Topics on Polynomial Equations in Noncommutative Rings and Motivic Aspects of Moduli Spaces

Yifeng Huang

University of Michigan

Mar. 14, 2022

Defense committee[†]:

Michael Zieve, chair
Jeffrey Lagarias, member
Mircea Mustaţă, member
Aaron Pierce, cognate

Overview of the talk

The talk covers (hopefully all) three independent topics at the interface of several research areas:

1. Part 1: Number theory
   Unit equations on the quaternion algebra; Diophantine equations.
2. Part 2: Combinatorics
   Polynomial equations on the algebra of n by n matrices; Point counting of moduli spaces of modules.
3. Part 3: Algebraic geometry
   Topology of configuration spaces of points; Mixed Hodge theory.

Two things stemming from equations

- Diophantine equation:
  a (system of) polynomial equation(s) that asks for integer (or sometimes rational) solutions.
  - We usually care about the existence and infinitude of solutions.
  - The nature is discrete, and when viewed naïvely, every solution is a coincidence to some extent.
  - Example: $x^3 + y^3 + z^3 = 42$ for integers x, y, z. (Booker and Sutherland, 2019; 17-digit solution!)
- Algebraic variety (or "variety"):
  the solution set of a (system of) polynomial equation(s), typically over the real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$.
  - We usually care about its geometry; rich structures can be put on the solution set.
  - The nature is continuous; solutions typically exist and form a continuum.
  - Examples: a parabola $y = x^2$, or more generally, a conic section $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$.

Unit equations: background

A unit equation is an equation of the form

$$x + y = 1,$$

where x and y are generally required to have a specific form expressed by multiplication.

Example

Find solutions of $x + y = 1$, where $x = \pm 2^n, y = \pm 3^n, m, n \in \mathbb{Z}$.

One can soon find these solutions:

$$(x, y) = (2, -1), (-2, 3), (4, -3), (-8, 9).$$

Question

Are there more solutions?

Unit equations: background

Example

Find solutions of $x + y = 1$, where $x = \pm 2^n, y = \pm 3^n, m, n \in \mathbb{Z}$.

Question

Are there more solutions?

Answer

No (nontrivial)! More generally, any equation of this kind only has at most finitely many solutions. (coming next)

Unit equations: background

Theorem (Beukers and Schlickewei, 1996)

Let Γ be a finitely generated subgroup of $\mathbb{C}^\times$ (the multiplicative group). Then the equation

$$x + y = 1, \qquad x, y \in \Gamma$$

has at most finitely many solutions (x, y).

The hypothesis means that x and y are of the form $a_1^{n_1} \dots a_r^{n_r}$ for fixed $a_1, \dots, a_r \in \mathbb{C}^\times$ and freely chosen integers $n_1, \dots, n_r$. This theorem tells us something deep about how addition and multiplication interact.

Unit equations: contributions

We proved the first noncommutative analogue of the theorem. We considered quaternions $\mathbb{H}$ in place of $\mathbb{C}$. Multiplication on $\mathbb{H}$ is not commutative.

Theorem 1 (H., 2020)

Let Γ_1, Γ_2 be finitely generated semigroups[a] of $\mathbb{H}^\times$. If Γ_1 is commutative, then the equation $x + y = 1$ has at most finitely many solutions with $x \in \Gamma_1$ and $y \in \Gamma_2$.

[a] Technical assumption: they must be generated by algebraic quaternions of norms greater than 1.

Typical example. Say f_1, f_2, a, b, c are fixed quaternions (satisfying the same technical condition) such that f_1, f_2 commute, then the unit equation $x + y = 1$ has at most finitely many solutions if x is of the form $f_1^{n_1} f_2^{n_2}$ where $n_1, n_2 \geq 0$, and y is any word in a, b, c (for example, $bccab$; here, inverses like a^{-1} are not allowed.).

Unit equations: methods

- What's old:
  - The proof used the "Baker's method", a method based on estimates of linear combinations of logarithms that has been widely applied to the study of unit equations.
- What's new:
  - Since quaternions are noncommutative, an essential tool for the classical unit equations, namely the p-adic norm, is no longer available.
  - Fortunately, the usual absolute value is available and turns out to be enough to prove the result.

Unit equations: applications

- The classical commutative result
  - was used to prove that certain Diophantine equations (for example, $y^2 = x^3 + x + 1$) have at most finitely many integer solutions.
  - was used to prove a result (Odesky 2020) about iterations of self-maps of abelian varieties with commutative endomorphism rings. (natural application, because composition of self-maps correspond to multiplication in the endomorphism ring.)
- The new noncommutative result relaxes the commutativity assumption in Odesky's result. Key: $\mathrm{End}(E) \subseteq \mathbb{H}$.

Corollary 2 (H., 2020)

Let E be a (possibly supersingular) elliptic curve over an algebraically closed field k, and let $f, g : E \to E$ be regular maps of degrees greater than 1. If there are points $A, B \in E(k)$ such that the forward orbits $O_f(A) := \{A, f(A), f^2(A), \ldots\}$ and $O_g(B) := \{B, g(B), g^2(B), \ldots\}$ have infinite intersection, then f and g have a common iterate, namely, $f^{m_0} = g^{n_0}$ for some positive integers m_0, n_0.

Pause 1 out of 3

Questions?

Matrix enumeration: background

In 1960, Feit and Fine proved a beautiful formula that counts pairs of commuting matrices over a finite field $\mathbb{F}_q$ of q elements.

Theorem (Feit and Fine, 1960)

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA\}|}{|\mathrm{GL}_n(\mathbb{F}_q))|} x^n = \prod_{i,j \geq 1} \frac{1}{1 - x^i q^{2-j}},$$

where

$$|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}).$$

One can read the counts from the x-coefficients of RHS. This generating function with a normalization factor $1/|\mathrm{GL}_n(\mathbb{F}_q)|$ is the nicest way to present the answer to the counting problem (for a good reason).

Matrix enumeration: background

How does this problem fit in the theme of the talk?

- It is essentially about the solution set of the equation $AB = BA$ on the noncommutative ring $\mathrm{Mat}_n(\mathbb{C})$. (Not $\mathbb{F}_q$!!)
- We focus on the geometric feature of how the solution set is composed of simpler varieties (like $\mathbb{C}^n$) via taking disjoint unions and complements.
- The essential part of this geometric feature is completely encapsulated by point counting over $\mathbb{F}_q$; this is why we stated the result over $\mathbb{F}_q$.
- The flavor of such a problem is geometric and combinatorial.

Matrix enumeration: contribution 1

We found the generating functions for the solution counts of two other matrix equations. The first one generalizes the result of Feit and Fine.

Theorem 3 (H., 2022)

Let ζ be a primitive m-th root of unity of $\mathbb{F}_q$. Then

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = \zeta BA\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n = \prod_{i=1}^{\infty} F_m(x^i; q),$$

where

$$F_m(x; q) := \frac{1 - x^m}{(1 - x)(1 - x^m q)} \cdot \frac{1}{(1 - x)(1 - xq^{-1})(1 - xq^{-2}) \dots}.$$

Feit–Fine is the case where $\zeta = 1, m = 1$. The right-hand side is an explicit series in x, which is notably an infinite product of simple factors.

Matrix enumeration: contribution 2

The second result is an analogue of Feit–Fine. It counts mutually annihilating matrices, namely, matrix pairs (A, B) with $AB = BA = 0$. We use the notation

$$(a;t)_n = (1-a)(1-at)\dots(1-at^{n-1}).$$

Theorem 4 (H., 2022+)

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n = \frac{1}{(x;q^{-1})_\infty^2} H_q(x),$$

where

$$H_q(x) := \sum_{k=0}^{\infty} \frac{q^{-k^2} x^{2k}}{(q^{-1};q^{-1})_k} (xq^{-k-1};q^{-1})_\infty.$$

Its significance will be explained after a general discussion.

Matrix enumeration: interpretations

Geometric interpretation in terms of moduli spaces:

- A moduli space is a space that parametrizes all possible structures of a certain kind.
  Example. $\mathbb{P}^1 = \{\text{lines through } 0 \text{ in } \mathbb{A}^2\}$.
- Each of the theorems above turns out to be the point count of a moduli space that parametrizes modules over a certain ring R, where
  - R is the affine plane $\mathbb{F}_q[X, Y]$ in Feit–Fine ($AB = BA$);
  - R is the quantum plane $\mathbb{F}_q\{X, Y\}/(XY - \zeta YX)$ in the $AB = \zeta BA$ theorem;
  - R is a nodal curve $\mathbb{F}_q[X, Y]/(XY)$ in the $AB = BA = 0$ theorem.
- **Last one explained.** An $\mathbb{F}_q[X, Y]/(XY)$-mod structure on ${\mathbb{F}_q}^n$ $\leftrightsquigarrow$ How X, Y act (say X as $A \curvearrowright {\mathbb{F}_q}^n$, Y as B) $\leftrightsquigarrow$ $AB = BA = 0$ in $\mathrm{Mat}_n(\mathbb{F}_q)$.
- The generating function (with the $1/|\mathrm{GL}_n(\mathbb{F}_q)|$ factor!) encodes a natural weighted count of those modules, called the Cohen–Lenstra measure.

Matrix enumeration: significance

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n = \frac{1}{(x; q^{-1})_\infty^2} H_q(x),$$

where

$$H_q(x) := \sum_{k=0}^{\infty} \frac{q^{-k^2} x^{2k}}{(q^{-1}; q^{-1})_k} (xq^{-k-1}; q^{-1})_\infty.$$

- Recall that this is the generating function associated to a nodal curve, which is singular.
- In fact, the generating function associated to any smooth curve and smooth surface is well-known.
- This is the first result about the singular case.
- The most surprising feature is that the mysterious factor $H_q(x)$ is an entire function in x. This suggests that singular cases, while mostly mysterious, may have some general patterns.

Pause 2 out of 3

Questions?

Configuration spaces: background

Let $n \geq 0$. The n-th configuration space of a base space X is the moduli space of unordered tuples of n distinct points on X:

$$\mathrm{Conf}^n(X) := \{(x_1, \ldots, x_n) \in X^n : x_i \neq x_j\}/S_n.$$

Here, X can be a topological space or a quasi-projective variety over any field.

Recall the geometric feature of how a variety is composed of simpler ones via "cut-and-paste". This invariant is called the motivic class. It turns out that the motivic classes of configuration spaces follow a simple combinatorial pattern (Vakil and Wood, 2015).

Configuration spaces: background

We focus on the Betti numbers of configuration spaces. For each space we can talk about the i-th Betti number $h^i(\cdot)$ for every $i \geq 0$. The Betti numbers are topological invariants that remember things like "the number of holes on a surface".

The motivic class determines many other invariants, such as point counts over finite fields and Euler characteristic. Such invariants are called motivic invariants. However, the Betti number is not a motivic invariant, so the Betti numbers of configuration spaces are not automatically known.

Nevertheless, this nonmotivic invariant often has combinatorial behaviors similar to those of the motivic invariants. We proved two results that illustrate this point.

Configuration spaces: contribution 1

The first result states that the Betti numbers of configuration spaces of a punctured torus are given by a rational generating function.

Theorem 5 (Cheong and H., 2022)

Let $E^\times$ be an elliptic curve over $\mathbb{C}$ minus one point, and let $h^i(\cdot)$ denote the i-th Betti number. Then

$$\sum_{i,n\geq 0} (-1)^i h^i(\mathrm{Conf}^n(E^\times)) u^{2n-w(i)} t^n = \frac{(1-ut)^2(1-u^2t^2)}{(1-u^2t)(1-ut^2)^2},$$

where $w(i) = \lfloor 3i/2 \rfloor$.

The right-hand side is in fact a certain motivic invariant of the spaces in question. The degree shifting $w(i)$ is required to "match" the nonmotivic invariant and the motivic one, and it turns out that $w(i)$ has a clear geometric meaning.

Configuration spaces: contribution 1

The geometric significance of $w(i)$ lies in the mixed Hodge theory. The following statement, which we do not explain its meaning, would directly imply our result using general arguments in the mixed Hodge theory.

Theorem 6 (Cheong and H., 2022)

The mixed Hodge structure on $H^i(\mathrm{Conf}^n(E^\times);\mathbb{Q})$ is pure of weight $w(i) = \lfloor 3i/2 \rfloor$.

This statement that finds the geometric meaning of $w(i)$ is in fact the major content of our work.

Configuration spaces: contribution 2

What if there are two or more punctures? The second result describes how puncturing a *noncompact* base space affects the Betti numbers of its configuration spaces. Let $X^\times$ denote X minus any one point.

Theorem 7 (H., 2022+)

Let X be a smooth noncompact complex variety of dimension d. Under a mixed-Hodge-theoretic assumption[a] on X, the Betti numbers of $\mathrm{Conf}^n(X^\times)$ are given by

$$\sum_{i,n\geq 0} h^i(\mathrm{Conf}^n(X^\times))u^i t^n = \frac{1}{1-u^{2d-1}t}\sum_{i,n\geq 0} h^i(\mathrm{Conf}^n(X))u^i t^n.$$

[a] The precise assumption is that X is a noncompact variety $\overline{X}$ minus zero or more points, such that the i-th cohomology of $\overline{X}$ is pure of a weight proportional to i.

If X is a connected smooth compact variety minus $r \geq 1$ points, then the assumption is satisfied; this recovers Kallel 2008.

Configuration spaces: contribution 2

$$\sum_{i,n\geq 0} h^i(\mathrm{Conf}^n(X^\times))u^i t^n = \frac{1}{1-u^{2d-1}t} \sum_{i,n\geq 0} h^i(\mathrm{Conf}^n(X))u^i t^n.$$

- An analogue in terms of motivic classes is known (and is an easy consequence of the knowledge of motivic classes of configuration spaces in general).
- The Betti number is not motivic, so the analogy needs a separate explanation.
- We gave a much refined result[1] that implies the theorem and its motivic analogue simultaneously, explaining the analogy; this is the major content of this work.

[1] The refined result is in terms of mixed Hodge numbers and the cohomology of the *ordered* configuration spaces as an S_n-representation.

Configuration spaces: methods

- Leray spectral sequence computes the cohomology of $\mathrm{Conf}^n(X)$ based on the cohomology of X and explicit generators and relations.
- There is a freedom here: we can actually choose any $\overline{X}$ such that X is open in $\overline{X}$. Then the Leray spectral sequence would involve cohomology of $\overline{X}$ and some extra generators and relations that depend on the combinatorics of the complement $\overline{X} \setminus X$.
- But the computation is only manageable if $\overline{X}$ satisfies a purity condition in the mixed Hodge theory.
- To work on the punctured elliptic curve $X = E^\times$ (Theorem 6), we just choose $\overline{X} = X$ because the purity condition is satisfied.
- To work on Theorem 7, say the case where X is a six-punctured curve, we must choose $\overline{X}$ to be a one-punctured curve, so $\overline{X}$ has the purity condition. The price is extra combinatorics due to the extra five punctures, but that turns out to be manageable.
- The noncompactness of $\overline{X}$ is equivalent to $H^{\mathrm{top}}(\overline{X}) = 0$, which is necessary as the computation turns out.

Pause 3 out of 3

Questions?

Thank you and happy π day!