Research statement

Sijun Liu

I am working on several topics in number theory, arithmetic geometry and arithmetic dynamics. One topic is the following conjecture

Conjecture 1 (Zieve)**.** *A morphism $V \to W$ between n-dimensional varieties over $\mathbb{Q}$ induces a map $V(\mathbb{Q}) \to W(\mathbb{Q})$ which is at most $c(n)$-to-1 outside a proper Zariski-closed subset of W, where $c(n)$ depends only on n.*

The conjecture has an analogue over an arbitrary degree-d number field K, where $c(n)$ is replaced by a constant depending only on n and d. I am working on the conjecture and its analogue when $n = 1$; this case generalizes Mazur and Merel's results on the uniform boundedness of rational torsion points on elliptic curves.

Another topic is, when does $f(x) = g(y)$ have infinitely many rational or integer solutions, where f, g are polynomials of certain forms. When f, g are both binomials, my paper [9] classified when $f(x) = g(y)$ has infinitely many solutions in a number field. As a consequence I obtain refinements and generalizations of the results of Schinzel et al. [13].

Another topic is the complex-analytic version: solve $f \circ u = g \circ v$ in functions u, v that are meromorphic on the complex plane and complex rational functions f, g that come from certain families. Specifically we've done this completely when f, g are binomials in [9].

Regarding dynamics, I am interested in the dynamics of rational functions over various fields, and dynamics on algebraic varieties. One project I did is on the dynamics of Lattès maps over finite fields. My paper [8] described the dynamics of all degree-2 Lattès maps over any finite fields. My theory covered all known examples [6, 16, 15] and provided many new types of examples. For instance, Lattès maps in new situations (e.g. maps from supersingular curves, map and curve have different field of definition, etc) are for first time studied, which are substantially harder and require many new techniques.

Below is a detailed description of my results.

1 Uniform boundedness conjecture (thesis topic)

My thesis is on Conjecture 1 when $n = 1$. Special cases are known to be true: maps between elliptic curves (reformulation of Mazur's result for $\mathbb{Q}$ [10, 11], where the bound is 16, and Merel's result [12] for the analogue), maps between genus 0 curves with a totally ramified rational point (Carney–Hortsch–Zieve [5], whose bound is 6). In my thesis I prove the conjecture for maps between genus 0 curves, in which some rational point has two rational preimages, and my future work will try to use this to prove the conjecture for $n = 1$.

Studying morphisms between genus 0 curves is the same as studying rational maps $f : \mathbb{P}^1 \to \mathbb{P}^1$, and the condition that some rational point has two rational preimages means f is a Laurent polynomial up to conjugation by linears (A Laurent polynomial is an element in $K[x, \frac{1}{x}]$). A uniform bound for rational maps would imply Mazur's result and Merel's result, through an analysis of the map on x coordinates induced by multiplication by n on an elliptic curve. My thesis deals with the Laurent polynomial case, and in the future I hope to generalize it to arbitrary rational functions. The idea of finding a uniform bound is as follows:

(1) Suppose $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ is at most N-to-1 over all but finitely many points, then the variety $f(x_1) = f(x_2) = \ldots = f(x_{N+1})$ has only finitely many rational points off all the diagonals $x_i = x_j$. This suggests we can firstly find all f such that $f(x_1) = f(x_2)$ has infinitely many rational points off the diagonal, and select those f such that $f(x_1) = f(x_2) = f(x_3)$ has infinitely many rational points off the diagonals. We keep adding variables $x_4, x_5, \ldots$, until some x_{N+1} such that no f is left. This way we will find the uniform bound N.

(2) By Faltings' theorem, if $f(x_1) = f(x_2)$ has infinitely many rational points off the diagonal then $\frac{f(x)-f(y)}{x-y}$ has a genus 0 or 1 component. To find all such f, firstly assume f is indecomposable, i.e. not a composition of two nonlinear polynomials. The monodromy group of f is defined to be the Galois group of $f(x) - t = 0$ over $\mathbb{C}(t)$. When f is indecomposable, the monodromy group is primitive, so all such groups can be understood in terms of powers of simple groups. As a consequence of the classification of finite simple groups, we can find all such groups, which gives information about the components of $\frac{f(x)-f(y)}{x-y}$. Then we use Abyhankar's lemma and the Riemann-Hurwitz genus formula to analyze the ramification in function field towers to get the possible ramification of f. For the general decomposable case, each component of $f(x)-g(y) = 0$ can be related to the indecomposable case via function field towers.

(3) Each step makes heavy use of group theory, Galois theory, the Riemann-Hurwitz formula, Abyhankar's lemma, Riemann's existence theorem, and analysis of ramification in function field towers.

The following is one result we got.

Theorem 1 (Liu-Zieve). *Let K be a number field and $f(x) \in K(x)$ be a Laurent polynomial. If the variety $f(x) = f(y)$ has infinitely many rational points off the diagonal, then the same thing is true if we replace f with $P \circ f \circ \mu$, where P, μ are Laurent polynomials and $\deg(\mu) = 1$. Up to this equivalence, f must be one of the following: x^n, Chebyshev polynomial, $x^i(x-1)^j$, or f is from a short list of families of Laurent polynomials of degree no more than 20.*

This result describes all Laurent polynomials which are at least 2-to-1 infinitely often, and I am currently using it to solve the analogous problem for 3-to-1, 4-to-1, and so on.

2 Diophantine equations $f(x) = g(y)$

Let f and g both be binomial plus constant. The following theorem from [9] gives conditions for $f(x) = g(y)$ to have infinitely many rational solutions. The theorem covers the result of Schinzel et al. [13], which studied when $f(x) = g(y)$ has infinitely many rational solutions with bounded denominator, and our approach is completely different.

Theorem 2 (Liu–Zieve). *Let F, G be polynomials over $\mathbb{Q}$ s.t. $F(x) - F(0)$ (resp. $G(y) - G(0)$) is binomial whose terms have coprime degrees. Let $f(x) = F(x^r)$ and $g(y) = G(y^s)$. If $\deg(f) > 12$ and $\deg(g) > 2$, then $f(x) = g(y)$ has infinitely many solutions in some number field if and only if there exist $u, v \in \mathbb{Q}^*$ such that one of the following holds*

(1) $G(y) = F(uy)$

(2) $f(ux) = g(vy)$, and it can be rewritten as $-nx^{n+1} + (n+1)x^n = k(-ny^{n+1} + (n+1)y^n)$ where $k \in \mathbb{Q}^*$.

Remark. *In [9], we found the list of all f, g (binomial plus a constant) where $f(x) = g(y)$ has infinitely many solutions in some number field. However, the low degree ones cannot be summarized by such simple conditions as the high degree ones in theorem 2.*

Remark. *In [9], when f and g have coprime degrees, we also determined when $f(x) = g(y)$ has infinitely many integer solutions.*

Remark. *It's infeasible to study rational solutions over $\mathbb{Q}$ instead of "some number field" in general, since this includes determining which elliptic curve over $\mathbb{Q}$ has positive rank. For, if $g(y) = y^2 + y$ and $f(x) = x^3 + ax + b$ ($a \neq 0$), then $g(y) = f(x)$ could be any elliptic curve over $\mathbb{Q}$ with nonzero j-invariant.*

The key idea here is to classify f, g such that $f(x) - g(y) = 0$ has a genus 0 or 1 component. The method is similar to my thesis topic. First we assume f, g are indecomposable, use the monodromy group of f and g to find the irreducible component(s) of $f(x) - g(y) = 0$, and then use the Riemann-Hurwitz genus formula to determine the ramification configuration of f and g. The general decomposable case can be solved by ramification analysis on function fields towers. The classification together with Siegel's and Faltings' theorem give the information on integer and rational solutions.

Compared to $\frac{f(x)-f(y)}{x-y}$, this time we need to consider the monodromy group of both f and g, and the ramification is harder to analyze since we need to deal with the ramification from both f and g.

3 Value distribution from functional equations

One connection of my research with complex analysis is through the functional equation $P(f) = Q(g)$, which arises in studying the distribution of values of meromorphic functions. It is studied in many papers [7, 18], where P, Q are polynomials with coefficients in $\mathbb{C}$, and f, g are meromorphic (or analytic) functions. In [7, 18], they treated certain special cases of the functional equation when P, Q have the form $x^n + a_1 x^{n-m} + a_2$ and a_1, a_2 are meromorphic functions which are small compared to f and g in the sense of Nevanlinna theory.

I have completely solved this problem (with P, Q of the form $x^n + a_1 x^{n-m} + a_2$) by combining the methods in my paper [9] with a result of Yamanoi [17], which generalizes Picard's big theorem to the setting of curves over the field of functions having bounded growth.

4 Dynamics of rational functions over finite fields

Dynamics studies the iteration of functions on fields. The dynamics of rational functions over finite field is related to several other areas and has many applications. For instance, it's related to the dynamics on characteristic 0 fields via "reduction by mod p", and it has been used to build finitely ramified number field towers in [1]. However, it appears that all functions behave "randomly" except those from coordinate projections of morphisms between one dimensional algebraic groups (additive groups, multiplicative groups, elliptic curves). These special functions seem to be the only ones we can possibly understand. Some of them are studied by several authors in [3, 4, 6, 2, 14, 16, 15], and for those from endomorphisms of elliptic curves (which we call Lattès maps), only a few special degree 2 examples are understood. In [8], we study and describe the dynamics of all degree-2 Lattès maps over finite fields.

A Lattès map is a rational function $f(x)$ which can make the following diagram commutative, where E is a genus 1 curve over $\bar{K}$, $\phi \in End(E)$ and pr is a nonconstant morphism.

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E \\ \downarrow{\scriptstyle pr} & & \downarrow{\scriptstyle pr} \\ \mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1 \end{array}$$

The dynamics of a rational function f on K is encoded in a graph $D(f, \mathbb{P}^1_K)$ which is defined as follows: its vertices are the elements of $\mathbb{P}^1_K = K \cup \{\infty\}$, and there is a directed edge from v to $f(v)$, for every v in $\mathbb{P}^1_K$.

Theorem 3 (Liu–Zieve)**.** *Let K be a finite field and f be any separable degree-2 Lattès map on K, then each component of $D(f, \mathbb{P}^1_K)$ is one of 6 special types of graphs.*

Remark. *See figure 1 to 4 for examples of the six types of graphs. Each type is formed by a cycle, and a binary tree attached to each cycle point. Trees attached at distinct cycle points are disjoint. Once the cycle length and maximum height of the trees are known, one can draw the component by simple recursive rules.*

The rough idea is: first use ramification and Galois-theoretic arguments to reduce to the case that pr is the projection map $E \to E/\Gamma$, where Γ is a finite group. This step enables us to find all degree-2 Lattès maps, and their associated elliptic curves and 2-isogenies.

Next find $\Omega = pr^{-1}(\mathbb{P}^1_K) \subseteq E(\bar{K})$ and analyze the dynamics of ϕ on Ω, then use it to study the dynamics of f on $\mathbb{P}^1_K$ via $pr : E \to E/\Gamma$. The basic case is $\Gamma = \mu_2$, E is ordinary and E, ϕ are both defined on K. In this case, $\Omega = E[\pi - 1] \cup E[\pi + 1]$ where π is the Frobenius, and crucially $End_K(E)$ is Euclidean so $E[\pi \pm 1]$ can be decomposed into the direct sum of ϕ-torsion part and ϕ-free part. This decomposition enable us to understand the dynamics of ϕ on Ω. Previous papers [6, 16, 15] worked out two examples of this case, using properties specific to their examples.

If E is supersingular or E, ϕ are not defined on K or $\Gamma \neq \mu_2$, this method won't work and the map is harder to analyze. My paper [8] provides a comprehensive theory and many new techniques to handle these situations. Our theory covers all known examples from previous papers [6, 16, 15], and provides many new types of examples.

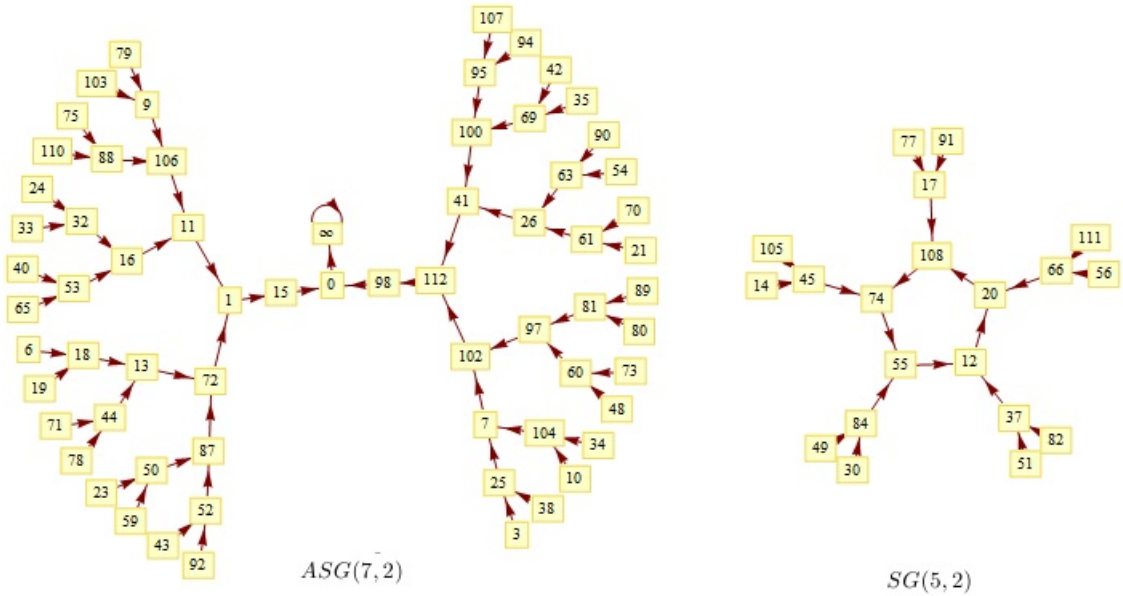

Figure 1: Two components from $D(\frac{15(x^2+1)}{x}, \mathbb{P}^1_{\mathbb{F}_{113}})$

References

[1] Wayne Aitken, Farshid Hajir, and Christian Maire. Finitely ramified iterated extensions. *International Mathematics Research Notices*, 2005(14):855–880, 2005.

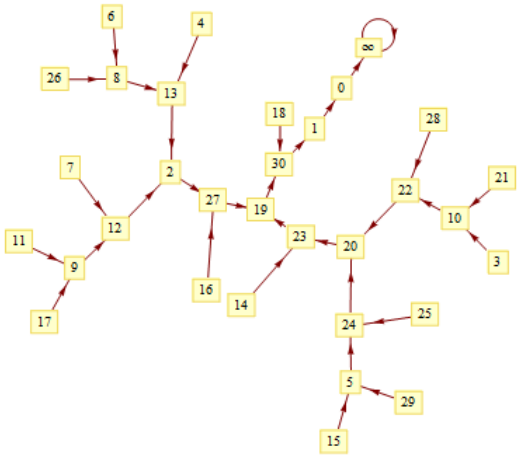

Figure 2: $D(-\frac{(x-1)^2}{4x}, \mathbb{P}^1_{\mathbb{F}_{31}})$

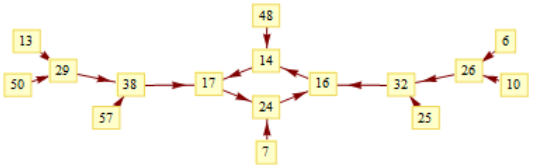

Figure 3: One component of $D(-\frac{(x-1)^2}{4x}, \mathbb{P}^1_{\mathbb{F}_{59}})$

[2] T. Alden Gassert. Chebyshev action on finite fields. *Discrete Math.*, 315:83–94, 2014.

[3] Anjula Batra and Patrick Morton. Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. I. *Rocky Mountain J. Math.*, 24(2):453–481, 1994.

[4] Anjula Batra and Patrick Morton. Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. II. *Rocky Mountain J. Math.*, 24(3):905–932, 1994.

[5] A Carney, R Hortsch, and Michael Zieve. Near-injectivity of polynomial maps. *preprint*, 2013.

[6] Shuhong Gao and Jang-Woo Park. Dynamics of $x + \frac{1}{x}$ via elliptic curves. *preprint*, 2011.

[7] Huy Khoai Ha and C. C. Yang. On the functional equation $P(f) = Q(g)$. In *Value distribution theory and related topics*, volume 3 of *Adv. Complex Anal. Appl.*, pages 201–207. Kluwer Acad. Publ., Boston, MA, 2004.

[8] Sijun Liu and Michael Zieve. The dynamics of lattès maps on finite fields. *preprint*, 2013.

[9] Sijun Liu and Michael Zieve. On the integer and rational solutions of equation $ax^m + bx^n + c = dy^p + ey^q$. *preprint*, 2013.

[10] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[11] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

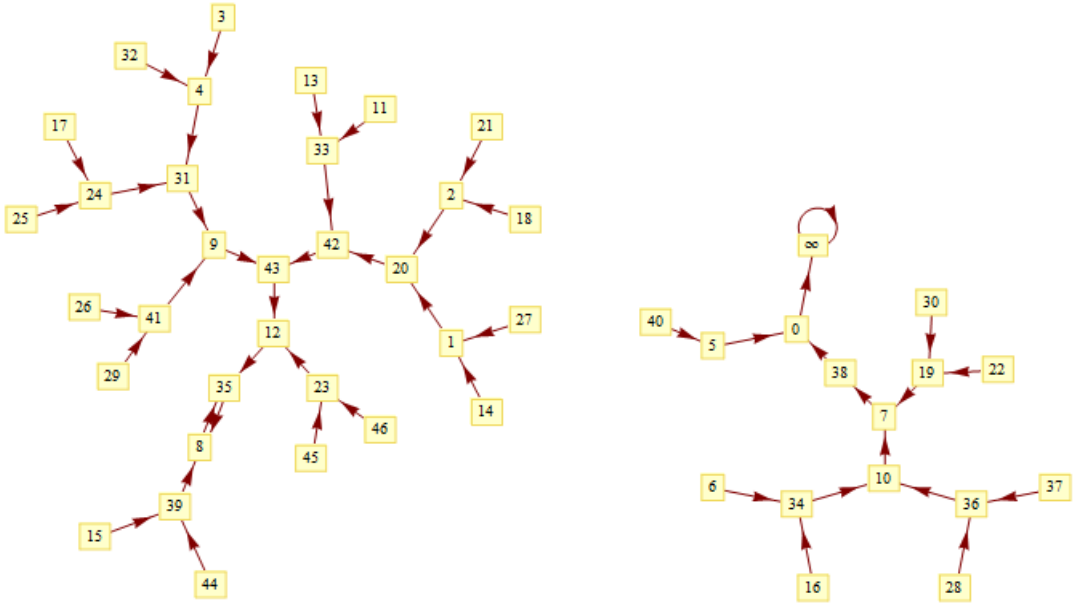

Figure 4: $D(-\frac{x}{2} - 2 - \frac{1}{x}, \mathbb{P}^1_{\mathbb{F}_{47}})$

[12] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[13] Gyöngyvér Péter, Ákos Pintér, and Andrzej Schinzel. On equal values of trinomials. *Monatsh. Math.*, 162(3):313–320, 2011.

[14] Thomas D. Rogers. The graph of the square mapping on the prime fields. *Discrete Math.*, 148(1-3):317–324, 1996.

[15] S. Ugolini. Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two. *Theory and applications of finite fields*, 579:187–204, 2012.

[16] S Ugolini. Graphs associated with the map x x+ x- 1 in finite fields of characteristic three and five. *Journal of Number Theory*, 133(4):1207–1228, 2013.

[17] Katsutoshi Yamanoi. The second main theorem for small functions and related problems. *Acta mathematica*, 192(2):225–294, 2004.

[18] Chung-Chun Yang and Ping Li. Some further results on the functional equation $P(f) = Q(g)$. In *Value distribution theory and related topics*, volume 3 of *Adv. Complex Anal. Appl.*, pages 219–231. Kluwer Acad. Publ., Boston, MA, 2004.