# Applications of the trace of Frobenius
# past, present, and future

Tony Feng

September 25, 2020

# Applications of the trace of Frobenius past, present, and future

Tony Feng

September 25, 2020

# Weil's conjecture for curves

Consider the equation

$$y^2 = x^3 + x^2 + x + 1$$

# Weil's conjecture for curves

Consider the equation

$$y^2 = x^3 + x^2 + x + 1$$

How many solutions in $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$?

# Weil's conjecture for curves

Consider the equation

$$y^2 = x^3 + x^2 + x + 1$$

How many solutions in $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$?

How many solutions in $\mathbb{F}_{p^n}$?

# Weil's conjecture for curves

Consider the equation

$$y^2 = x^3 + x^2 + x + 1$$

How many solutions in $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$?

How many solutions in $\mathbb{F}_{p^n}$?

Answer: $p^n + O(p^{n/2})$

# Weil's conjecture for curves

Consider the equation

$$y^2 = x^3 + x^2 + x + 1$$

How many solutions in $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$?

How many solutions in $\mathbb{F}_{p^n}$?

Answer: $p^n + O(p^{n/2})$

This is a case of Weil's conjecture.

# Frobenius endomorphism

$$y^2 = x^3 + x^2 + x + 1$$

# Frobenius endomorphism

$$y^2 = x^3 + x^2 + x + 1$$

In characteristic $p$, $(a + b)^p = a^p + b^p$.

# Frobenius endomorphism

$$y^2 = x^3 + x^2 + x + 1$$

In characteristic $p$, $(a + b)^p = a^p + b^p$.

If $(a, b)$ is a solution, then $(a^p, b^p)$ is a solution:

# Frobenius endomorphism

$$y^2 = x^3 + x^2 + x + 1$$

In characteristic $p$, $(a + b)^p = a^p + b^p$.

If $(a, b)$ is a solution, then $(a^p, b^p)$ is a solution:

$$0 = (b^2 - a^3 - a^2 - a - 1)^p$$

# Frobenius endomorphism

$$y^2 = x^3 + x^2 + x + 1$$

In characteristic $p$, $(a+b)^p = a^p + b^p$.

If $(a, b)$ is a solution, then $(a^p, b^p)$ is a solution:

$$0 = (b^2 - a^3 - a^2 - a - 1)^p = (b^p)^2 - (a^p)^3 - (a^p)^2 - a^p - 1$$

# Frobenius endomorphism

$$y^2 = x^3 + x^2 + x + 1$$

In characteristic $p$, $(a+b)^p = a^p + b^p$.

If $(a, b)$ is a solution, then $(a^p, b^p)$ is a solution:

$$0 = (b^2 - a^3 - a^2 - a - 1)^p = (b^p)^2 - (a^p)^3 - (a^p)^2 - a^p - 1$$

$\implies$ there is a **symmetry** $(a, b) \mapsto (a^p, b^p)$ on the space of solutions, called the Frobenius endomorphism.

# Weil's conjecture for curves

Consider the equation

$$y^2 = x^3 + x^2 + x + 1$$

How many solutions in $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$?

How many solutions in $\mathbb{F}_{p^n}$?

Answer: $p^n + O(p^{n/2})$

This is a case of Weil's conjecture.

# Weil's conjecture

There is a generalization to more complicated systems of equations $Z$, called Weil's Conjecture, proved by Deligne (1974).

# Weil's conjecture

There is a generalization to more complicated systems of equations $Z$, called Weil's Conjecture, proved by Deligne (1974).

**Fundamental identity** (Grothendieck)

$$\#\{\text{solutions to } Z \text{ in } \mathbb{F}_{p^n}\} = \mathrm{Tr}(\mathrm{Frob}_p^n, H^*(Z)).$$

# Weil's conjecture

There is a generalization to more complicated systems of equations $Z$, called Weil's Conjecture, proved by Deligne (1974).

**Fundamental identity** (Grothendieck)

$$\#\{\text{solutions to } Z \text{ in } \mathbb{F}_{p^n}\} = \mathrm{Tr}(\mathrm{Frob}_p^n, H^*(Z)).$$

Enables geometric and algebraic tools:

- nearby cycles, monodromy, Lefschetz pencils, spectral sequences, etc.

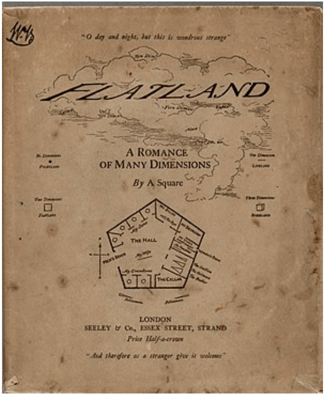
# The past

$$\boxed{\underbrace{\#\{\text{solutions to } Z \text{ in } \mathbb{F}_{p^n}\}}_{\text{number}} = \mathrm{Tr}(\mathrm{Frob}_p^n,\ \ \underbrace{H^*(Z)}_{\text{vector space}}\ \ )}$$

# The past

$$\boxed{\underbrace{\#\{\text{solutions to } Z \text{ in } \mathbb{F}_{p^n}\}}_{\text{number}} = \mathrm{Tr}(\mathrm{Frob}_p^n,\quad \underbrace{H^*(Z)}_{\text{vector space}}\ )}$$

What's next?



"O day and night, but this is wondrous strange"

FLATLAND

A ROMANCE
OF MANY DIMENSIONS

*By* A Square

LONDON
SEELEY & Co., ESSEX STREET, STRAND
*Price Half-a-crown*

"And therefore as a stranger give it welcome"

# Hierarchy of traces

$$\begin{tikzcd} \text{Numbers} & \text{Vector spaces} \arrow[l, bend right, "\text{Trace}"'] & ??? \arrow[l, bend right, "\text{Trace}"'] \end{tikzcd}$$

(Rings, complexes, etc.)

2

3

$4 = 2^2$

5

$\mathbb{R}^2 \to \mathbb{R}^3$

$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^n}$

$$\begin{tikzcd} \mathbb{C}[x] \arrow[d] \\ \mathbb{C}[x]/x^2 \end{tikzcd}$$

# Hierarchy of traces

Numbers $\xleftarrow{\text{Trace}}$ Vector spaces $\xleftarrow{\text{Trace}}$ ???

(Rings, complexes, etc.)

2

3

$4 = 2^2$

5

- Equality between objects.

$\mathbb{R}^2 \to \mathbb{R}^3$

$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^n}$

$\mathbb{C}[x] \twoheadrightarrow \mathbb{C}[x]/x^2$

- Maps between objects.
- Equality between maps.

# Hierarchy of traces

$$\begin{tikzcd} \text{Numbers} & \text{Vector spaces} \arrow[l, bend right, "\text{Trace}"] & & \text{Categories} \arrow[ll, bend right, "\text{Trace}"] \end{tikzcd}$$

(Rings, complexes, etc.)

2

3

$4 = 2^2$

5

$\mathbb{R}^2 \to \mathbb{R}^3$

$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^n}$

$$\begin{tikzcd} \mathbb{C}[x] \arrow[d] \\ \mathbb{C}[x]/x^2 \end{tikzcd}$$

$$\begin{tikzcd} \mathrm{Sheaves}(X) \arrow[d, bend right, "f_!"'] \arrow[d, bend left, "f_*"] \arrow[d, phantom, "\Longrightarrow"] \\ \mathrm{Sheaves}(Y) \end{tikzcd}$$

- Equality between objects.

- Maps between objects.
- Equality between maps.

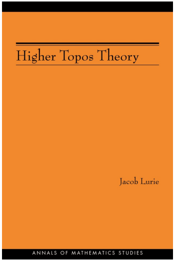
- Maps between objects.
- Maps between maps.

# Categorical traces

Ben-Zvi–Nadler, Gaitsgory: an endomorphism of a category has a trace.

# Categorical traces

Ben-Zvi–Nadler, Gaitsgory: an endomorphism of a category has a trace.



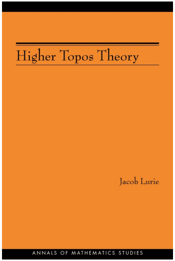
Higher Topos Theory

Jacob Lurie

ANNALS OF MATHEMATICS STUDIES

# Categorical traces

Ben-Zvi–Nadler, Gaitsgory: an endomorphism of a category has a trace.

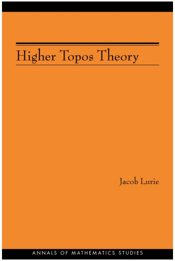


Applications:

- Categorical proof of Hirzebruch-Riemann-Roch

# Categorical traces

Ben-Zvi–Nadler, Gaitsgory: an endomorphism of a category has a trace.



Applications:

- Categorical proof of Hirzebruch-Riemann-Roch
- (Xiao-Zhu) Tate conjecture on products of Shimura varieties

# The commuting variety conjecture

Lie algebra $\mathfrak{g}$ = vector space (of matrices) with notion of commutator $[X, Y]$ for $X, Y \in \mathfrak{g}$.

# The commuting variety conjecture

Lie algebra $\mathfrak{g}$ = vector space (of matrices) with notion of commutator $[X, Y]$ for $X, Y \in \mathfrak{g}$.

- ("Type A") $\mathfrak{gl}_n = \{X \in \mathrm{Mat}_n(\mathbb{C})\}$,

$$[X, Y] = XY - YX.$$

# The commuting variety conjecture

Lie algebra $\mathfrak{g}$ = vector space (of matrices) with notion of commutator $[X, Y]$ for $X, Y \in \mathfrak{g}$.

- ("Type A") $\mathfrak{gl}_n = \{X \in \mathrm{Mat}_n(\mathbb{C})\}$,

$$[X, Y] = XY - YX.$$

- ("Type $B$") $\mathfrak{so}_{2n+1} = \{X \in \mathrm{Mat}_{2n+1}(\mathbb{C}) \colon X + X^t = 0\}$

$$[X, Y] = XY - YX.$$

# The commuting variety conjecture

Lie algebra $\mathfrak{g}$ = vector space (of matrices) with notion of commutator $[X, Y]$ for $X, Y \in \mathfrak{g}$.

- ("Type A") $\mathfrak{gl}_n = \{X \in \mathrm{Mat}_n(\mathbb{C})\}$,

$$[X, Y] = XY - YX.$$

- ("Type $B$") $\mathfrak{so}_{2n+1} = \{X \in \mathrm{Mat}_{2n+1}(\mathbb{C}) \colon X + X^t = 0\}$

$$[X, Y] = XY - YX.$$

**Conjecture**

*The commuting variety* $\{X, Y \in \mathfrak{g} \colon [X, Y] = 0\}$ *is reduced, i.e.* $f^2 = 0 \implies f = 0$.

# The commuting variety conjecture

Example: $\mathfrak{gl}_2$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}$$

# The commuting variety conjecture

Example: $\mathfrak{gl}_2$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}$$

Reduced means if $P^2 = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$, then $P = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$.

# The commuting variety conjecture

Example: $\mathfrak{gl}_2$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}$$

Reduced means if $P^2 = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$, then $P = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$.

Example of something non-reduced: $\mathbb{C}[a]/a^2$.

# The commuting variety conjecture

Example: $\mathfrak{gl}_2$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}$$

Reduced means if $P^2 = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$, then $P = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$.

Example of something non-reduced: $\mathbb{C}[a]/a^2$.

Note: $\mathrm{GL}_2(\mathbb{C})$ acts on the space of solutions by simultaneous conjugation.

# The commuting variety conjecture

Example: $\mathfrak{gl}_2$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}$$

Reduced means if $P^2 = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$, then $P = 0 \in \mathbb{C}[a, b, c, d, e, f, g, h]/(ae + bg = ae + fc, \ldots)$.

Example of something non-reduced: $\mathbb{C}[a]/a^2$.

Note: $\mathrm{GL}_2(\mathbb{C})$ acts on the space of solutions by simultaneous conjugation.

**Conjecture**

*The variety $\{X, Y \in \mathfrak{g} \colon [X, Y] = 0\}/$conjugation by $G$ is reduced.*

# Trace of Frobenius on the Satake category

(Joint with Dennis Gaitsgory)

# Trace of Frobenius on the Satake category

(Joint with Dennis Gaitsgory)

$$\begin{tikzcd}
\text{(modular) coherent} \\ \text{Satake category for } G \arrow[d, dashed, "\text{trace of Frob}"'] \\
\sim \dfrac{\text{commuting variety of } \mathfrak{g}}{\text{conjugation by } G}
\end{tikzcd}$$

# Trace of Frobenius on the Satake category

(Joint with Dennis Gaitsgory)

$$\begin{tikzcd}
\begin{array}{c}\text{(modular) coherent} \\ \text{Satake category for } G\end{array} \arrow[r, equal, "\text{Arinkin-Bezrukavnikov}"] \arrow[d, dashed, "\text{trace of Frob}"'] & \begin{array}{c}\text{(modular) constructible} \\ \text{Satake category for } \widehat{G}\end{array} \\
\sim \dfrac{\text{commuting variety of } \mathfrak{g}}{\text{conjugation by } G} &
\end{tikzcd}$$

# Trace of Frobenius on the Satake category

(Joint with Dennis Gaitsgory)

$$\begin{tikzcd}
\begin{array}{c}\text{(modular) coherent} \\ \text{Satake category for } G\end{array} \arrow[r, equal, "\text{Arinkin-Bezrukavnikov}"] \arrow[d, dashed, "\text{trace of Frob}"'] & \begin{array}{c}\text{(modular) constructible} \\ \text{Satake category for } \widehat{G}\end{array} \arrow[d, dashed, "\text{trace of Frob}"] \\
\sim \dfrac{\text{commuting variety of } \mathfrak{g}}{\text{conjugation by } G} \arrow[r, dashed, leftrightarrow] & \begin{array}{c}\text{derived Hecke algebra for } \widehat{G} \\ \text{(Venkatesh)}\end{array}
\end{tikzcd}$$

# Trace of Frobenius on the Satake category

(Joint with Dennis Gaitsgory)

$$\begin{tikzcd}
\begin{array}{c}\text{(modular) coherent}\\ \text{Satake category for } G\end{array} \arrow[r, equal, "\text{Arinkin-Bezrukavnikov}"] \arrow[d, dashed, "\text{trace of Frob}"'] & \begin{array}{c}\text{(modular) constructible}\\ \text{Satake category for } \widehat{G}\end{array} \arrow[d, dashed, "\text{trace of Frob}"] \\
\sim \dfrac{\text{commuting variety of } \mathfrak{g}}{\text{conjugation by } G} \arrow[r, leftrightarrow, dashed] & \begin{array}{c}\text{derived Hecke algebra for } \widehat{G}\\ \text{(Venkatesh)}\end{array}
\end{tikzcd}$$

## Theorem

*If this picture is correct, then* $\dfrac{\textit{commuting variety of } \mathfrak{g}}{\textit{conjugation by } G}$ *is reduced in types* $A, B, C$ *(as a consequence of a much more precise theorem).*

# Trace of Frobenius on the Satake category

(Joint with Dennis Gaitsgory)

$$\begin{tikzcd}
\begin{array}{c}\text{(modular) coherent} \\ \text{Satake category for } G\end{array} \arrow[r, equal, "\text{Arinkin-Bezrukavnikov}"] \arrow[d, dashed, "\text{trace of Frob}"'] & \begin{array}{c}\text{(modular) constructible} \\ \text{Satake category for } \widehat{G}\end{array} \arrow[d, dashed, "\text{trace of Frob}"] \\
\sim \dfrac{\text{commuting variety of } \mathfrak{g}}{\text{conjugation by } G} \arrow[r, dashed, leftrightarrow] & \begin{array}{c}\text{derived Hecke algebra for } \widehat{G} \\ \text{(Venkatesh)}\end{array}
\end{tikzcd}$$

## Theorem

*If this picture is correct, then* $\frac{\text{commuting variety of } \mathfrak{g}}{\text{conjugation by } G}$ *is reduced in types* $A, B, C$ *(as a consequence of a much more precise theorem).*

## Theorem

*If this picture is correct, then the derived Hecke algebra for* $\widehat{G}$ *is commutative (except possibly in small characteristics).*

For $T\colon V \to V$, $\mathrm{Tr}(T)$ is

$$k \to V \otimes V^\vee \xrightarrow{T \otimes \mathrm{Id}} V \otimes V^\vee \to k.$$

$$(\text{Derived commuting variety of } \mathfrak{g})^{\widehat{G}} \xrightarrow{\sim} (\text{Derived commuting variety of } \mathfrak{t})^{W}$$