Rank and Bias in Families of Hyperelliptic Curves

Trajan Hammonds [1] Ben Logsdon [2]
thammond@andrew.cmu.edu bcl5@williams.edu
Joint with Seoyoung Kim [3] and Steven J. Miller [2]

[1]Carnegie Mellon University [2]Williams College [3]Brown University

Québec-Maine Number Theory Conference
Université Laval, October 2018

Hyperelliptic Curves

Define a hyperelliptic curve of genus g over $\mathbb{Q}(T)$:

$$\mathcal{X} : y^2 = f(x, T) = x^{2g+1} + A_{2g}(T)x^{2g} + \cdots + A_1(T)x + A_0(T).$$

Hyperelliptic Curves

Define a hyperelliptic curve of genus g over $\mathbb{Q}(T)$:

$$\mathcal{X} : y^2 = f(x, T) = x^{2g+1} + A_{2g}(T)x^{2g} + \cdots + A_1(T)x + A_0(T).$$

Let $a_{\mathcal{X}}(p) = p + 1 - \#\mathcal{X}(\mathbb{F}_p)$. Then

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

Hyperelliptic Curves

Define a hyperelliptic curve of genus g over $\mathbb{Q}(T)$:

$$\mathcal{X} : y^2 = f(x,T) = x^{2g+1} + A_{2g}(T)x^{2g} + \cdots + A_1(T)x + A_0(T).$$

Let $a_{\mathcal{X}}(p) = p + 1 - \#\mathcal{X}(\mathbb{F}_p)$. Then

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

and its m-th power sum

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

Generalized Nagao's conjecture

Generalized Nagao's Conjecture

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

Generalized Nagao's conjecture

Generalized Nagao's Conjecture

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

Goal: Construct families of hyperelliptic curves with high rank.

Hyperelliptic curves with moderately large rank over $\mathbb{Q}(T)$

Moderate-Rank Family

Theorem (HLKM, 2018)

Assume the Generalized Nagao Conjecture and trivial Chow trace Jacobian. For any $g \geq 1$, we can construct infinitely many genus g hyperelliptic curves $\mathcal{X}$ over $\mathbb{Q}(T)$ such that

$$\text{rank } J_{\mathcal{X}}(\mathbb{Q}(T)) = 4g + 2.$$

Moderate-Rank Family

Theorem (HLKM, 2018)

Assume the Generalized Nagao Conjecture and trivial Chow trace Jacobian. For any $g \geq 1$, we can construct infinitely many genus g hyperelliptic curves $\mathcal{X}$ over $\mathbb{Q}(T)$ such that

$$\mathrm{rank}\ J_{\mathcal{X}}(\mathbb{Q}(T)) = 4g + 2.$$

- Close to current record of $4g + 7$.

Moderate-Rank Family

Theorem (HLKM, 2018)

Assume the Generalized Nagao Conjecture and trivial Chow trace Jacobian. For any $g \geq 1$, we can construct infinitely many genus g hyperelliptic curves $\mathcal{X}$ over $\mathbb{Q}(T)$ such that

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

- Close to current record of $4g + 7$.
- No height matrix or basis computation.

Moderate-Rank Family

Theorem (HLKM, 2018)

Assume the Generalized Nagao Conjecture and trivial Chow trace Jacobian. For any $g \geq 1$, we can construct infinitely many genus g hyperelliptic curves $\mathcal{X}$ over $\mathbb{Q}(T)$ such that

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

- Close to current record of $4g + 7$.
- No height matrix or basis computation.

This generalizes a construction of Arms, Lozano-Robledo, and Miller in the elliptic surface case.

Idea of Construction

Define a genus g curve

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

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

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

The discriminant of the quadratic polynomial is

$$D_T(x) := g(x)^2 + x^{2g+1}h(x).$$

Idea of Construction

$$-A_{1,\mathcal{X}}(p) = \sum_{t(p)} \sum_{x(p)} \left(\frac{f(x,t)}{p} \right)$$

Idea of Construction

$$-A_{1,\mathcal{X}}(p) = \sum_{t(p)} \sum_{x(p)} \left(\frac{f(x,t)}{p}\right)$$

$$= \sum_{\substack{x(p) \\ D_t(x)\equiv 0}} (p-1) \left(\frac{x^{2g+1}}{p}\right) + \sum_{\substack{x(p) \\ D_t(x)\not\equiv 0}} (-1) \left(\frac{x^{2g+1}}{p}\right)$$

Idea of Construction

$$-A_{1,\mathcal{X}}(p) = \sum_{t(p)} \sum_{x(p)} \left(\frac{f(x,t)}{p}\right)$$

$$= \sum_{\substack{x(p) \\ D_t(x) \equiv 0}} (p-1) \left(\frac{x^{2g+1}}{p}\right) + \sum_{\substack{x(p) \\ D_t(x) \not\equiv 0}} (-1) \left(\frac{x^{2g+1}}{p}\right)$$

$$= \sum_{\substack{x(p) \\ D_t(x) \equiv 0}} p \left(\frac{x}{p}\right) - \sum_{x(p)} \left(\frac{x}{p}\right)$$

Idea of Construction

$$-A_{1,\mathcal{X}}(p) = \sum_{t(p)} \sum_{x(p)} \left(\frac{f(x,t)}{p}\right)$$

$$= \sum_{\substack{x(p) \\ D_t(x)\equiv 0}} (p-1)\left(\frac{x^{2g+1}}{p}\right) + \sum_{\substack{x(p) \\ D_t(x)\not\equiv 0}} (-1)\left(\frac{x^{2g+1}}{p}\right)$$

$$= \sum_{\substack{x(p) \\ D_t(x)\equiv 0}} p\left(\frac{x}{p}\right)$$

Idea of Construction

$$
\begin{aligned}
-A_{1,\mathcal{X}}(p) &= \sum_{t(p)} \sum_{x(p)} \left(\frac{f(x,t)}{p}\right) \\
&= \sum_{\substack{x(p) \\ D_t(x)\equiv 0}} (p-1) \left(\frac{x^{2g+1}}{p}\right) + \sum_{\substack{x(p) \\ D_t(x)\not\equiv 0}} (-1) \left(\frac{x^{2g+1}}{p}\right) \\
&= \sum_{\substack{x(p) \\ D_t(x)\equiv 0}} p \left(\frac{x}{p}\right)
\end{aligned}
$$

Therefore, $-A_{1,\mathcal{X}}(p)$ is $p\left(\frac{x}{p}\right)$ summed over the roots of $D_t(x)$.

Idea of Construction

$$-A_{1,\mathcal{X}}(p) = \sum_{t(p)} \sum_{x(p)} \left(\frac{f(x,t)}{p}\right)$$

$$= \sum_{\substack{x(p) \\ D_t(x)\equiv 0}} (p-1)\left(\frac{x^{2g+1}}{p}\right) + \sum_{\substack{x(p) \\ D_t(x)\not\equiv 0}} (-1)\left(\frac{x^{2g+1}}{p}\right)$$

$$= \sum_{\substack{x(p) \\ D_t(x)\equiv 0}} p\left(\frac{x}{p}\right)$$

Therefore, $-A_{1,\mathcal{X}}(p)$ is $p\left(\frac{x}{p}\right)$ summed over the roots of $D_t(x)$. To maximize the sum, we make each x a perfect square.

Idea of 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

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

Idea of 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

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

Idea of 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

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

- Solve the nonlinear system for the coefficients of g, h.

Idea of the Construction

$$-A_{1,\chi}(p)$$

Idea of the Construction

$$-A_{1,\chi}(p) = p \sum_{\substack{x \bmod p \\ D_t(x) \equiv 0}} \left(\frac{x^{2g+1}}{p}\right)$$

Idea of the Construction

$$-A_{1,\chi}(p) = p \sum_{\substack{x \bmod p \\ D_t(x) \equiv 0}} \left(\frac{x^{2g+1}}{p}\right)$$
$$= p \cdot (\text{\# of perfect-square roots of } D_t(x))$$
$$= p \cdot (4g+2)\,.$$

Idea of the Construction

$$-A_{1,\chi}(p) = p \sum_{\substack{x \mod p \\ D_t(x) \equiv 0}} \left(\frac{x^{2g+1}}{p}\right)$$
$$= p \cdot (\text{\# of perfect-square roots of } D_t(x))$$
$$= p \cdot (4g+2)\,.$$

Then by the Generalized Nagao Conjecture

$$\lim_{X \to \infty} \frac{1}{X} \sum_{p \le X} \frac{1}{p} \cdot p \cdot (4g+2) \log p = 4g+2 = \operatorname{rank} J_{\mathcal{X}}(\mathbb{Q}(T))\,.$$

Future Work

- Find a linearly independent basis.
- Generalizing another technique in Arms, Lozano-Robledo, and Miller.

Bias Conjecture

Bias Conjecture

Michel's Theorem

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

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

Bias Conjecture

Michel's Theorem

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

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

Bias Conjecture (Miller)

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

Bias Conjecture

Michel's Theorem

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

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

Bias Conjecture (Miller)

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

Goal: Find as many hyperelliptic families with as much bias as possible.

The Bias Family

Theorem (HLKM 2018)

Consider $\mathcal{X} : y^2 = x^n + x^h T^k$. If $\gcd(k, n-h, p-1) = 1$, then

$$A_{2,\mathcal{X}}(p) = \begin{cases} (\gcd(n-h, p-1) - 1)(p^2 - p) & h \text{ even} \\ \gcd(n-h, p-1)(p^2 - p) & h \text{ odd } (-) \\ 0 & \text{otherwise} \end{cases}$$

Calculations Part 1: *k*-Periodicity

$$A_{2,\mathcal{X}}(p) = \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)$$

Calculations Part 1: *k*-Periodicity

$$A_{2,\mathcal{X}}(p) = \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)$$

$$= \sum_{t,x,y(p)} \left(\frac{(t^{-n}x^n) + (t^{-h}x^h)t^k}{p}\right)\left(\frac{(t^{-n}y^n) + (t^{-h}y^h)t^k}{p}\right)$$

Calculations Part 1: *k*-Periodicity

$$
\begin{aligned}
A_{2,\mathcal{X}}(p) &= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right) \\
&= \sum_{t,x,y(p)} \left(\frac{(t^{-n}x^n) + (t^{-h}x^h)t^k}{p}\right)\left(\frac{(t^{-n}y^n) + (t^{-h}y^h)t^k}{p}\right) \\
&= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^{(k+(n-h))}}{p}\right)\left(\frac{y^n + y^h t^{(k+(n-h))}}{p}\right)
\end{aligned}
$$

Calculations Part 1: *k*-Periodicity

$$A_{2,\mathcal{X}}(p) = \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)$$

$$= \sum_{t,x,y(p)} \left(\frac{(t^{-n}x^n) + (t^{-h}x^h)t^k}{p}\right)\left(\frac{(t^{-n}y^n) + (t^{-h}y^h)t^k}{p}\right)$$

$$= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^{(k+(n-h))}}{p}\right)\left(\frac{y^n + y^h t^{(k+(n-h))}}{p}\right)$$

The second moment is periodic in k with period $(n-h)$.

Calculations Part 2

$$A_{2,\mathcal{X}}(p) = \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)$$

Calculations Part 2

$$A_{2,\mathcal{X}}(p) = \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)$$

$$= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^{m}}{p}\right)\left(\frac{y^n + y^h t^{m}}{p}\right) \quad (m \equiv_{n-h} k)$$

Calculations Part 2

$$
\begin{aligned}
A_{2,\mathcal{X}}(p) &= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right) \\
&= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^{m}}{p}\right)\left(\frac{y^n + y^h t^{m}}{p}\right) \qquad (m \equiv_{n-h} k) \\
&= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t}{p}\right)\left(\frac{y^n + y^h t}{p}\right) \qquad \text{(Frobenius)}
\end{aligned}
$$

Calculations Part 2

$$A_{2,\mathcal{X}}(p) = \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)$$

$$= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^{m}}{p}\right)\left(\frac{y^n + y^h t^{m}}{p}\right) \quad (m \equiv_{n-h} k)$$

$$= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t}{p}\right)\left(\frac{y^n + y^h t}{p}\right) \quad \text{(Frobenius)}$$

$$\gcd(n-h, k, p-1) = 1$$

Calculations Part 2

$$\begin{aligned} A_{2,\mathcal{X}}(p) &= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right) \\ &= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t^m}{p}\right)\left(\frac{y^n + y^h t^m}{p}\right) \quad (m \equiv_{n-h} k) \\ &= \sum_{t,x,y(p)} \left(\frac{x^n + x^h t}{p}\right)\left(\frac{y^n + y^h t}{p}\right) \quad \text{(Frobenius)} \end{aligned}$$

$$\gcd(n-h, k, p-1) = 1$$

Thus, this reduces to calculating the second moment of $y^2 = x^n + x^h T$, which is straightforward.

We thank our advisors Steven J. Miller and Seoyoung Kim, Williams College, the Finnerty Fund, the SMALL REU and the National Science Foundation (grants DMS-1659037 and DMS-1561945).