An Upper Bound for the Average Rank of Elliptic Curves over Global Function Fields, via 2-Selmer Groups

Niven Achenjang
MIT

January 4, 2024

Hilbert's 10th Problem

Question (Hilbert's 10th Problem 1900, H10)

Does there exist an algorithm which, given a polynomial $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, outputs whether or not $f = 0$ admits a solution over $\mathbb{Z}$?

Answer (Davis-Putnam-Robinson 1961 + Matiyasevich 1970)

No

Remark

In fact, Zhi-Wei Sun (2021) proved that the answer to H10 is 'No' even if one restricts to polynomials in at most 11 variables.

H10 over $\mathbb{Q}$

Question

Does there exist an algorithm which, given a polynomial $f(x_1, \dots, x_n) \in \mathbb{Q}[x_1, \dots, x_n]$, outputs whether or not $f = 0$ admits a solution over $\mathbb{Q}$?

Remark

The answer is 'Yes' if one restricts to polynomials in $n = 1$ variable. However, in general, the answer to this question is still unknown.

What about other small values of n?

A Motivating Question

Question

Does there exist an algorithm which, given a polynomial $f(x, y) \in \mathbb{Q}[x, y]$ in two variables, outputs all pairs $(a, b) \in \mathbb{Q}^2$ such that $f(a, b) = 0$?

Equivalently, is there an algorithm which, given a 'nice' **curve** $C/\mathbb{Q}$, outputs a description of $C(\mathbb{Q})$?

This is still too hard, but it becomes more tractable if we ask about statistical behavior instead.

Motivating Question

Given a class $\mathcal{C}$ of (isomorphism classes of) curves, can we determine the ***average size*** *of $C(\mathbb{Q})$, for $C \in \mathcal{C}$?*

Elliptic Curves

Recall

If F is a field, and E/F is an elliptic curve, then $E(F)$ is an abelian group.

Theorem (Mordell-Weil)

*Let K be a **global field** – i.e. a number field or the function field of a curve over a finite field – and let E/K be an elliptic curve. Then, the abelian group $E(K)$ is finitely generated.*

Defining Average Rank of Elliptic Curves

Fix a global field K (e.g. $\mathbb{Q}, \mathbb{F}_q(t)$, etc.) for the remainder of the talk.

Motivating Question

Let $\mathcal{E}$ denote the class of all elliptic curves E/K. Can we determine the average value of $\operatorname{rank} E(K)$, for $E \in \mathcal{E}$?

Defining Average Rank of Elliptic Curves

Fix a global field K (e.g. $\mathbb{Q}, \mathbb{F}_q(t)$, etc.) for the remainder of the talk.

Motivating Question

Let $\mathcal{E}$ denote the class of all elliptic curves E/K. Can we determine the average value of $\operatorname{rank} E(K)$*, for* $E \in \mathcal{E}$*?*

This "average" is defined via a two-step limiting process.

(1) Define a notion of the 'height' $\operatorname{ht}(E)$ of an elliptic curve E/K. This should be defined so that there are only **finitely many curves of bounded height**, up to isomorphism.

Example (somewhat imprecise)

Over $K = \mathbb{Q}$, every elliptic curve comes from an equation of the form $E\colon y^2 = x^3 + ax + b$, for some $a, b \in \mathbb{Z}$. In this case, we can take $\operatorname{ht}(E) := \max\{27b^2, 4|a|^3\}$.

Defining Average Rank of Elliptic Curves, continued

This "average" is defined via a two-step limiting process.

(1) Define an appropriate notion of the 'height' $\mathrm{ht}(E)$ of an elliptic curve E/K, designed so that there are only **finitely many curves of bounded height**, up to isomorphism.

Defining Average Rank of Elliptic Curves, continued

This "average" is defined via a two-step limiting process.

(1) Define an appropriate notion of the 'height' $\mathrm{ht}(E)$ of an elliptic curve E/K, designed so that there are only **finitely many curves of bounded height**, up to isomorphism.

(2) Define the average rank $\mathrm{AR}(K)$ as a limit of averages for curves of bounded height:

$$\mathrm{AR}_X(K) := \frac{\sum_{E\colon \mathrm{ht}(E)\leq X} \operatorname{rank} E(K)}{\sum_{E\colon \mathrm{ht}(E)\leq X} 1}$$

$$\mathrm{AR}(K) := \lim_{X\to\infty} \mathrm{AR}_X(K).$$

Selmer Groups

Motivating Question

Can we compute $\mathrm{AR}(K)$*, the average rank of elliptic curves* E/K*?*

As a first step, can one bound $\overline{\mathrm{AR}}(K) := \limsup_{X\to\infty} \mathrm{AR}_X(K)$? It is not a priori obvious that this is even finite.

The main new result presented in this talk will be a bound for this quantity when K is an arbitrary global function field.

Remark

While computing rank $E(K)$ can be difficult in general, there exists some standard tools for bounding this quantity. Of note are the **Selmer groups**.

Average Sizes of Selmer Groups

Given an elliptic curve E/K and an integer $n \geq 1$, one can define its n-**Selmer group** $\mathrm{Sel}_n(E)$. This is a finite $\mathbb{Z}/n\mathbb{Z}$-module whose main utility to us is that

$$n^{\mathrm{rank}_{\mathbb{Z}} E(K)} \leq \# \mathrm{Sel}_n(E).$$

Average Sizes of Selmer Groups

Given an elliptic curve E/K and an integer $n \geq 1$, one can define its n-**Selmer group** $\mathrm{Sel}_n(E)$. This is a finite $\mathbb{Z}/n\mathbb{Z}$-module whose main utility to us is that

$$n^{\mathrm{rank}_{\mathbb{Z}} E(K)} \leq \# \mathrm{Sel}_n(E).$$

We define the average sizes $\mathrm{AS}_n(K), \mathrm{AS}_{n,X}(K)$ in the same way as $\mathrm{AR}(K), \mathrm{AR}_X(K)$, respectively, but using $\# \mathrm{Sel}_n(E)$ in place of rank $E(K)$. We similarly define $\overline{\mathrm{AS}}_n(K) := \limsup_{X \to \infty} \mathrm{AS}_{n,X}(K)$.

Stating our Main Question

Motivating Question (Recall)

Can we compute $\mathrm{AR}(K)$, *the average rank of elliptic curves* E/K*?*

We suggested bounding $\overline{\mathrm{AR}}(K)$ as a first step, and introduced the Selmer groups as a tool to do so.

Question (Main question for this talk)

Can we compute $\mathrm{AS}_n(K)$ *for some* n*?*

Stating our Main Question

Motivating Question (Recall)

Can we compute $\mathrm{AR}(K)$*, the average rank of elliptic curves* E/K*?*

We suggested bounding $\overline{\mathrm{AR}}(K)$ as a first step, and introduced the Selmer groups as a tool to do so.

Question (Main question for this talk)

Can we compute $\mathrm{AS}_n(K)$ *for some* n*?*

Remark/Example ($n = 2$)

If $r = \operatorname{rank} E(K)$, then

$$2r \leq 2^r \leq \# \mathrm{Sel}_2(E).$$

Hence, $2 \cdot \overline{\mathrm{AR}}(K) \leq \overline{\mathrm{AS}}_2(K)$.

The Conjectures

Conjecture (Goldfeld 1979, folklore)

$\mathrm{AR}(K) = \frac{1}{2}$.

Conjecture (Bhargava–Shankar, Poonen–Rains)

For all $n \geq 1$, $\mathrm{AS}_n(K) = \sum_{d|n} d$. *For example,* $\mathrm{AS}_2(K) = 1 + 2 = 3$.

The Conjectures

Conjecture (Goldfeld 1979, folklore)

$\mathrm{AR}(K) = \frac{1}{2}$.

Conjecture (Bhargava–Shankar, Poonen–Rains)

For all $n \geq 1$, $\mathrm{AS}_n(K) = \sum_{d|n} d$. *For example,* $\mathrm{AS}_2(K) = 1 + 2 = 3$.

Remark

The latter conjecture implies that 100% of elliptic curves have rank 0 or 1.

Some Earlier Results

Theorem (Brumer, 1992)

If $K = \mathbb{F}_q(t)$ *and* $\mathrm{char}\,\mathbb{F}_q \neq 2, 3,$ *then* $\mathrm{AR}(K) \leq 2.3.$

Some Earlier Results

Theorem (Brumer, 1992)

If $K = \mathbb{F}_q(t)$ *and* $\operatorname{char}\mathbb{F}_q \neq 2, 3,$ *then* $\mathrm{AR}(K) \leq 2.3$.

Theorem (de Jong, 2002)

As q *ranges over prime powers,* $\limsup_{q\to\infty} \overline{\mathrm{AS}}_3(\mathbb{F}_q(t)) \leq 4$.

Consequently, $\limsup_{q\to\infty} \overline{\mathrm{AR}}(\mathbb{F}_q(t)) \leq 7/6$.[a]

[a] de Jong proves an upper bound of 3/2 in his paper, but Bhargava-Shankar show how to deduce 7/6 instead.

Some Earlier Results

Theorem (Brumer, 1992)

If $K = \mathbb{F}_q(t)$ *and* $\mathrm{char}\,\mathbb{F}_q \neq 2, 3$*, then* $\mathrm{AR}(K) \leq 2.3$*.*

Theorem (de Jong, 2002)

As q ranges over prime powers, $\limsup_{q\to\infty} \overline{\mathrm{AS}}_3(\mathbb{F}_q(t)) \leq 4$*.*

Consequently, $\limsup_{q\to\infty} \overline{\mathrm{AR}}(\mathbb{F}_q(t)) \leq 7/6$*.*[a]

[a] de Jong proves an upper bound of 3/2 in his paper, but Bhargava-Shankar show how to deduce 7/6 instead.

Theorem (Bhargava-Shankar, 2013)

Let $K = \mathbb{Q}$*. Then,* $\mathrm{AS}_n(\mathbb{Q}) = \sum_{d|n} d$ *if* $n = 1, 2, 3, 4, 5$*.*

Consequently, $\overline{\mathrm{AR}}(\mathbb{Q}) \leq 0.885$*.*

Some Variants in the function field setting

Working in the "large q limit," where one lets the size of the ground field go to infinity *before* letting the height go to infinity, Landesman has proven:

Theorem (Landesman, 2021)

For any $n \geq 1$ *and any* $X \geq 2$,

$$\lim_{\substack{q \to \infty \\ \gcd(q, 2n) = 1}} \mathrm{AS}_{n,X}(\mathbb{F}_q(t)) = \sum_{d \mid n} d.$$

Some Variants in the function field setting

Working in the "large q limit," where one lets the size of the ground field go to infinity *before* letting the height go to infinity, Landesman has proven:

Theorem (Landesman, 2021)

For any $n \geq 1$ and any $X \geq 2$,

$$\lim_{\substack{q \to \infty \\ \gcd(q, 2n)=1}} \mathrm{AS}_{n,X}(\mathbb{F}_q(t)) = \sum_{d \mid n} d.$$

Other known statements deal with

- the "distribution" of $\mathrm{Sel}_n(E)$ instead of just its average size; or
- quadratic twist families instead of all elliptic curves over K.

2-Selmer Over Function Fields

Theorem (Hồ–Lê Hùng–Ngô, 2014)

Let K be the function field of a nice curve $B/\mathbb{F}_q$. Assume that $\operatorname{char} \mathbb{F}_q \neq 2, 3$ *and that* $q > 64$. *Then,*

$$3\zeta_B(10)^{-1} \leq \overline{\mathrm{AS}}_2(K) \leq 3 + O_K\left(\frac{1}{q}\right),$$

as $q \to \infty$, *where* ζ_B *is the usual zeta function of* B.

2-Selmer Over Function Fields

Theorem (Hồ–Lê Hùng–Ngô, 2014)

Let K be the function field of a nice curve $B/\mathbb{F}_q$. Assume that $\operatorname{char}\mathbb{F}_q \neq 2, 3$ *and that* $q > 64$. *Then,*

$$3\zeta_B(10)^{-1} \leq \overline{\mathrm{AS}}_2(K) \leq 3 + O_K\left(\frac{1}{q}\right),$$

as $q \to \infty$, *where* ζ_B *is the usual zeta function of* B.

Theorem (A., 2023)

Let K be the function field of a nice curve $B/\mathbb{F}_q$. Then,

$$\overline{\mathrm{AS}}_2(K) \leq 1 + 2\zeta_B(2)\zeta_B(10) = 3 + \frac{2}{q} + O_K\left(\frac{1}{q^2}\right).$$

2-Selmer Over Function Fields

Theorem (Hồ–Lê Hùng–Ngô, 2014)

Let K be the function field of a nice curve $B/\mathbb{F}_q$. Assume that $\operatorname{char}\mathbb{F}_q \neq 2, 3$ *and that* $q > 64$. *Then,*

$$3\zeta_B(10)^{-1} \leq \overline{\mathrm{AS}}_2(K) \leq 3 + O_K\left(\frac{1}{q}\right),$$

as $q \to \infty$, *where* ζ_B *is the usual zeta function of* B.

Theorem (A., 2023)

Let K be the function field of a nice curve $B/\mathbb{F}_q$. Then,

$$\overline{\mathrm{AS}}_2(K) \leq 1 + 2\zeta_B(2)\zeta_B(10) = 3 + \frac{2}{q} + O_K\left(\frac{1}{q^2}\right).$$

Consequently, in either theorem, $\overline{\mathrm{AR}}(K) \leq 3/2 + O_K(1/q)$.

Geometric Interpretation of 2-Selmer elements

As before, let K be the function field of a nice curve $B/\mathbb{F}_q$.

Geometric Interpretation of 2-Selmer elements

As before, let K be the function field of a nice curve $B/\mathbb{F}_q$.

(1) Every $\alpha \in \mathrm{Sel}_2(E)$ can be represented by a pair (C, D), where C is a genus 1 curve with a simply transitive E-action and $D \subset C$ is an effective, degree 2 divisor.

Geometric Interpretation of 2-Selmer elements

As before, let K be the function field of a nice curve $B/\mathbb{F}_q$.

(1) Every $\alpha \in \mathrm{Sel}_2(E)$ can be represented by a pair (C, D), where C is a genus 1 curve with a simply transitive E-action and $D \subset C$ is an effective, degree 2 divisor.

(2) Such a pair (C, D) can always be written in the form

$$C\colon Y^2 + (a_0X^2 + a_1XZ + a_2Z^2)Y = c_0X^4 + c_1X^3Z + c_2X^2Z^2 + c_3XZ^3 + c_4Z^4$$

inside $\mathbb{P}(1,2,1)$ for some $a_i, c_j \in K$, with $D = \{Z = 0\}$.

Geometric Interpretation of 2-Selmer elements, continued

(3) Each (C, D) has an integral model $(\mathcal{C}, \mathcal{D})$, akin to the minimal Weierstrass model of an elliptic curve. The height of the elliptic curve attached to (C, D) can be extracted from $(\mathcal{C}, \mathcal{D})$. To count 2-Selmer elements, one counts integral models $(\mathcal{C}, \mathcal{D})$ instead.

Geometric Interpretation of 2-Selmer elements, continued

(3) Each (C, D) has an integral model $(\mathcal{C}, \mathcal{D})$, akin to the minimal Weierstrass model of an elliptic curve. The height of the elliptic curve attached to (C, D) can be extracted from $(\mathcal{C}, \mathcal{D})$. To count 2-Selmer elements, one counts integral models $(\mathcal{C}, \mathcal{D})$ instead.

(4) Each $(\mathcal{C}, \mathcal{D})$ can be embedded in some relative $\mathbb{P}(1, 2, 1)$-bundle over B, which I will call $\mathbb{P} = \mathbb{P}(\mathcal{C}, \mathcal{D})$. Given $\mathbb{P}$, $(\mathcal{C}, \mathcal{D})$ is determined by a choice of section of a certain rank 8 vector bundle on B. This bundle controls the variation of the coefficients of the equation cutting out $\mathcal{C} \hookrightarrow \mathbb{P}$, i.e. the variation of the a_i's and c_j's from last slide.

Geometric Interpretation of 2-Selmer elements, continued

(5) To count integral models $(\mathcal{C}, \mathcal{D})$, one can determine which rank 8 vector bundles can arise and count their sections.

Geometric Interpretation of 2-Selmer elements, continued

(5) To count integral models $(\mathcal{C}, \mathcal{D})$, one can determine which rank 8 vector bundles can arise and count their sections.

(6) In the end, one shows that the vector bundles which arise are "almost semistable" so that their number of sections is well-approximated by Riemann-Roch. Afterwards, the actual counting becomes more straightforward.

Summary

- One first constructs suitable integral models $(\mathcal{C}, \mathcal{D})$ of 2-Selmer elements.
- Then, one uses the algebraic geometry of vector bundles on curves to count the number of integral models $(\mathcal{C}, \mathcal{D})$.
- From this, one can obtain a general bound the average 2-Selmer group size for elliptic curves over **any** global function field K, removing restrictions on the underlying finite field previous authors had to impose.
- This then yields statistical information about the ranks of elliptic curves over K.