Arithmetic statistics and graded Lie algebras

Jef Laga

University of Cambridge

March 17, 2022

Motivation

Given a family of curves $\mathcal{F}$ over $\mathbb{Q}$, want to study statistical behaviour of $C \in \mathcal{F}$:

- Rational points $C(\mathbb{Q})$,
- Mordell-Weil group $J(\mathbb{Q})$,
- 2-Selmer group $\mathrm{Sel}_2 J$.

Recall the exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}_2 J \to Ш(J)[2] \to 0.$$

Example 1: Elliptic Curves

$\mathcal{F} = \{\text{elliptic curves over } \mathbb{Q}\}$. Every $E \in \mathcal{F}$ has unique equation

$$E_{A,B} : y^2 = x^3 + Ax + B, \quad (A, B \in \mathbb{Z})$$

where no prime p has $p^4 \mid A$ and $p^6 \mid B$. Define

$$H(E_{A,B}) = \max\left(|A|^3, |B|^2\right).$$

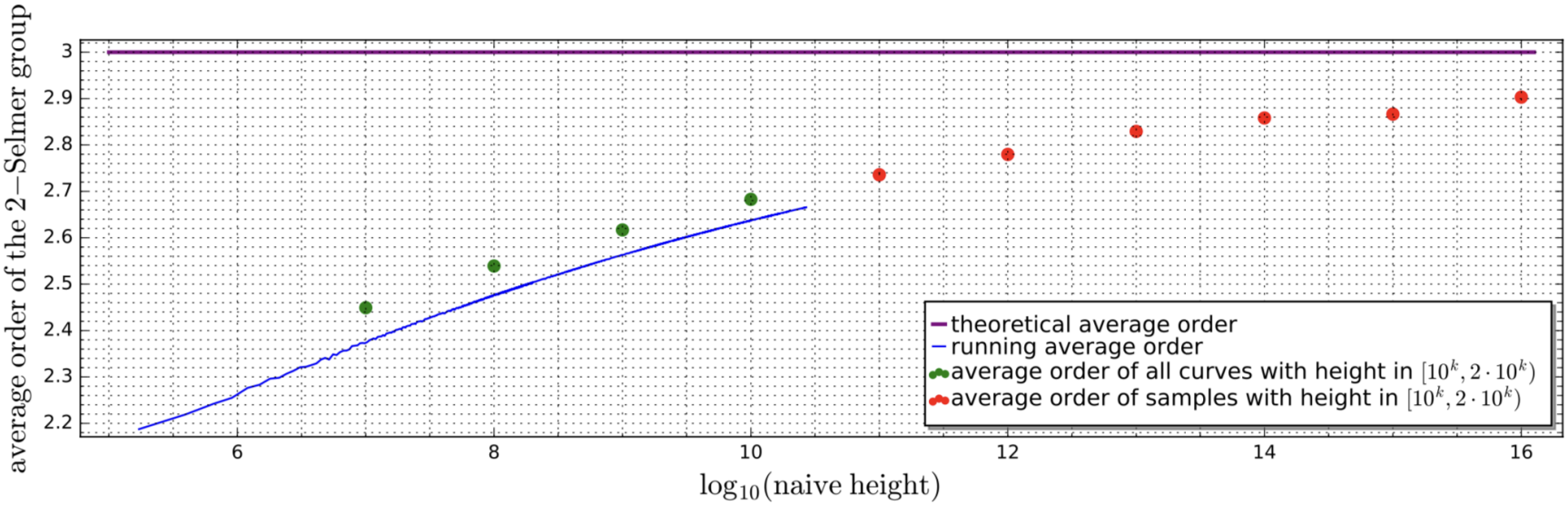
Theorem (Bhargava-Shankar)

When ordered by height,

$$\mathit{Average}(\#\,\mathrm{Sel}_2(E) \mid E \in \mathcal{F}) = 3.$$

Example 1: Elliptic curves

FIGURE 6. *Average order of the 2-Selmer groups, including samples ($\log_{10}$ scale)*



Source: Balakrishnan, Ho, Kaplan, ... (ANTS XII)

Example 2: Hyperelliptic curves

Bhargava and Gross obtained similar results for the family

$$\mathcal{F}_g = \{\text{odd hyperelliptic curves of genus } g/\mathbb{Q}\}$$

for every $g \geq 1$. Poonen and Stoll used this to show that

$$\mathbb{P}(C \in \mathcal{F}_g \mid \#C(\mathbb{Q}) = 1) \to 1$$

as $g \to +\infty$.

Proof method

Roughly speaking, two steps in proving the theorems of Bhargava–Shankar and Bhargava–Gross:

1. Find a representation V of a reductive group $G/\mathbb{Q}$ such that

$$\left\{\begin{array}{c}\text{certain } G(\mathbb{Q})\text{-orbits} \\ \text{of } V(\mathbb{Q})\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\mathrm{Sel}_2 J \text{ for all} \\ C \in \mathcal{F}\end{array}\right\}$$

2. Count integral orbits in (G, V).

Example

Elements of $\mathrm{Sel}_2 E$ (with $E/\mathbb{Q}$ elliptic curve) correspond to $\mathrm{PGL}_2(\mathbb{Q})$-orbits of binary quartic forms. [Reason: a double cover $C \to \mathbb{P}^1$ with $Jac(C) = E$ is defined by a binary quartic]

Question

Where does (G, V) come from?

Graded Lie algebras

Definition

A Lie algebra $\mathfrak{h}$ over a field k is *m-graded* if

$$\mathfrak{h} = \bigoplus_{i \in \mathbb{Z}/m\mathbb{Z}} \mathfrak{h}_i$$

where $[\mathfrak{h}_i, \mathfrak{h}_j] \subset \mathfrak{h}_{i+j}$ for all i, j.

A graded Lie algebra defines a representation

$\mathfrak{h} \curvearrowright \mathfrak{h}$ via the adjoint representation, so $\mathfrak{g} := \mathfrak{h}_0$ acts on $V := \mathfrak{h}_1$ via restriction.

If H is an algebraic group with $\mathrm{Lie} H = \mathfrak{h}$ and $G \subset H$ a closed subgroup with $\mathrm{Lie} G = \mathfrak{g}$, then similarly $G \curvearrowright V$ and (G, V) is called a **Vinberg representation**.

Graded Lie algebras

Observation (Gross)

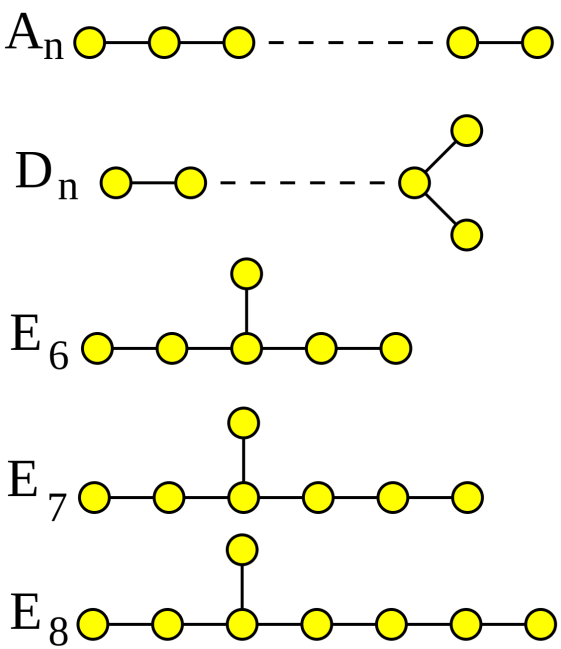
All representations appearing in the arithmetic statistics literature are Vinberg representations! (Apart from a few special cases)

Punchline of talk/"Main result"

We can use graded Lie algebras as a *starting point* to (re)prove theorems in arithmetic statistics.

Main results

Given an ADE Dynkin diagram, we can *canonically* construct a Vinberg representation and a family of curves (Thorne):



Main results

Explicit example: A_2

- $\mathfrak{h} = \mathfrak{sl}_3$, $H = \mathrm{PGL}_3$, $\theta\colon H \to H$, $g \mapsto (g^*)^{-1}$ where $(-)^*$ denotes reflection along anti-diagonal
- $G = H^\theta$, $V = \mathfrak{h}^{d\theta = -\mathrm{Id}}$ given by $(\mathrm{PGL}_2, \mathrm{Sym}^2(4))$.
- A_2 singularity is a cusp: $(y^2 = x^3) \rightsquigarrow \mathcal{F} = \{y^2 = x^3 + Ax + B \mid A, B \in \mathbb{Z}\}$.

We can find $\mathcal{F}$ inside V: elements of the form

$$\begin{pmatrix} x & 0 & 1 \\ y & -2x & 0 \\ w & z & x \end{pmatrix} \subset V$$

with characteristic polynomial $t^3 + At + B$ are described by the affine curve $(y^2 = x^3 + Ax + B)$

Main results

Theorem (L.)

Let $\mathcal{D} \neq A_1$ be an ADE Dynkin diagram, giving a representation (G, V) and family of curves $\mathcal{F}$. Then:

1. *For every $C \in \mathcal{F}$, there exists a 'natural' injection*

$$\mathrm{Sel}_2 J \hookrightarrow G(\mathbb{Q})\backslash V(\mathbb{Q}).$$

2. *When ordered by a suitable height, there exists an explicit $m \in \mathbb{Z}_{\geq 1}$ such that*

$$\mathit{Average}(\#\,\mathrm{Sel}_2(J)) \leq 3 \cdot 2^{m-1}.$$

Remarks

Previously known cases

- A_2: Bhargava–Shankar
- A_{2g}: Bhargava–Gross
- A_{2g+1}: Shankar–Wang
- D_{2g+1}: (Ananth) Shankar
- A_3, D_4: Bhargava–Ho.

The proofs of Theorems 1 and 2 are uniform.

Concrete consequence of E_6 case

Let

$$\mathcal{F} = \left\{ \begin{array}{c} \text{non-hyperelliptic genus 3 curves } C/\mathbb{Q} \\ \text{with a marked rational hyperflex } P \in C(\mathbb{Q}) \end{array} \right\}$$

Given by smooth members of the form

$$y^3 = x^4 + (p_2x^2 + p_5x + p_8)y + (p_6x^2 + p_9x + p_{12}),$$

Consequence 1

A majority ($> 61\%$) of curves in $\mathcal{F}$ have at most 26 rational points.

Consequence 2

A positive proportion of curves in $\mathcal{F}$ have only one rational point.

Proof of Theorem 1

1. Construct 'identity' $\kappa_C \in V(\mathbb{Q})$ for each $C \in \mathcal{F}$.
2. 'Twist' κ_C:

$$G(\mathbb{Q}) \setminus (V(\mathbb{Q}) \cap G(\bar{\mathbb{Q}}) \cdot \kappa_C) \leftrightarrow \ker(H^1(\mathbb{Q}, Stab_G(\kappa_C)) \to H^1(\mathbb{Q}, G))$$

3. Thorne: $Stab_G(\kappa_C) \simeq J[2]$ as Galois modules. So need to show composition

$$\mathrm{Sel}_2 J \hookrightarrow H^1(\mathbb{Q}, J[2]) \simeq H^1(\mathbb{Q}, Stab_G(\kappa_C)) \to H^1(\mathbb{Q}, G)$$

is trivial. In fact, suffices to show

$$J(k)/2J(k) \hookrightarrow H^1(k, J[2]) \to H^1(k, G)$$

is trivial for every field $k/\mathbb{Q}$.

Proof of Theorem 1

Consider 'universal' curve/Jacobian

$$\mathcal{C}, \mathcal{J} \to \mathbb{A}^n \setminus \{\text{discriminant}\}$$

Example

A_2 : then $\mathcal{C} = \mathcal{J} \subset \mathbb{P}^2 \times (\mathbb{A}^2 \setminus \{\Delta = 0\})$ is the universal Weierstrass equation $y^2z = x^3 + Axz^2 + Bz^3$.

$$J(k) \to H^1(k, J[2]) \simeq H^1(k, Stab_G(\kappa_C)) \to H^1(k, G)$$

Every $P \in J(k)$ gives a class $\alpha_P \in H^1(k, G)$.
There exists a G-torsor $\mathcal{T} \to \mathcal{J}$ interpolating all these classes.

Theorem

$\mathcal{T}$ is Zariski locally trivial.

Proof of Theorem 1

Theorem

$\mathcal{T}$ is Zariski locally trivial.

Two essential ingredients:

First ingredient: geometry of $\mathcal{J}$

The total space $\mathcal{J}$ is rational.

Proof: extend $\mathcal{J}$ to singular curves and get *compactified Jacobian*

$$\bar{\mathcal{J}} \to \mathbb{A}^n$$

BB decomposition $\rightsquigarrow \bar{\mathcal{J}}$ has an affine cell decomposition.

Example

A_2 case:

$$\bar{\mathcal{J}} \subset \mathbb{P}^2 \times \mathbb{A}^2$$

is a union $\mathbb{A}^3 \cup \mathbb{A}^2$

Proof of Theorem 1

Second ingredient: Generalities on torsors

Let $U \subset \mathbb{A}^N_{\mathbb{Q}}$ be an open with $\operatorname{codim}(\mathbb{A}^N \setminus U, \mathbb{A}^N) \geq 2$ and let $T \to U$ be a G-torsor. Suppose that T_x is trivial for some $x \in U(\mathbb{Q})$. Then T_y is trivial for every $y \in U(\mathbb{Q})$. (In fact, T is Zariski trivial.)

Similar to results of Colliot-Thelene, Sansuc.

Finishing touch:

Special case of Grothendieck–Serre conjecture

If $\mathcal{T} \to \mathcal{J}$ is generically trivial, then $\mathcal{T}$ is Zariski locally trivial.

Summary

Theorem

$\mathcal{T}$ is Zariski locally trivial.

Proof.

1. There exists an open $V \subset \mathcal{J}$ which is also an open in $\mathbb{A}^N$. (First ingredient)
2. The torsor $\mathcal{T}|_V \to V$ extends to one on $U \subset \mathbb{A}^N$ with $\mathrm{codim}(\mathbb{A}^N \setminus U, \mathbb{A}^N) \geq 2$.
3. $\mathcal{T}_x$ is trivial for some $x \in V(\mathbb{Q})$, since $2\mathcal{J}(\mathbb{Q}) \cap V \neq \emptyset$. (Using rationality of $\mathcal{J}$ and dominance of $\mathcal{J} \xrightarrow{\times 2} \mathcal{J}$)
4. Therefore $\mathcal{T}|_V$ is Zariski trivial. (Second ingredient)
5. We conclude $\mathcal{T}$ is Zariski trivial. (GS conjecture)

□

Thank you for your attention!