Rank and Bias in Families of Curves via Nagao's Conjecture

Trajan Hammonds and Steven J Miller
CMU and CMU & Williams College

sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu
http://www.williams.edu/Mathematics/sjmiller
Joint with Scott Arms, Seoyoung Kim, Ben Logsdon and Alvaro Lozano-Robledo

33rd Automorphic Forms Workshop, March 8, 2019

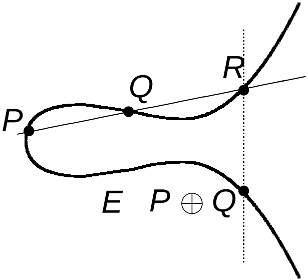
Outline

- Review Basics of Elliptic Curves.
- Describe Construction of Moderate Rank Families.
- Discuss Applications.
- Explore Generalizations.

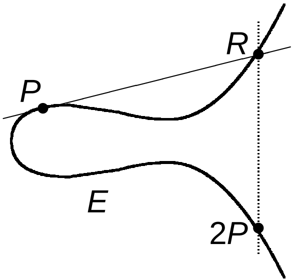
Introduction

Elliptic Curves: Mordell-Weil Group

Elliptic curve $y^2 = x^3 + ax + b$ with rational solutions $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and connecting line $y = mx + b$.



Addition of distinct points P and Q



Adding a point P to itself

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

Elliptic curve L-function

$E : y^2 = x^3 + ax + b$, associate L-function

$$L(s, E) = \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} = \prod_{p \text{ prime}} L_E(p^{-s}),$$

where

$$a_E(p) = p - \#\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 : y^2 \equiv x^3 + ax + b \bmod p\}.$$

Elliptic curve L-function

$E : y^2 = x^3 + ax + b$, associate L-function

$$L(s,E) = \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} = \prod_{p \text{ prime}} L_E(p^{-s}),$$

where

$$a_E(p) = p - \#\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 : y^2 \equiv x^3 + ax + b \bmod p\}.$$

Birch and Swinnerton-Dyer Conjecture

Rank of group of rational solutions equals order of vanishing of $L(s,E)$ at $s = 1/2$.

Theorem: Preliminaries

Consider a one-parameter family

$$\mathcal{E} : y^2 + a_1(T)xy + a_3(T)y \ = \ x^3 + a_2(T)x^2 + a_4(T)x + a_6(T).$$

Let $a_t(p) = p + 1 - N_p$, where N_p is the number of solutions mod p (including ∞). Define

$$A_{\mathcal{E}}(p) \ := \ \frac{1}{p} \sum_{t(p)} a_t(p).$$

$A_{\mathcal{E}}(p)$ is bounded independent of p (Deligne).

Methods for Obtaining Explicit Formulas

For a family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$, we can write

$$a_{\mathcal{E}(t)}(p) = -\sum_{x \bmod p} \left(\frac{x^3 + A(t)x + B(t)}{p} \right)$$

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

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a non-zero square modulo } p \\ 0 & \text{if } x \equiv 0 \bmod p \\ -1 & \text{otherwise.} \end{cases}$$

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

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

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

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

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

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

Average Values of Legendre Symbols

The value of $\left(\frac{x}{p}\right)$ for $x \in \mathbb{Z}$, when averaged over all primes p, is 1 if x is a non-zero square, and 0 otherwise.

Tate's Conjecture

Tate's Conjecture for Elliptic Surfaces

Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\text{ét}}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies

$$-\mathrm{ord}_{s=2}L_2(\mathcal{E}, s) \ = \ \mathrm{rank}\ NS(\mathcal{E}/\mathbb{Q}),$$

where $NS(\mathcal{E}/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $\mathcal{E}$. Further, $L_2(\mathcal{E}, s)$ does not vanish on the line $\mathrm{Re}(s) = 2$.

Theorem: Preliminaries

Theorem

Rosen-Silverman (Conjecture of Nagao): For an elliptic surface (a one-parameter family), assume Tate's conjecture. Then

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

Tate's conjecture is known for rational surfaces: An elliptic surface $y^2 = x^3 + A(T)x + B(T)$ is rational iff one of the following is true:

- $0 < \max\{3\deg A, 2\deg B\} < 12$;
- $3\deg A = 2\deg B = 12$ and $\mathrm{ord}_{T=0} T^{12}\Delta(T^{-1}) = 0$.

Small Rank

Moderate Rank

Rank 6 Family

Rational Surface of Rank 6 over $\mathbb{Q}(T)$:

$$\begin{aligned} y^2 &= x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x \\ &\quad + (2cT - D)(T^2 + 2T - A + 1)^2 \end{aligned}$$

$$\begin{aligned} A &= 8,916,100,448,256,000,000 \\ B &= -811,365,140,824,616,222,208 \\ C &= 26,497,490,347,321,493,520,384 \\ D &= -343,107,594,345,448,813,363,200 \\ a &= 16,660,111,104 \\ b &= -1,603,174,809,600 \\ c &= 2,149,908,480,000 \end{aligned}$$

Constructing Rank 6 Family

Idea: can explicitly evaluate linear and quadratic Legendre sums.

Use: a and b are not both zero mod p and $p > 2$, then for $t \in \mathbb{Z}$

$$\sum_{t=0}^{p-1} \left(\frac{at^2+bt+c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p|(b^2-4ac) \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases}$$

Thus if $p|(b^2-4ac)$, the summands are $\left(\frac{a(t-t')^2}{p}\right) = \left(\frac{a}{p}\right)$, and the t-sum is large.

Constructing Rank 6 Family

$$\begin{aligned} y^2 = f(x,T) &= x^3T^2 + 2g(x)T - h(x) \\ g(x) &= x^3 + ax^2 + bx + c, \; c \neq 0 \\ h(x) &= (A-1)x^3 + Bx^2 + Cx + D \\ D_T(x) &= g(x)^2 + x^3h(x). \end{aligned}$$

$D_T(x)$ is one-fourth of the discriminant of the quadratic (in T) polynomial $f(x,T)$.

$\mathcal{E}$ not in standard form, as the coefficient of x^3 is T^2, harmless. As $y^2 = f(x,T)$, for the fiber at $T = t$:

$$a_t(p) = -\sum_{x(p)} \left(\frac{f(x,t)}{p}\right) = -\sum_{x(p)} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right).$$

Constructing Rank 6 Family

We study $-pA_{\mathcal{E}}(p) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right)$.
When $x \equiv 0$ the t-sum vanishes if $c \not\equiv 0$, as it is just $\sum_{t=0}^{p-1}\left(\frac{2ct-D}{p}\right)$.

Assume now $x \not\equiv 0$. By the lemma on Quadratic Legendre Sums

$$\sum_{t=0}^{p-1}\left(\frac{x^3t^2+2g(x)t-h(x)}{p}\right) = \begin{cases}(p-1)\left(\frac{x^3}{p}\right) & \text{if } p \mid D_t(x) \\ -\left(\frac{x^3}{p}\right) & \text{otherwise.}\end{cases}$$

Goal:find coefficients a, b, c, A, B, C, D so that $D_t(x)$ has six distinct, non-zero roots that are squares.

Constructing Rank 6 Family

Assume we can find such coefficients. Then

$$\begin{aligned}
-pA_{\mathcal{E}}(p) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3t^2+2g(x)t-h(x)}{p}\right) \\
&= \sum_{x=0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) + \sum_{x:D_t(x)\equiv 0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) \\
&\quad + \sum_{x:xD_t(x)\not\equiv 0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) \\
&= 0 + 6(p-1) - \sum_{x:xD_t(x)\not\equiv 0}\left(\frac{x^3}{p}\right) = 6p.
\end{aligned}$$

Constructing Rank 6 Family

We must find $a, \dots, D$ such that $D_t(x)$ has six distinct, non-zero roots ρ_i^2:

$$\begin{aligned} D_t(x) &= g(x)^2 + x^3 h(x) \\ &= Ax^6 + (B+2a)x^5 + (C+a^2+2b)x^4 \\ &\quad + (D+2ab+2c)x^3 \\ &\quad + (2ac+b^2)x^2 + (2bc)x + c^2 \\ &= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0) \\ &= A(x-\rho_1^2)(x-\rho_2^2)(x-\rho_3^2)(x-\rho_4^2)(x-\rho_5^2)(x-\rho_6^2). \end{aligned}$$

Constructing Rank 6 Family

Because of the freedom to choose B, C, D there is no problem matching coefficients for the x^5, x^4, x^3 terms. We must simultaneously solve in integers

$$\begin{aligned} 2ac + b^2 &= R_2 A \\ 2bc &= R_1 A \\ c^2 &= R_0 A. \end{aligned}$$

For simplicity, take $A = 64R_0^3$. Then

$$\begin{array}{rclcrcl} c^2 &=& 64R_0^4 & \longrightarrow & c &=& 8R_0^2 \\ 2bc &=& 64R_0^3 R_1 & \longrightarrow & b &=& 4R_0R_1 \\ 2ac + b^2 &=& 64R_0^3 R_2 & \longrightarrow & a &=& 4R_0R_2 - R_1^2. \end{array}$$

Constructing Rank 6 Family

For an explicit example, take $r_i = \rho_i^2 = i^2$. For these choices of roots,

$$R_0 = 518400, \; R_1 = -773136, \; R_2 = 296296.$$

Solving for a through D yields

$$\begin{aligned}
A &= 64R_0^3 &= 8916100448256000000 \\
c &= 8R_0^2 &= 2149908480000 \\
b &= 4R_0R_1 &= -1603174809600 \\
a &= 4R_0R_2 - R_1^2 &= 16660111104 \\
B &= R_5A - 2a &= -811365140824616222208 \\
C &= R_4A - a^2 - 2b &= 26497490347321493520384 \\
D &= R_3A - 2ab - 2c &= -343107594345448813363200
\end{aligned}$$

Constructing Rank 6 Family

We convert $y^2 = f(x,t)$ to $y^2 = F(x,T)$, which is in Weierstrass normal form. We send $y \to \frac{y}{T^2+2T-A+1}$, $x \to \frac{x}{T^2+2T-A+1}$, and then multiply both sides by $(T^2+2T-A+1)^2$. For future reference, we note that

$$\begin{aligned} T^2+2T-A+1 &= (T+1-\sqrt{A})(T+1+\sqrt{A}) \\ &= (T-t_1)(T-t_2) \\ &= (T-2985983999)(T+2985984001). \end{aligned}$$

We have

$$\begin{aligned} f(x,T) &= T^2x^3+(2x^3+2ax^2+2bx+2c)T-(A-1)x^3-Bx^2-Cx-D \\ &= (T^2+2T-A+1)x^3+(2aT-B)x^2+(2bT-C)x+(2cT-D) \\ F(x,T) &= x^3+(2aT-B)x^2+(2bT-C)(T^2+2T-A+1)x \\ &\quad +(2cT-D)(T^2+2T-A+1)^2. \end{aligned}$$

Constructing Rank 6 Family

We now study the $-pA_{\mathcal{E}}(p)$ arising from $y^2 = F(x, T)$. It is enough to show this is $6p + O(1)$ for all p greater than some p_0. Note that t_1, t_2 are the unique roots of $t^2 + 2t - A + 1 \equiv 0 \bmod p$. We find

$$-pA_{\mathcal{E}}(p) = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) = \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right).$$

For $t \neq t_1, t_2$, send $x \longrightarrow (t^2 + 2t - A + 1)x$. As $(t^2 + 2t - A + 1) \not\equiv 0$, $\left(\frac{(t^2+2t-A+1)^2}{p}\right) = 1$. Simple algebra yields

$$\begin{aligned} -pA_{\mathcal{E}}(p) &= 6p + O(1) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\ &= 6p + O(1) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{(2at-B)x^2 + (2bt-C)x + (2ct-D)}{p}\right). \end{aligned}$$

Constructing Rank 6 Family

The last sum above is negligible (i.e., is $O(1)$) if

$$D(t) \;=\; (2bt - C)^2 - 4(2at - B)(2ct - D) \not\equiv 0(p).$$

Calculating yields

$$\begin{aligned}
D(t_1) &= 4291243480243836561123092143580209905401856 \\
&= 2^{32} \cdot 3^{25} \cdot 7^5 \cdot 11^2 \cdot 13 \cdot 19 \cdot 29 \cdot 31 \cdot 47 \cdot 67 \cdot 83 \cdot 97 \cdot 103 \\
D(t_2) &= 4291243816662452751895093255391719515488256 \\
&= 2^{33} \cdot 3^{12} \cdot 7 \cdot 11 \cdot 13 \cdot 41 \cdot 173 \cdot 17389 \cdot 805873 \cdot 9447850813.
\end{aligned}$$

Constructing Rank 6 Family

Hence, except for finitely many primes (coming from factors of $D(t_i)$, $a, \dots, D$, t_1 and t_2), $-A_{\mathcal{E}}(p) = 6p + O(1)$ as desired.

We have shown: There exist integers a, b, c, A, B, C, D so that the curve $\mathcal{E} : y^2 = x^3T^2 + 2g(x)T - h(x)$ over $\mathbb{Q}(T)$, with $g(x) = x^3 + ax^2 + bx + c$ and $h(x) = (A-1)x^3 + Bx^2 + Cx + D$, has rank 6 over $\mathbb{Q}(T)$. In particular, with the choices of a through D above, $\mathcal{E}$ is a rational elliptic surface and has Weierstrass form

$$\begin{aligned} y^2 &= x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x \\ &\quad + (2cT - D)(T^2 + 2T - A + 1)^2 \end{aligned}$$

Constructing Rank 6 Family

We show $\mathcal{E}$ is a rational elliptic surface by translating $x \mapsto x - (2aT - B)/3$, which yields $y^2 = x^3 + A(T)x + B(T)$ with $\deg(A) = 3, \deg(B) = 5$.

The Rosen-Silverman theorem is applicable, and as we can compute $A_{\mathcal{E}}(p)$, we know the rank is exactly 6 (and we never need to calculate height matrices). $\square$

Applications

Biases in Lower Order Terms

Let $n_{3,2,p}$ equal the number of cube roots of 2 modulo p, and set $c_0(p) = \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p$, $c_1(p) = \left[\sum_{x \bmod p} \left(\frac{x^3-x}{p}\right)\right]^2$, $c_{3/2}(p) = p\sum_{x(p)} \left(\frac{4x^3+1}{p}\right)$.

Family	$A_{1,\mathcal{E}}(p)$	$A_{2,\mathcal{E}}(p)$
$y^2 = x^3 + Sx + T$	0	$p^3 - p^2$
$y^2 = x^3 + 2^4(-3)^3(9T+1)^2$	0	$\begin{cases} 2p^2-2p & p\equiv 2 \bmod 3 \\ 0 & p\equiv 1 \bmod 3 \end{cases}$
$y^2 = x^3 \pm 4(4T+2)x$	0	$\begin{cases} 2p^2-2p & p\equiv 1 \bmod 4 \\ 0 & p\equiv 3 \bmod 4 \end{cases}$
$y^2 = x^3 + (T+1)x^2 + Tx$	0	$p^2 - 2p - 1$
$y^2 = x^3 + x^2 + 2T + 1$	0	$p^2 - 2p - \left(\frac{-3}{p}\right)$
$y^2 = x^3 + Tx^2 + 1$	$-p$	$p^2 - n_{3,2,p}p - 1 + c_{3/2}(p)$
$y^2 = x^3 - T^2x + T^2$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 - T^2x + T^4$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 + Tx^2 - (T+3)x + 1$	$-2c_{p,1;4}p$	$p^2 - 4c_{p,1;6}p - 1$

where $c_{p,a;m} = 1$ if $p \equiv a \bmod m$ and otherwise is 0.

Biases in Lower Order Terms

The first family is the family of all elliptic curves; it is a two parameter family and we expect the main term of its second moment to be p^3.

Note that except for our family $y^2 = x^3 + Tx^2 + 1$, all the families $\mathcal{E}$ have $A_{2,\mathcal{E}}(p) = p^2 - h(p)p + O(1)$, where $h(p)$ is non-negative. Further, many of the families have $h(p) = m_{\mathcal{E}} > 0$.

Note $c_1(p)$ is the square of the coefficients from an elliptic curve with complex multiplication. It is non-negative and of size p for $p \not\equiv 3 \bmod 4$, and zero for $p \equiv 1 \bmod 4$ (send $x \mapsto -x \bmod p$ and note $\left(\frac{-1}{p}\right) = -1$).

It is somewhat remarkable that all these families have a correction to the main term in Michel's theorem in the same direction, and we analyze the consequence this has on the average rank. For our family which has a $p^{3/2}$ term, note that on average this term is zero and the p term is negative.

Lower order terms and average rank

$$\frac{1}{N}\sum_{t=N}^{2N}\sum_{\gamma_t}\phi\left(\gamma_t\frac{\log R}{2\pi}\right) = \widehat{\phi}(0)+\phi(0)-\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p}\widehat{\phi}\left(\frac{\log p}{\log R}\right)a_t(p)$$
$$-\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p^2}\widehat{\phi}\left(\frac{2\log p}{\log R}\right)a_t(p)^2+O\left(\frac{\log\log R}{\log R}\right).$$

If ϕ is non-negative, we obtain a bound for the average rank in the family by restricting the sum to be only over zeros at the central point. The error $O\left(\frac{\log\log R}{\log R}\right)$ comes from trivial estimation and ignores probable cancellation, and we expect $O\left(\frac{1}{\log R}\right)$ or smaller to be the correct magnitude. For most families $\log R \sim \log N^a$ for some integer a.

Lower order terms and average rank (cont)

The main term of the first and second moments of the $a_t(p)$ give $r\phi(0)$ and $-\frac{1}{2}\phi(0)$.

Assume the second moment of $a_t(p)^2$ is $p^2 - m_{\mathcal{E}}p + O(1)$, $m_{\mathcal{E}} > 0$.

We have already handled the contribution from p^2, and $-m_{\mathcal{E}}p$ contributes

$$\begin{aligned} S_2 &\sim \frac{-2}{N}\sum_p \frac{\log p}{\log R}\widehat{\phi}\left(2\frac{\log p}{\log R}\right)\frac{1}{p^2}\frac{N}{p}(-m_{\mathcal{E}}p) \\ &= \frac{2m_{\mathcal{E}}}{\log R}\sum_p \widehat{\phi}\left(2\frac{\log p}{\log R}\right)\frac{\log p}{p^2}. \end{aligned}$$

Thus there is a contribution of size $1/\log R$.

Lower order terms and average rank (cont)

A good choice of test functions (see Appendix A of [ILS]) is the Fourier pair

$$\phi(x) \ = \ \frac{\sin^2(2\pi\frac{\sigma}{2}x)}{(2\pi x)^2}, \qquad \widehat{\phi}(u) \ = \ \begin{cases} \frac{\sigma-|u|}{4} & \text{if } |u| \le \sigma \\ 0 & \text{otherwise.} \end{cases}$$

Note $\phi(0) = \frac{\sigma^2}{4}$, $\widehat{\phi}(0) = \frac{\sigma}{4} = \frac{\phi(0)}{\sigma}$, and evaluating the prime sum gives

$$S_2 \quad \sim \quad \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2 \log R}\right) \frac{m_{\mathcal{E}}}{\log R}\, \phi(0).$$

Lower order terms and average rank (cont)

Let r_t denote the number of zeros of E_t at the central point (i.e., the analytic rank). Then up to our $O\left(\frac{\log\log R}{\log R}\right)$ errors (which we think should be smaller), we have

$$\begin{aligned}
\frac{1}{N}\sum_{t=N}^{2N} r_t\phi(0) &\le \frac{\phi(0)}{\sigma} + \left(r+\frac{1}{2}\right)\phi(0) + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}\phi(0) \\
\text{Ave Rank}_{[N,2N]}(\mathcal{E}) &\le \frac{1}{\sigma} + r + \frac{1}{2} + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}.
\end{aligned}$$

$\sigma = 1$, $m_{\mathcal{E}} = 1$: for conductors of size 10^{12}, the average rank is bounded by $1 + r + \frac{1}{2} + .03 = r + \frac{1}{2} + 1.03$. This is significantly higher than Fermigier's observed $r + \frac{1}{2} + .40$.

$\sigma = 2$: lower order correction contributes .02 for conductors of size 10^{12}, the average rank bounded by $\frac{1}{2} + r + \frac{1}{2} + .02 = r + \frac{1}{2} + .52$. Now in the ballpark of Fermigier's bound (already there without the potential correction term!).

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

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

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

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

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

Goal: Construct families of hyperelliptic curves with high rank.

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

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

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

Generalizes 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

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

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

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

- 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

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

Then by the Generalized Nagao Conjecture

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

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 (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.

Bias Example

Theorem (HLKM 2018)

Consider $\mathcal{X} : y^2 = x^n + x^h T^k$. If h is odd assume $\nu_2(p-1) > \nu_2(n-h)$, where ν_2 is the 2-adic valuation. 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

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

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

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

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

Calculations Part 2: Assume $\gcd(n-h, k, p-1) = 1$

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

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

Open Questions and References

Open Questions

- Higher rank.
- Bias conjecture.
- Higher moments.
- Higher degrees.

Publications: Elliptic Curves

1. 1- *and* 2-*level densities for families of elliptic curves: evidence for the underlying group symmetries*, Compositio Mathematica **140** (2004), 952–992. http://arxiv.org/pdf/math/0310159
2. *Variation in the number of points on elliptic curves and applications to excess rank*, C. R. Math. Rep. Acad. Sci. Canada **27** (2005), no. 4, 111–120. http://arxiv.org/abs/math/0506461
3. *Constructing one-parameter families of elliptic curves over $\mathbb{Q}(T)$ with moderate rank* (with Scott Arms and Álvaro Lozano-Robledo), Journal of Number Theory **123** (2007), no. 2, 388–402. http://arxiv.org/abs/math/0406579
4. *Towards an 'average' version of the Birch and Swinnerton-Dyer Conjecture* (with John Goes), Journal of Number Theory **130** (2010), no. 10, 2341–2358. http://arxiv.org/abs/0911.2871
5. *Moments of the rank of elliptic curves* (with Siman Wong), Canad. J. of Math. **64** (2012), no. 1, 151–182. http://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/mwMomentsRanksEC812final.pdf
6. *Lower-Order Biases in Elliptic Curve Fourier Coefficients in Families* (with B. Mackall, C. Rapti and K. Winsor), Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures (David Kohel and Igor Shparlinski, editors), Contemporary Mathematics **663**, AMS, Providence, RI 2016.
7. *Lower-Order Biases Second Moments of Fourier Coefficients in Families of L-Functions* (with Megumi Asada, Ryan Chen, Eva Fourakis, Yujin Kim, Andrew Kwon, Jared Lichtman, Blake Mackall, Eric Winsor, Karl Winsor, Jianing Yang, Kevin Yang), preprint.
8. *Rank and Bias in Families of Hyperelliptic Curves via Nagao's Conjecture* (with Trajan Hammonds, Seoyoung Kim, Benjamin Logsdon), 2019, in preparation.