(P) : P \in \mathbb{C} \cup \{\infty\},\ f(P) = Q\}.$$

Key Tool

Definition (Ramification)

The *ramification index* of a rational function $f(X)$ at a point $P \in \mathbb{C} \cup \{\infty\}$, denoted $e_f(P)$, is the multiplicity of P as a root of $f(X) - f(P)$. The *ramification multiset* of $f(X)$ over a point $Q \in \mathbb{C} \cup \{\infty\}$ is

$$E_f(Q) := \{e_f(P) : P \in \mathbb{C} \cup \{\infty\},\ f(P) = Q\}.$$

Example: For $f(X) = X^3 + X^4 = X^3(X+1)$ we have $e_f(0) = 3$ and $e_f(-1) = 1$, and thus $E_f(0) = [1, 3]$.

Key Tool

Definition (Ramification)

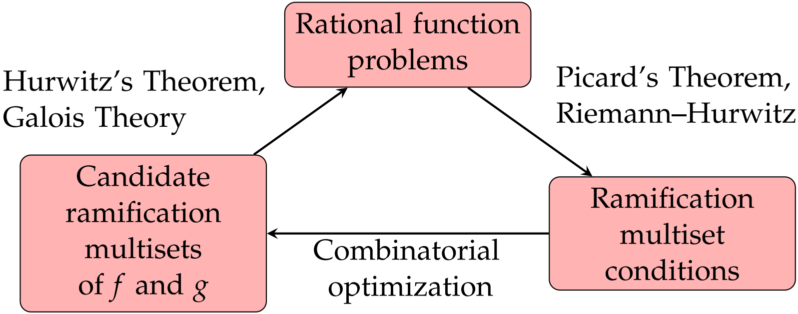
The *ramification index* of a rational function $f(X)$ at a point $P \in \mathbb{C} \cup \{\infty\}$, denoted $e_f(P)$, is the multiplicity of P as a root of $f(X) - f(P)$. The *ramification multiset* of $f(X)$ over a point $Q \in \mathbb{C} \cup \{\infty\}$ is

$$E_f(Q) := \{e_f(P) : P \in \mathbb{C} \cup \{\infty\}, \ f(P) = Q\}.$$

Example: For $f(X) = X^3 + X^4 = X^3(X+1)$ we have $e_f(0) = 3$ and $e_f(-1) = 1$, and thus $E_f(0) = [1,3]$.

Example: For $f(x) = (X+1)(X+2)^3(X-3)^5$ we have $e_f(-1) = 1$ and $e_f(-2) = 3$ and $e_f(3) = 5$, and thus $E_f(0) = [1,3,5]$.

Outline of our strategy



Combinatorial Optimization

Our key innovation is to study the multisets over a single point, and show that they must have a very special property, namely that almost all ramification indices equal one another.

Combinatorial Optimization

Our key innovation is to study the multisets over a single point, and show that they must have a very special property, namely that almost all ramification indices equal one another.

Acceptable Ramification Multiset: $E_f(0) = [4, 4, 4, 4, 4, 4, 4, 4, 7]$

Combinatorial Optimization

Our key innovation is to study the multisets over a single point, and show that they must have a very special property, namely that almost all ramification indices equal one another.

Acceptable Ramification Multiset: $E_f(0) = [4, 4, 4, 4, 4, 4, 4, 4, 7]$

Unacceptable Ramification Multiset: $E_f(0) = [1, 3, 6, 7, 8, 9]$

Our Result

Theorem

For any $f, g \in \mathbb{C}(X)$ such that the numerator of $f(X) - g(Y)$ is an irreducible polynomial in $\mathbb{C}[X, Y]$, if there are nonconstant rational functions $\hat{f}, \hat{g}$ on the complex plane such that $f \circ \hat{f} = g \circ \hat{g}$ then:

1. *If $f(X) - g(Y)$ has degree greater than 150, then either f or g belongs to an explicit list of nice functions (for instance, $f(X)$ could be X^m or $X^m + X^{-m}$). More rigorously, at least one of the extensions $\mathbb{C}(X)/\mathbb{C}(f(X))$ or $\mathbb{C}(X)/\mathbb{C}(g(X))$ has Galois closure of genus 0 or 1. We can also control the ramification of the other function.*

2. *If $f(X) - g(Y)$ has degree less than or equal to 150, then there are a finite number of possibilities for the ramification of f and g. We can therefore implement an exhaustive search by computer to find all possibilities for f and g.*

Conclusions

- If nonconstant $f, g, \hat{f}, \hat{g} \in \mathbb{C}(X)$ satisfy $f \circ \hat{f} = g \circ \hat{g}$, where the numerator of $f(X) - g(Y)$ is irreducible and has degree greater than 150, then we describe the ramification of f and g, and explicitly determine at least one of these functions.
- If $f(X) - g(Y)$ has degree at most 150, then there is a finite list of possible ramification for f and g.
- In the future, we will use the case where $f(X) - g(Y)$ has irreducible numerator to resolve the case where $f(X) - g(Y)$ can have reducible numerator, much like Ritt did with the original functional equation.

Acknowledgements

- Professor Michael Zieve of the University of Michigan
- Thao Do of MIT
- Tanya Khovanova of MIT
- The MIT-PRIMES program
- My parents