Bias and Rank in Families of Hyperelliptic Curves

Trajan Hammonds [1] Ben Logsdon [2]
Joint with Seoyoung Kim and Steven J. Miller

[1] Carnegie Mellon University

[2] Williams College

Young Mathematicians Conference, Ohio State University, August 2018

Elliptic Curves

An elliptic curve E is the set of solutions to (x, y) to an equation of the form

$$E \; : \; y^2 = x^3 + ax + b,$$

with $a, b \in \mathbb{Z}$.

Rank of Elliptic Curves

Mordell-Weil Theorem

The set of rational points on an elliptic curve $E(\mathbb{Q})$ forms a finitely generated abelian group and hence can be written as

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

We say r is the rank of the elliptic curve $E(\mathbb{Q})$.

Rank of Elliptic Curves

Mordell-Weil Theorem

The set of rational points on an elliptic curve $E(\mathbb{Q})$ forms a finitely generated abelian group and hence can be written as

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

We say r is the rank of the elliptic curve $E(\mathbb{Q})$.

- Noam Elkies found an elliptic curve with rank ≥ 28

Rank of Elliptic Curves

Mordell-Weil Theorem

The set of rational points on an elliptic curve $E(\mathbb{Q})$ forms a finitely generated abelian group and hence can be written as

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

We say r is the rank of the elliptic curve $E(\mathbb{Q})$.

- Noam Elkies found an elliptic curve with rank ≥ 28
- **Conjecture:** Rank is unbounded

Rank of Elliptic Curves

Mordell-Weil Theorem

The set of rational points on an elliptic curve $E(\mathbb{Q})$ forms a finitely generated abelian group and hence can be written as

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

We say r is the rank of the elliptic curve $E(\mathbb{Q})$.

- Noam Elkies found an elliptic curve with rank ≥ 28
- **Conjecture:** Rank is unbounded
- **Conjecture:** There are only finitely many curves with rank ≥ 21

Counting points over $\mathbb{F}_p$

Define $a_E(p)$ as

$$a_E(p) = p - \#\{(x, y) : y^2 = x^3 + ax + b \mod p\}$$
$$= p - \sum_{x=0}^{p-1} 1 + \left(\frac{x^3 + ax + b}{p}\right)$$
$$= -\sum_{x(p)} \left(\frac{x^3 + ax + b}{p}\right),$$

where the Legendre symbol $\left(\frac{\cdot}{p}\right)$ is defined by

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \equiv a^2 \mod p \\ 0 & \text{if } x \equiv 0 \mod p \\ -1 & \text{otherwise} \end{cases}$$

Families of Elliptic Curves

A one-parameter family of elliptic curves is given by

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T).$$

Families of Elliptic Curves

A one-parameter family of elliptic curves is given by

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T).$$

Specializing $T \to t$ yields an elliptic curve over $\mathbb{Q}$.

Families of Elliptic Curves

A one-parameter family of elliptic curves is given by

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T).$$

Specializing $T \to t$ yields an elliptic curve over $\mathbb{Q}$.

Silverman's Specialization Theorem

For most t, $\mathrm{rank}\ \mathcal{E}_t \geq \mathrm{rank}\ \mathcal{E}$.

Nagao's Conjecture

Consider a family $\mathcal{E} : y^2 = f(x, T)$.

Nagao's Conjecture

Consider a family $\mathcal{E} : y^2 = f(x, T)$. Define its m-th moment

$$A_{m,\mathcal{E}}(p) = \sum_{t(p)} a_E(p)^m.$$

Consider a family $\mathcal{E} : y^2 = f(x, T)$. Define its m-th moment

$$A_{m,\mathcal{E}}(p) = \sum_{t(p)} a_E(p)^m.$$

Nagao's Conjecture

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} \frac{\log p}{p}(-A_{1,\mathcal{E}}(p)) = \text{rank } (\mathcal{E}(\mathbb{Q}(\text{T}))).$$

Nagao's Conjecture

Consider a family $\mathcal{E} : y^2 = f(x, T)$. Define its m-th moment

$$A_{m,\mathcal{E}}(p) = \sum_{t(p)} a_E(p)^m.$$

Nagao's Conjecture

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} \frac{\log p}{p}(-A_{1,\mathcal{E}}(p)) = \mathrm{rank}\ \left(\mathcal{E}(\mathbb{Q}(\mathrm{T}))\right).$$

If $A_{1,\mathcal{E}} = -rp$, then it follows from the prime number theorem that $\mathrm{rank}\ \mathcal{E}\left(\mathbb{Q}(\mathrm{T})\right) = \mathrm{r}$.

Hyperelliptic Curves

- A hyperelliptic curve with genus $g \geq 2$ is a curve of the form
$$\chi : y^2 = f(x),$$
where $f(x)$ is a degree $2g+1$ polynomial.

Hyperelliptic Curves

- A hyperelliptic curve with genus $g \geq 2$ is a curve of the form
$$\chi : y^2 = f(x),$$
where $f(x)$ is a degree $2g + 1$ polynomial.
- The set of rational points of a hyperelliptic curve is finite, due to Falting's theorem, so there is no rank.

- A hyperelliptic curve with genus $g \geq 2$ is a curve of the form
$$\chi : y^2 = f(x),$$
where $f(x)$ is a degree $2g+1$ polynomial.
- The set of rational points of a hyperelliptic curve is finite, due to Falting's theorem, so there is no rank.
- Instead we consider the rank of the Jacobian variety J_χ, which is a Mordell-Weil group.

Hyperelliptic Curves

- A hyperelliptic curve with genus $g \geq 2$ is a curve of the form
$$\chi : y^2 = f(x),$$
where $f(x)$ is a degree $2g+1$ polynomial.
- The set of rational points of a hyperelliptic curve is finite, due to Falting's theorem, so there is no rank.
- Instead we consider the rank of the Jacobian variety J_χ, which is a Mordell-Weil group.
- A one-parameter family of hyperelliptic curves is given by
$$y^2 = x^{2g+1} + A_{2g}(T)x^{2g} + \cdots + A_1(T)x + A_0(T) = f(x, T).$$

Generalized Nagao's conjecture

In the hyperelliptic curve case we still may write

$$a_\chi(p) = -\sum_{x(p)} \left(\frac{f(x,T)}{p} \right),$$

and also its first moment

$$A_{1,\chi}(p) = \sum_{t(p)} a_\chi(p).$$

Generalized Nagao's conjecture

In the hyperelliptic curve case we still may write

$$a_\chi(p) = -\sum_{x(p)} \left(\frac{f(x,T)}{p} \right),$$

and also its first moment

$$A_{1,\chi}(p) = \sum_{t(p)} a_\chi(p).$$

Generalized Nagao's Conjecture

$$\lim_{X\to\infty} \sum_{p\leq X} -\frac{1}{p} A_{1,\chi}(p) \log(p) = \mathrm{rank}\ \mathrm{J}_\chi\left(\mathbb{Q}(\mathrm{T})\right).$$

In the hyperelliptic curve case we still may write

$$a_\chi(p) = -\sum_{x(p)} \left(\frac{f(x,T)}{p}\right),$$

and also its first moment

$$A_{1,\chi}(p) = \sum_{t(p)} a_\chi(p).$$

Generalized Nagao's Conjecture

$$\lim_{X\to\infty} \sum_{p\le X} -\frac{1}{p} A_{1,\chi}(p)\log(p) = \mathrm{rank}\ \mathrm{J}_\chi\left(\mathbb{Q}(\mathrm{T})\right).$$

Goal: Construct families of hyperelliptic curves with high rank.

Hyperelliptic curves with moderate rank

Calculations

For a family $\chi : y^2 = f(x, T)$, we can write

$$a_{\chi,t}(p) = -\sum_{x(p)} \left(\frac{f(x, T)}{p} \right),$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol mod p with

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \equiv a^2 \bmod p \text{ for some } a \neq 0 \\ 0 & \text{if } x \equiv 0 \bmod p \\ -1 & \text{otherwise} \end{cases}$$

Linear and Quadratic Legendre Sums

$$\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0 \text{ if } p \nmid a$$

$$\sum_{t \bmod p} \left(\frac{at^2+bt+c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2-4ac \\ -\left(\frac{a}{p}\right) & \text{if } p \nmid b^2-4ac. \end{cases}$$

Conjecture Theorem

Let $\chi : y^2 = f(x, T)$ be a genus g curve satisfying

$$y^2 = f(x, T) = x^{2g+1}T^2 + 2g(x)T - h(x)$$

$$g(x) = x^{2g+1} + \sum_{i=0}^{2g} a_i x^i$$

$$h(x) = (A-1)x^{2g+1} + \sum_{i=0}^{2g} A_i x^i.$$

Now we can calculate the discriminant $D_T(x) := g(x)^2 + x^{2g+1}h(x)$ of the quadratic polynomial $f(x, T)$ in T.

Conjecture (HLKM, 2018)

Let χ be defined as in the previous slide. Then

$$\mathrm{rank}\ \mathrm{J}_{\chi}\left(\mathbb{Q}(\mathrm{T})\right) = 4\mathrm{g} + 2.$$

Conjecture Theorem

Conjecture (HLKM, 2018)

Let χ be defined as in the previous slide. Then

$$\mathrm{rank}\ \mathrm{J}_{\chi}\left(\mathbb{Q}(\mathrm{T})\right) = 4\mathrm{g} + 2.$$

Theorem (HLKM, 2018)

The above conjecture is true for $g = 2$ and $g = 3$.

Conjecture (HLKM, 2018)

Let χ be defined as in the previous slide. Then

$$\mathrm{rank}\, \mathrm{J}_\chi\left(\mathbb{Q}(\mathrm{T})\right) = 4\mathrm{g} + 2.$$

Theorem (HLKM, 2018)

The above conjecture is true for $g = 2$ and $g = 3$.

This work generalizes a result of Arms, Lozano-Robledo, and Miller who constructed a family of elliptic curves with rank 6. Indeed, for the elliptic curve, $g = 1$ and surely $6 = 4 \cdot 1 + 2$.

Construction

Key Idea

Make the roots of $D_t(x)$ distinct nonzero perfect squares.

- Choose roots ρ_i^2 of $D_t(x)$ so that

$$D_t(x) = A \prod_{i=1}^{4g+2} \left(x - \rho_i^2\right)$$

Construction

Key Idea

Make the roots of $D_t(x)$ distinct nonzero perfect squares.

- Choose roots ρ_i^2 of $D_t(x)$ so that

$$D_t(x) = A \prod_{i=1}^{4g+2} \left(x - \rho_i^2\right)$$

- Equate coefficients in

$$D_t(x) = A \prod_{i=1}^{4g+2} \left(x - \rho_i^2\right) = g(x)^2 + x^{2g+1} h(x).$$

Construction

Key Idea

Make the roots of $D_t(x)$ distinct nonzero perfect squares.

- Choose roots ρ_i^2 of $D_t(x)$ so that

$$D_t(x) = A \prod_{i=1}^{4g+2} (x - \rho_i^2)$$

- Equate coefficients in

$$D_t(x) = A \prod_{i=1}^{4g+2} (x - \rho_i^2) = g(x)^2 + x^{2g+1} h(x).$$

- Solve the nonlinear system for a_i, A_i.

Sketch of the proof

$$
\begin{aligned}
-A_{1,\chi}(p) &= \sum_{t(p)} a_{\chi_t}(p) = \sum_{t \bmod p} \sum_{x \bmod p} \left(\frac{f(x,T)}{p} \right) \\
&= \sum_{x \bmod p} \sum_{t \bmod p} \left(\frac{x^{2g+1}T^2 + 2g(x)T - h(x)}{p} \right) \\
&= \sum_{\substack{x \bmod p \\ D_t(x) \equiv 0}} (p-1) \left(\frac{x^{2g+1}}{p} \right) - \sum_{\substack{x \bmod p \\ D_t(x) \not\equiv 0}} \left(\frac{x^{2g+1}}{p} \right) \\
&= p \sum_{\substack{x \bmod p \\ D_t(x) \equiv 0}} \left(\frac{x^{2g+1}}{p} \right) - \sum_{x \bmod p} \left(\frac{x^{2g+1}}{p} \right) \\
&= p\,(\#\text{ of perfect-square roots of } D_t(x)) = p\,(4g+2)\,.
\end{aligned}
$$

Bias Conjectures

Michel's Theorem

For one-parameter families of elliptic curves $\mathcal{E}$, the second moment $A_{2,\mathcal{E}}(p)$ is

$$A_{2,\mathcal{E}}(p) = p^2 + O\left(p^{3/2}\right).$$

Michel's Theorem

For one-parameter families of elliptic curves $\mathcal{E}$, the second moment $A_{2,\mathcal{E}}(p)$ is

$$A_{2,\mathcal{E}}(p) = p^2 + O\left(p^{3/2}\right).$$

Upon examining the lower order terms $p^{3/2}$, p, $p^{1/2}$ and 1 Miller et.al formed the following conjecture:

Bias Conjecture

The largest lower order term in the second moment expansion that does not average to 0 is on average **negative**.

Evidence

In every family of hyperelliptic curves we have studied, both Michel's Theorem and the Bias conjecture appear to hold. Namely, the following families:

- $\chi : y^2 = x^5 + x + T$, $A_{2,\chi}(p) = pN_p - p^2$
- $\chi : y^2 = x^5 + xT$, $A_{2,\chi}(p) = 4p^2 - 4p$ if $p \equiv 1 \mod 8$
- $\chi : y^2 = x^{2g+1} + T^k$,
  $A_{2,\chi}(p) = (\gcd(p-1, 2g+1) - 1)(p^2 - p)$
- $\chi : y^2 = x^{2g+1} + x^k T$

We thank our advisors Steven J. Miller and Seoyoung Kim, Williams College, the SMALL REU and the National Science Foundation (grant DMS-1659037).