# A positive proportion of hyperelliptic curves have no unexpected quadratic points


Ashvin A. Swaminathan

in joint work with Manjul Bhargava, Jef Laga, and Arul Shankar


Five College Number Theory Seminar

Amherst College

March 12th, 2024

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \setminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Standard families of hyperelliptic curves of genus $g \geq 2$

- Recall: A *hyperelliptic curve* over $\mathbb{Q}$ is a nice (i.e., smooth, projective, and geometrically integral) curve with a degree-2 map to $\mathbb{P}^1_{\mathbb{Q}}$

**Families with marked $\mathbb{Q}$-rational points**

- Monic odd degree: $y^2 = x^{2g+1} + c_{2g-1}x^{2g-1} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have marked $\mathbb{Q}$-rational Weierstrass point at $\infty$
- Monic even degree: $y^2 = x^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$
  - Have a pair of marked $\mathbb{Q}$-rational non-Weierstrass points $\{\infty, \tau(\infty)\}$

**Families without marked $\mathbb{Q}$-rational points**

- Non-monic even degree: $y^2 = cx^{2g+2} + c_{2g}x^{2g} + \cdots + c_0$, for $c_i \in \mathbb{Z}$ and fixed $c \in \mathbb{Z} \smallsetminus \{n^2 : n \in \mathbb{Z}\}$
- General even degree: $y^2 = c_{2g+2}x^{2g+2} + \cdots + c_0$
  - So-called "universal family" of hyperelliptic curves over $\mathbb{Q}$

# Motivating questions

- Let $\mathscr{F}$ be a standard family of hyperelliptic curves of genus $g \geq 2$
- Given $C \in \mathscr{F}$ and $P \in C(\mathbb{Q})$, we call $P$ *expected* if $P$ is among the marked points of the family $\mathscr{F}$, and *unexpected* otherwise
- Falting's Theorem $\Longrightarrow \#C(\mathbb{Q}) < \infty$ for each $C \in \mathscr{F}$; i.e., the set of unexpected $\mathbb{Q}$-rational points on $C$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coeff-icients), how often does $C$ have no unexpected $\mathbb{Q}$-rational points?

# Motivating questions

- Let $\mathscr{F}$ be a standard family of hyperelliptic curves of genus $g \geq 2$
- Given $C \in \mathscr{F}$ and $P \in C(\mathbb{Q})$, we call $P$ *expected* if $P$ is among the marked points of the family $\mathscr{F}$, and *unexpected* otherwise
- Falting's Theorem $\implies \#C(\mathbb{Q}) < \infty$ for each $C \in \mathscr{F}$; i.e., the set of unexpected $\mathbb{Q}$-rational points on $C$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coeff- icients), how often does $C$ have no unexpected $\mathbb{Q}$-rational points?

# Motivating questions

- Let $\mathscr{F}$ be a standard family of hyperelliptic curves of genus $g \geq 2$
- Given $C \in \mathscr{F}$ and $P \in C(\mathbb{Q})$, we call $P$ *expected* if $P$ is among the marked points of the family $\mathscr{F}$, and *unexpected* otherwise
- Falting's Theorem $\implies \#C(\mathbb{Q}) < \infty$ for each $C \in \mathscr{F}$; i.e., the set of unexpected $\mathbb{Q}$-rational points on $C$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coeff-icients), how often does $C$ have no unexpected $\mathbb{Q}$-rational points?

# Motivating questions

- Let $\mathscr{F}$ be a standard family of hyperelliptic curves of genus $g \geq 2$
- Given $C \in \mathscr{F}$ and $P \in C(\mathbb{Q})$, we call $P$ *expected* if $P$ is among the marked points of the family $\mathscr{F}$, and *unexpected* otherwise
- Falting's Theorem $\Longrightarrow \#C(\mathbb{Q}) < \infty$ for each $C \in \mathscr{F}$; i.e., the set of unexpected $\mathbb{Q}$-rational points on $C$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coeff-icients), how often does $C$ have no unexpected $\mathbb{Q}$-rational points?

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

**Theorem (Bhargava, 2013)**

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])**

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\mathrm{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

**Theorem (Bhargava, 2013)**

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])**

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\mathrm{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

**Theorem (Bhargava, 2013)**

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])**

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\mathrm{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

**Theorem (Bhargava, 2013)**

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])**

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\mathrm{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

**Theorem (Bhargava, 2013)**

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])**

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\mathrm{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

**Theorem (Bhargava, 2013)**

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])**

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\operatorname{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

## Theorem (Bhargava, 2013)

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

## Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\mathrm{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves

**Families without marked $\mathbb{Q}$-rational points**

**Theorem (Bhargava, 2013)**

*When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$ (and is $> 50\%$ for every $g \geq 2$); and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Bhargava-Gross-Wang, 2017 [corrected in BSS, 2021])**

*Let $k$ be odd. When even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $(\mathrm{Sym}^k C)(\mathbb{Q}) = \varnothing$*

- *is $> 0$ for every $g \geq 1$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** Show that most curves have no locally soluble 2-covers

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

**Theorem (Poonen-Stoll, 2013)**

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 3$; and*
- *tends to 100% as $g \to \infty$.*

**Theorem (Shankar-Wang, 2018)**

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 9$; and*
- *tends to 100% as $g \to \infty$.*

**Proof strategy:** "Selmer-group Chabauty"

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

**Theorem (Poonen-Stoll, 2013)**

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 3$; and*
- *tends to 100% as $g \to \infty$.*

**Theorem (Shankar-Wang, 2018)**

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 9$; and*
- *tends to 100% as $g \to \infty$.*

**Proof strategy:** "Selmer-group Chabauty"

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

**Theorem (Poonen-Stoll, 2013)**

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 3$; and*
- *tends to 100% as $g \to \infty$.*

**Theorem (Shankar-Wang, 2018)**

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 9$; and*
- *tends to 100% as $g \to \infty$.*

**Proof strategy:** "Selmer-group Chabauty"

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

**Theorem (Poonen-Stoll, 2013)**

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 3$; and*
- *tends to 100% as $g \to \infty$.*

**Theorem (Shankar-Wang, 2018)**

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 9$; and*
- *tends to 100% as $g \to \infty$.*

**Proof strategy:** "Selmer-group Chabauty"

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

**Theorem (Poonen-Stoll, 2013)**

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is* $\gg 16^{-g} > 0$ *for every* $g \geq 3$; *and*
- *tends to* $100\%$ *as* $g \to \infty$.

**Theorem (Shankar-Wang, 2018)**

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is* $\gg 16^{-g} > 0$ *for every* $g \geq 9$; *and*
- *tends to* $100\%$ *as* $g \to \infty$.

**Proof strategy:** "Selmer-group Chabauty"

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

**Theorem (Poonen-Stoll, 2013)**

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 3$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Shankar-Wang, 2018)**

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 9$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** "Selmer-group Chabauty"

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

**Theorem (Poonen-Stoll, 2013)**

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 3$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Theorem (Shankar-Wang, 2018)**

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 9$; and*
- *tends to $100\%$ as $g \to \infty$.*

**Proof strategy:** "Selmer-group Chabauty"

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Families with marked $\mathbb{Q}$-rational points**

## Theorem (Poonen-Stoll, 2013)

*When monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 3$; and*
- *tends to 100% as $g \to \infty$.*

## Theorem (Shankar-Wang, 2018)

*When monic even-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g$ are ordered by height, the proportion of curves $C$ such that $C(\mathbb{Q}) = \{\infty, \tau(\infty)\}$*

- *is $\gg 16^{-g} > 0$ for every $g \geq 9$; and*
- *tends to 100% as $g \to \infty$.*

**Proof strategy:** "Selmer-group Chabauty"

# Motivating questions (cont.)

What about points of even degree?

- Given $C \in \mathscr{F}$ and $P \in (\mathrm{Sym}^2 C)(\mathbb{Q})$, we call $P$ *expected* if $P$ is the preimage of $\mathbb{Q}$-rational point under the hyperelliptic map $C \to \mathbb{P}^1_{\mathbb{Q}}$, and *unexpected* otherwise
- Faltings proved that if $g \geq 4$, the set of unexpected points in $(\mathrm{Sym}^2 C)(\mathbb{Q})$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coefficients), how often does $\mathrm{Sym}^2 C$ have no unexpected $\mathbb{Q}$-rational points? (I.e., how often does $C$ have no unexpected quadratic points?)

# Motivating questions (cont.)

What about points of even degree?

- Given $C \in \mathscr{F}$ and $P \in (\mathrm{Sym}^2 C)(\mathbb{Q})$, we call $P$ *expected* if $P$ is the preimage of $\mathbb{Q}$-rational point under the hyperelliptic map $C \to \mathbb{P}^1_{\mathbb{Q}}$, and *unexpected* otherwise
- Faltings proved that if $g \geq 4$, the set of unexpected points in $(\mathrm{Sym}^2 C)(\mathbb{Q})$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coefficients), how often does $\mathrm{Sym}^2 C$ have no unexpected $\mathbb{Q}$-rational points? (I.e., how often does $C$ have no unexpected quadratic points?)

# Motivating questions (cont.)

What about points of even degree?

- Given $C \in \mathscr{F}$ and $P \in (\mathrm{Sym}^2 C)(\mathbb{Q})$, we call $P$ *expected* if $P$ is the preimage of $\mathbb{Q}$-rational point under the hyperelliptic map $C \to \mathbb{P}^1_{\mathbb{Q}}$, and *unexpected* otherwise
- Faltings proved that if $g \geq 4$, the set of unexpected points in $(\mathrm{Sym}^2 C)(\mathbb{Q})$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coefficients), how often does $\mathrm{Sym}^2 C$ have no unexpected $\mathbb{Q}$-rational points? (I.e., how often does $C$ have no unexpected quadratic points?)

# Motivating questions (cont.)

What about points of even degree?

- Given $C \in \mathscr{F}$ and $P \in (\operatorname{Sym}^2 C)(\mathbb{Q})$, we call $P$ *expected* if $P$ is the preimage of $\mathbb{Q}$-rational point under the hyperelliptic map $C \to \mathbb{P}^1_{\mathbb{Q}}$, and *unexpected* otherwise
- Faltings proved that if $g \geq 4$, the set of unexpected points in $(\operatorname{Sym}^2 C)(\mathbb{Q})$ is finite

**Question**

When curves $C \in \mathscr{F}$ are ordered by height ($\approx$ the sizes of their coefficients), how often does $\operatorname{Sym}^2 C$ have no unexpected $\mathbb{Q}$-rational points? (I.e., how often does $C$ have no unexpected quadratic points?)

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\mathrm{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C)) \leq^* 3 \implies$ $\mathrm{Avg}\,\mathrm{rk}\, J(\mathbb{Q}) \leq 3/2 \implies$ a positive proportion of $C$ have $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\mathrm{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\operatorname{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\operatorname{rk} J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C)) \leq^* 3 \implies \operatorname{Avg} \operatorname{rk} J(\mathbb{Q}) \leq 3/2 \implies$ a positive proportion of $C$ have $\operatorname{rk} J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\operatorname{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\operatorname{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\operatorname{rk} J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\operatorname{Avg} \# \operatorname{Sel}_2(J(C)) \leq^* 3 \Longrightarrow \operatorname{Avg} \operatorname{rk} J(\mathbb{Q}) \leq 3/2 \Longrightarrow$ a positive proportion of $C$ have $\operatorname{rk} J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\operatorname{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\mathrm{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\operatorname{rk} J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\operatorname{Avg} \# \mathrm{Sel}_2(\mathrm{J}(C)) \leq^* 3 \implies \operatorname{Avg} \operatorname{rk} J(\mathbb{Q}) \leq 3/2 \implies$ a positive proportion of $C$ have $\operatorname{rk} J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\mathrm{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\mathrm{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\mathrm{Avg}\, \#\, \mathrm{Sel}_2(\mathrm{J}(C)) \leq^* 3 \Longrightarrow \mathrm{Avg}\, \mathrm{rk}\, J(\mathbb{Q}) \leq 3/2 \Longrightarrow$ a positive proportion of $C$ have $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\mathrm{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\mathrm{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\mathrm{Avg}\, \#\, \mathrm{Sel}_2(\mathrm{J}(C)) \leq^* 3 \implies \mathrm{Avg}\,\mathrm{rk}\, J(\mathbb{Q}) \leq 3/2 \implies$ a positive proportion of $C$ have $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\mathrm{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\mathrm{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\mathrm{Avg}\, \#\, \mathrm{Sel}_2(\mathrm{J}(C)) \leq^* 3 \implies \mathrm{Avg}\, \mathrm{rk}\, J(\mathbb{Q}) \leq 3/2 \implies$ a positive proportion of $C$ have $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\mathrm{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\operatorname{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\operatorname{rk} J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C)) \leq^* 3 \implies$ $\operatorname{Avg} \operatorname{rk} J(\mathbb{Q}) \leq 3/2 \implies$ a positive proportion of $C$ have $\operatorname{rk} J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\operatorname{Sym}^2 C)(\mathbb{Q})$

# Earlier work on pointlessness of hyperelliptic curves (cont.)

**Monic odd hyperelliptic curves**

**Theorem (Gunther-Morrow, 2017)**

*Under a technical assumption, when monic odd-degree hyperelliptic curves $C/\mathbb{Q}$ of genus $g \geq 4$ are ordered by height, a positive proportion of curves $C$ are such that $\mathrm{Sym}^2 C$ has $\leq 24$ unexpected $\mathbb{Q}$-rational points.*

**Proof strategy**:

- Park (2016) developed Chabauty for symmetric powers of curves, under the hypothesis $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$; combine with the result of Bhargava-Gross (2013) that $\mathrm{Avg}\, \#\, \mathrm{Sel}_2(\mathrm{J}(C)) \leq^* 3 \Longrightarrow$ $\mathrm{Avg}\, \mathrm{rk}\, J(\mathbb{Q}) \leq 3/2 \Longrightarrow$ a positive proportion of $C$ have $\mathrm{rk}\, J(\mathbb{Q}) \leq 1$
- But Park's work was missing a technical assumption on the transversality of the intersection of the vanishing loci of 1-forms used to bound $(\mathrm{Sym}^2 C)(\mathbb{Q})$

# Main result

**Theorem (BLSS, work in progress, 2024)**

*Let $\mathscr{F}$ be any one of the standard families of hyperelliptic curves of genus $g$ over $\mathbb{Q}$. When ordered by height, the proportion of curves $C \in \mathscr{F}$ with the property that $\operatorname{Sym}^2 C$ has no unexpected $\mathbb{Q}$-rational points is $\gg 16^{-g} > 0$ for every $g \geq 4$.*

# Selmer-group Chabauty

- Let $C$ be monic odd hyperelliptic of genus $g \geq 4$. Let $J = \mathrm{J}(C)$ be the Jacobian, and let $X = \mathrm{im}(\mathrm{Sym}^2 C \to J)$
- For a prime $p$, let $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ be the $p$-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Consider the following diagram:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[rr, hook] \arrow[d, hook] & & X(\mathbb{Q}_p) \arrow[d, hook] & & \\
J(\mathbb{Q}) \arrow[r, hook] \arrow[d, two heads] & \overline{J(\mathbb{Q})} \arrow[r, hook] \arrow[d, two heads] & J(\mathbb{Q}_p) \arrow[r, two heads, "\log"] \arrow[d, two heads] & \mathbb{Z}_p^g \arrow[d, two heads] \arrow[dr, dashed, "\rho"] & \\
J(\mathbb{Q})/pJ(\mathbb{Q}) \arrow[r, two heads] \arrow[dr] & \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \arrow[r] & J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \arrow[r, two heads, "\log \otimes \mathbb{F}_p"] & \mathbb{F}_p^g \arrow[r, dashed, "\mathbb{P}"] & \mathbb{P}^{g-1}(\mathbb{F}_p) \\
& \mathrm{Sel}_p J \arrow[ur] \arrow[urr, "\sigma"] & & &
\end{tikzcd}$$

- The map $\log \colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ is a local diffeomorphism onto its image, which can be identified with $\mathbb{Z}_p^g$; $\ker \log = J(\mathbb{Q}_p)^{\mathrm{tors}}$
- The map $\rho$ is defined on $\mathbb{Z}_p^g \setminus \{0\}$, given by scaling to an element of $\mathbb{P}^{g-1}(\mathbb{Z}_p)$ and reducing mod $p$

- Let $C$ be monic odd hyperelliptic of genus $g \geq 4$. Let $J = \mathrm{J}(C)$ be the Jacobian, and let $X = \mathrm{im}(\mathrm{Sym}^2 C \to J)$
- For a prime $p$, let $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ be the $p$-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Consider the following diagram:

$$
\begin{tikzcd}
X(\mathbb{Q}) \arrow[rr, hook] \arrow[d, hook] & & X(\mathbb{Q}_p) \arrow[d, hook] & & \\
J(\mathbb{Q}) \arrow[r, hook] \arrow[d, two heads] & \overline{J(\mathbb{Q})} \arrow[r, hook] \arrow[d, two heads] & J(\mathbb{Q}_p) \arrow[r, two heads, "\log"] \arrow[d, two heads] & \mathbb{Z}_p^g \arrow[d, two heads] \arrow[dr, dashed, "\rho"] & \\
J(\mathbb{Q})/pJ(\mathbb{Q}) \arrow[r, two heads] \arrow[dr] & \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \arrow[r] & J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \arrow[r, two heads, "\log \otimes \mathbb{F}_p"] & \mathbb{F}_p^g \arrow[r, dashed, "\mathbb{P}"] & \mathbb{P}^{g-1}(\mathbb{F}_p) \\
 & \mathrm{Sel}_p J \arrow[ur] \arrow[urr, "\sigma"'] & & &
\end{tikzcd}
$$

- The map $\log \colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ is a local diffeomorphism onto its image, which can be identified with $\mathbb{Z}_p^g$; $\ker \log = J(\mathbb{Q}_p)^{\mathrm{tors}}$
- The map $\rho$ is defined on $\mathbb{Z}_p^g \setminus \{0\}$, given by scaling to an element of $\mathbb{P}^{g-1}(\mathbb{Z}_p)$ and reducing mod $p$

- Let $C$ be monic odd hyperelliptic of genus $g \geq 4$. Let $J = \mathrm{J}(C)$ be the Jacobian, and let $X = \mathrm{im}(\mathrm{Sym}^2 C \to J)$
- For a prime $p$, let $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ be the $p$-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Consider the following diagram:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[rr, hook] \arrow[d, hook] & & X(\mathbb{Q}_p) \arrow[d, hook] & & \\
J(\mathbb{Q}) \arrow[r, hook] \arrow[d, two heads] & \overline{J(\mathbb{Q})} \arrow[r, hook] \arrow[d, two heads] & J(\mathbb{Q}_p) \arrow[r, two heads, "\log"] \arrow[d, two heads] & \mathbb{Z}_p^g \arrow[d, two heads] \arrow[dr, dashed, "\rho"] & \\
J(\mathbb{Q})/pJ(\mathbb{Q}) \arrow[r, two heads] \arrow[dr] & \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \arrow[r] & J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \arrow[r, two heads, "\log \otimes \mathbb{F}_p"] & \mathbb{F}_p^g \arrow[r, dashed, "\mathbb{P}"] & \mathbb{P}^{g-1}(\mathbb{F}_p) \\
& \mathrm{Sel}_p J \arrow[ur] \arrow[urr, "\sigma"'] & & &
\end{tikzcd}$$

- The map $\log \colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ is a local diffeomorphism onto its image, which can be identified with $\mathbb{Z}_p^g$; $\ker \log = J(\mathbb{Q}_p)^{\mathrm{tors}}$
- The map $\rho$ is defined on $\mathbb{Z}_p^g \setminus \{0\}$, given by scaling to an element of $\mathbb{P}^{g-1}(\mathbb{Z}_p)$ and reducing mod $p$

# Selmer-group Chabauty

- Let $C$ be monic odd hyperelliptic of genus $g \geq 4$. Let $J = \mathrm{J}(C)$ be the Jacobian, and let $X = \mathrm{im}(\mathrm{Sym}^2 C \to J)$
- For a prime $p$, let $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ be the $p$-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Consider the following diagram:

$$
\begin{tikzcd}
X(\mathbb{Q}) \arrow[rr, hook] \arrow[d, hook] & & {\color{red} X(\mathbb{Q}_p)} \arrow[d, hook] & & \\
J(\mathbb{Q}) \arrow[r, hook] \arrow[d, two heads] & {\color{red} \overline{J(\mathbb{Q})}} \arrow[r, hook] \arrow[d, two heads] & J(\mathbb{Q}_p) \arrow[r, two heads, "\log"] \arrow[d, two heads] & \mathbb{Z}_p^g \arrow[d, two heads] \arrow[dr, dashed, "\rho"] & \\
J(\mathbb{Q})/pJ(\mathbb{Q}) \arrow[r, two heads] \arrow[dr, hook] & \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \arrow[r] & J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \arrow[r, two heads, "\log \otimes \mathbb{F}_p"] & \mathbb{F}_p^g \arrow[r, dashed, "\mathbb{P}"] & \mathbb{P}^{g-1}(\mathbb{F}_p) \\
& \mathrm{Sel}_p\, J \arrow[ur] \arrow[urr, two heads, "\sigma"'] & & &
\end{tikzcd}
$$

- The map $\log\colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ is a local diffeomorphism onto its image, which can be identified with $\mathbb{Z}_p^g$; $\ker \log = J(\mathbb{Q}_p)^{\mathrm{tors}}$
- The map $\rho$ is defined on $\mathbb{Z}_p^g \setminus \{0\}$, given by scaling to an element of $\mathbb{P}^{g-1}(\mathbb{Z}_p)$ and reducing mod $p$

- Let $C$ be monic odd hyperelliptic of genus $g \geq 4$. Let $J = \mathrm{J}(C)$ be the Jacobian, and let $X = \mathrm{im}(\mathrm{Sym}^2 C \to J)$
- For a prime $p$, let $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ be the $p$-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Consider the following diagram:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[rr, hook] \arrow[d, hook] & & \color{red}{X(\mathbb{Q}_p)} \arrow[d, hook] & & \\
J(\mathbb{Q}) \arrow[r, hook] \arrow[d, two heads] & \color{red}{\overline{J(\mathbb{Q})}} \arrow[r, hook] \arrow[d, two heads] & J(\mathbb{Q}_p) \arrow[r, two heads, "\log"] \arrow[d, two heads] & \mathbb{Z}_p^g \arrow[d, two heads] \arrow[dr, dashed, "\rho"] & \\
J(\mathbb{Q})/pJ(\mathbb{Q}) \arrow[r, two heads] \arrow[dr, hook] & \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \arrow[r] & J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \arrow[r, two heads, "\log \otimes \mathbb{F}_p"] & \mathbb{F}_p^g \arrow[r, dashed, "\mathbb{P}"] & \mathbb{P}^{g-1}(\mathbb{F}_p) \\
& \mathrm{Sel}_p J \arrow[ur] \arrow[urr, "\sigma"'] & & &
\end{tikzcd}$$

- The map $\log \colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ is a local diffeomorphism onto its image, which can be identified with $\mathbb{Z}_p^g$; $\ker \log = J(\mathbb{Q}_p)^{\mathrm{tors}}$
- The map $\rho$ is defined on $\mathbb{Z}_p^g \setminus \{0\}$, given by scaling to an element of $\mathbb{P}^{g-1}(\mathbb{Z}_p)$ and reducing mod $p$

# Selmer-group Chabauty

- Let $C$ be monic odd hyperelliptic of genus $g \geq 4$. Let $J = \mathrm{J}(C)$ be the Jacobian, and let $X = \mathrm{im}(\mathrm{Sym}^2 C \to J)$
- For a prime $p$, let $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ be the $p$-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Consider the following diagram:

$$
\begin{tikzcd}
X(\mathbb{Q}) \arrow[rr, hook] \arrow[d, hook] & & {\color{red} X(\mathbb{Q}_p)} \arrow[d, hook] & & \\
J(\mathbb{Q}) \arrow[r, hook] \arrow[d, two heads] & {\color{red}\overline{J(\mathbb{Q})}} \arrow[r, hook] \arrow[d, two heads] & J(\mathbb{Q}_p) \arrow[r, two heads, "\log"] \arrow[d, two heads] & \mathbb{Z}_p^g \arrow[d, two heads] \arrow[dr, dashed, "\rho"] & \\
J(\mathbb{Q})/pJ(\mathbb{Q}) \arrow[r, two heads] \arrow[dr] & \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \arrow[r] & J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \arrow[r, two heads, "\log \otimes \mathbb{F}_p"] & \mathbb{F}_p^g \arrow[r, dashed, "\mathbb{P}"] & \mathbb{P}^{g-1}(\mathbb{F}_p) \\
 & \mathrm{Sel}_p J \arrow[ur] \arrow[urr, "\sigma"'] & & &
\end{tikzcd}
$$

- The map $\log\colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ is a local diffeomorphism onto its image, which can be identified with $\mathbb{Z}_p^g$; $\ker \log = J(\mathbb{Q}_p)^{\mathrm{tors}}$
- The map $\rho$ is defined on $\mathbb{Z}_p^g \setminus \{0\}$, given by scaling to an element of $\mathbb{P}^{g-1}(\mathbb{Z}_p)$ and reducing mod $p$

# Selmer-group Chabauty

- Let $C$ be monic odd hyperelliptic of genus $g \geq 4$. Let $J = \mathrm{J}(C)$ be the Jacobian, and let $X = \mathrm{im}(\mathrm{Sym}^2 C \to J)$
- For a prime $p$, let $\overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)$ be the $p$-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Consider the following diagram:

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[rr, hook] \arrow[d, hook] & & X(\mathbb{Q}_p) \arrow[d, hook] & & \\
J(\mathbb{Q}) \arrow[r, hook] \arrow[d, two heads] & \overline{J(\mathbb{Q})} \arrow[r, hook] \arrow[d, two heads] & J(\mathbb{Q}_p) \arrow[r, two heads, "\log"] \arrow[d, two heads] & \mathbb{Z}_p^g \arrow[d, two heads] \arrow[dr, dashed, "\rho"] & \\
J(\mathbb{Q})/pJ(\mathbb{Q}) \arrow[r, two heads] \arrow[dr, hook] & \overline{J(\mathbb{Q})}/p\overline{J(\mathbb{Q})} \arrow[r] & J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \arrow[r, two heads, "\log \otimes \mathbb{F}_p"] & \mathbb{F}_p^g \arrow[r, dashed, "\mathbb{P}"] & \mathbb{P}^{g-1}(\mathbb{F}_p) \\
& \mathrm{Sel}_p J \arrow[ur] \arrow[urr, "\sigma"'] & & &
\end{tikzcd}$$

- The map $\log \colon J(\mathbb{Q}_p) \to T_0 J \simeq \mathbb{Q}_p^g$ is a local diffeomorphism onto its image, which can be identified with $\mathbb{Z}_p^g$; $\ker \log = J(\mathbb{Q}_p)^{\mathrm{tors}}$
- The map $\rho$ is defined on $\mathbb{Z}_p^g \setminus \{0\}$, given by scaling to an element of $\mathbb{P}^{g-1}(\mathbb{Z}_p)$ and reducing mod $p$

# Selmer-group Chabauty (cont.)

**Lemma**

*Suppose that*

1. *The composite map* $\sigma\colon \operatorname{Sel}_p J \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \to \mathbb{F}_p^g$ *is injective;*
2. $\mathbb{P}\sigma(\operatorname{Sel}_p J) \cap \rho \log(X(\mathbb{Q}_p)) = \varnothing$

*Then we have* $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)[p']$.

**Lemma**

*The generic monic odd hyperelliptic curve $C$ over $\mathbb{Q}_p$ has the property that* $X(\overline{\mathbb{Q}}_p) \cap J(\overline{\mathbb{Q}}_p)_{\mathrm{tors}} \subset J(\overline{\mathbb{Q}}_p)[2]$.

- Thus, under conditions of the first lemma, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} = 0$ $\implies \operatorname{Sym}^2 C$ has no unexpected quadratic points
- Remains to verify the conditions, which we do for $p = 2$

# Selmer-group Chabauty (cont.)

**Lemma**

*Suppose that*

1. *The composite map* $\sigma\colon \operatorname{Sel}_p J \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \to \mathbb{F}_p^g$ *is injective;*
2. $\mathbb{P}\sigma(\operatorname{Sel}_p J) \cap \rho \log(X(\mathbb{Q}_p)) = \varnothing$

*Then we have* $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)[p']$.

**Lemma**

*The generic monic odd hyperelliptic curve $C$ over $\mathbb{Q}_p$ has the property that* $X(\overline{\mathbb{Q}}_p) \cap J(\overline{\mathbb{Q}}_p)_{\mathrm{tors}} \subset J(\overline{\mathbb{Q}}_p)[2]$.

- Thus, under conditions of the first lemma, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} = 0$ $\implies \operatorname{Sym}^2 C$ has no unexpected quadratic points
- Remains to verify the conditions, which we do for $p = 2$

# Selmer-group Chabauty (cont.)

**Lemma**

*Suppose that*

1. *The composite map* $\sigma\colon \operatorname{Sel}_p J \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \to \mathbb{F}_p^g$ *is injective;*
2. $\mathbb{P}\sigma(\operatorname{Sel}_p J) \cap \rho\log(X(\mathbb{Q}_p)) = \varnothing$

*Then we have* $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)[p']$.

**Lemma**

*The generic monic odd hyperelliptic curve* $C$ *over* $\mathbb{Q}_p$ *has the property that* $X(\overline{\mathbb{Q}}_p) \cap J(\overline{\mathbb{Q}}_p)_{\mathrm{tors}} \subset J(\overline{\mathbb{Q}}_p)[2]$.

- Thus, under conditions of the first lemma, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} = 0$
  $\implies \operatorname{Sym}^2 C$ has no unexpected quadratic points
- Remains to verify the conditions, which we do for $p = 2$

# Selmer-group Chabauty (cont.)

**Lemma**

*Suppose that*

1. *The composite map* $\sigma\colon \operatorname{Sel}_p J \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \to \mathbb{F}_p^g$ *is injective;*
2. $\mathbb{P}\sigma(\operatorname{Sel}_p J) \cap \rho \log(X(\mathbb{Q}_p)) = \varnothing$

*Then we have* $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)[p']$.

**Lemma**

*The generic monic odd hyperelliptic curve* $C$ *over* $\mathbb{Q}_p$ *has the property that* $X(\overline{\mathbb{Q}}_p) \cap J(\overline{\mathbb{Q}}_p)_{\mathrm{tors}} \subset J(\overline{\mathbb{Q}}_p)[2]$.

- Thus, under conditions of the first lemma, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} = 0$ $\implies \operatorname{Sym}^2 C$ has no unexpected quadratic points
- Remains to verify the conditions, which we do for $p = 2$

# Selmer-group Chabauty (cont.)

**Lemma**

*Suppose that*

1. *The composite map* $\sigma\colon \operatorname{Sel}_p J \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p) \to \mathbb{F}_p^g$ *is injective;*
2. $\mathbb{P}\sigma(\operatorname{Sel}_p J) \cap \rho \log(X(\mathbb{Q}_p)) = \varnothing$

*Then we have* $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \subset J(\mathbb{Q}_p)[p']$.

**Lemma**

*The generic monic odd hyperelliptic curve* $C$ *over* $\mathbb{Q}_p$ *has the property that* $X(\overline{\mathbb{Q}}_p) \cap J(\overline{\mathbb{Q}}_p)_{\mathrm{tors}} \subset J(\overline{\mathbb{Q}}_p)[2]$.

- Thus, under conditions of the first lemma, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} = 0$ $\Longrightarrow \operatorname{Sym}^2 C$ has no unexpected quadratic points
- Remains to verify the conditions, which we do for $p = 2$

# Selmer-group Chabauty (cont.)

**Condition 1: Injectivity of $\sigma$**

- Bhargava-Gross (2013) proved two crucial facts about the statistical behavior of 2-Selmer groups of monic odd hyperelliptic Jacobians:
  - $\text{Avg}\,\#\,\text{Sel}_2(J) \leq 3$
  - Let $C$ vary in a sufficiently small subfamily defined by local conditions at 2 so that the group $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \simeq \Gamma$ is constant. Then the non-identity elements of the $\text{Sel}_2 J$ equidistribute in $\Gamma$
- Thus, the composite map $\sigma\colon \text{Sel}_2 J \to J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \to \mathbb{F}_2^g$ is very typically injective
- Analogous results were proven by Shankar-Wang for the monic even family, and by BLSS for the non-monic and universal families

**Condition 1: Injectivity of $\sigma$**

- Bhargava-Gross (2013) proved two crucial facts about the statistical behavior of 2-Selmer groups of monic odd hyperelliptic Jacobians:
  - Avg $\# \operatorname{Sel}_2(J) \leq 3$
  - Let $C$ vary in a sufficiently small subfamily defined by local conditions at 2 so that the group $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \simeq \Gamma$ is constant. Then the non-identity elements of the $\operatorname{Sel}_2 J$ equidistribute in $\Gamma$
- Thus, the composite map $\sigma\colon \operatorname{Sel}_2 J \to J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \to \mathbb{F}_2^g$ is very typically injective
- Analogous results were proven by Shankar-Wang for the monic even family, and by BLSS for the non-monic and universal families

# Selmer-group Chabauty (cont.)

**Condition 1: Injectivity of $\sigma$**

- Bhargava-Gross (2013) proved two crucial facts about the statistical behavior of 2-Selmer groups of monic odd hyperelliptic Jacobians:
  - $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J) \leq 3$
  - Let $C$ vary in a sufficiently small subfamily defined by local conditions at 2 so that the group $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \simeq \Gamma$ is constant. Then the non-identity elements of the $\mathrm{Sel}_2 J$ equidistribute in $\Gamma$
- Thus, the composite map $\sigma\colon \mathrm{Sel}_2 J \to J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \to \mathbb{F}_2^g$ is very typically injective
- Analogous results were proven by Shankar-Wang for the monic even family, and by BLSS for the non-monic and universal families

# Selmer-group Chabauty (cont.)

**Condition 1: Injectivity of $\sigma$**

- Bhargava-Gross (2013) proved two crucial facts about the statistical behavior of 2-Selmer groups of monic odd hyperelliptic Jacobians:
  - $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J) \leq 3$
  - Let $C$ vary in a sufficiently small subfamily defined by local conditions at 2 so that the group $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \simeq \Gamma$ is constant. Then the non-identity elements of the $\mathrm{Sel}_2 J$ equidistribute in $\Gamma$
- Thus, the composite map $\sigma\colon \mathrm{Sel}_2 J \to J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \to \mathbb{F}_2^g$ is very typically injective
- Analogous results were proven by Shankar-Wang for the monic even family, and by BLSS for the non-monic and universal families

# Selmer-group Chabauty (cont.)

**Condition 1: Injectivity of $\sigma$**

- Bhargava-Gross (2013) proved two crucial facts about the statistical behavior of 2-Selmer groups of monic odd hyperelliptic Jacobians:
  - $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J) \leq 3$
  - Let $C$ vary in a sufficiently small subfamily defined by local conditions at 2 so that the group $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \simeq \Gamma$ is constant. Then the non-identity elements of the $\mathrm{Sel}_2 J$ equidistribute in $\Gamma$
- Thus, the composite map $\sigma\colon \mathrm{Sel}_2 J \to J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \to \mathbb{F}_2^g$ is very typically injective
- Analogous results were proven by Shankar-Wang for the monic even family, and by BLSS for the non-monic and universal families

# Selmer-group Chabauty (cont.)

**Condition 2:** $\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) = \varnothing$

- Consider the subfamily of curves $C$ with special fiber at 2 given by $y^2 + y = x^{2g+1} + x + 1$ if $g \equiv 1 \pmod 3$ and $y^2 + y = x^{2g+1} + x^3 + 1$ otherwise.
  (This happens a fraction of $\gg 16^{-g}$ of the time)
- $C(\mathbb{F}_2) = \{\infty\}$ and $C(\mathbb{F}_4) = \{\infty, (0, \alpha), (0, \alpha + 1), (1, \alpha), (1, \alpha + 1)\}$
- Compute log explicitly in terms of power series on the residue disks lying above these points, and then use this explicit formula for log to compute a fixed subset $S \subset \mathbb{P}^{g-1}(\mathbb{F}_2)$ such that $\#S = 5$ and $\rho \log(X(\mathbb{Q}_2)) \subset S$ for every curve $C$ in the subfamily
- On the other hand, $\#\mathbb{P}\sigma(\mathrm{Sel}_2 J) \leq 3$ and equidistributes among elements of $\mathbb{F}_2^g$, so we typically have

$$\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) \subset \mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap S = \varnothing$$

# Selmer-group Chabauty (cont.)

**Condition 2:** $\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) = \varnothing$

- Consider the subfamily of curves $C$ with special fiber at 2 given by $y^2 + y = x^{2g+1} + x + 1$ if $g \equiv 1 \pmod 3$ and $y^2 + y = x^{2g+1} + x^3 + 1$ otherwise.
  (This happens a fraction of $\gg 16^{-g}$ of the time)
- $C(\mathbb{F}_2) = \{\infty\}$ and $C(\mathbb{F}_4) = \{\infty, (0, \alpha), (0, \alpha + 1), (1, \alpha), (1, \alpha + 1)\}$
- Compute log explicitly in terms of power series on the residue disks lying above these points, and then use this explicit formula for log to compute a fixed subset $S \subset \mathbb{P}^{g-1}(\mathbb{F}_2)$ such that $\#S = 5$ and $\rho \log(X(\mathbb{Q}_2)) \subset S$ for every curve $C$ in the subfamily
- On the other hand, $\#\mathbb{P}\sigma(\mathrm{Sel}_2 J) \leq 3$ and equidistributes among elements of $\mathbb{F}_2^g$, so we typically have

$$\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) \subset \mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap S = \varnothing$$

# Selmer-group Chabauty (cont.)

**Condition 2:** $\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) = \varnothing$

- Consider the subfamily of curves $C$ with special fiber at 2 given by $y^2 + y = x^{2g+1} + x + 1$ if $g \equiv 1 \pmod 3$ and $y^2 + y = x^{2g+1} + x^3 + 1$ otherwise. (This happens a fraction of $\gg 16^{-g}$ of the time)
- $C(\mathbb{F}_2) = \{\infty\}$ and $C(\mathbb{F}_4) = \{\infty, (0, \alpha), (0, \alpha + 1), (1, \alpha), (1, \alpha + 1)\}$
- Compute log explicitly in terms of power series on the residue disks lying above these points, and then use this explicit formula for log to compute a fixed subset $S \subset \mathbb{P}^{g-1}(\mathbb{F}_2)$ such that $\#S = 5$ and $\rho \log(X(\mathbb{Q}_2)) \subset S$ for every curve $C$ in the subfamily
- On the other hand, $\#\mathbb{P}\sigma(\mathrm{Sel}_2 J) \leq 3$ and equidistributes among elements of $\mathbb{F}_2^g$, so we typically have

$$\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) \subset \mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap S = \varnothing$$

# Selmer-group Chabauty (cont.)

**Condition 2:** $\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) = \varnothing$

- Consider the subfamily of curves $C$ with special fiber at 2 given by $y^2 + y = x^{2g+1} + x + 1$ if $g \equiv 1 \pmod 3$ and $y^2 + y = x^{2g+1} + x^3 + 1$ otherwise. (This happens a fraction of $\gg 16^{-g}$ of the time)
- $C(\mathbb{F}_2) = \{\infty\}$ and $C(\mathbb{F}_4) = \{\infty, (0,\alpha), (0,\alpha+1), (1,\alpha), (1,\alpha+1)\}$
- Compute log explicitly in terms of power series on the residue disks lying above these points, and then use this explicit formula for log to compute a fixed subset $S \subset \mathbb{P}^{g-1}(\mathbb{F}_2)$ such that $\#S = 5$ and $\rho \log(X(\mathbb{Q}_2)) \subset S$ for every curve $C$ in the subfamily
- On the other hand, $\#\mathbb{P}\sigma(\mathrm{Sel}_2 J) \leq 3$ and equidistributes among elements of $\mathbb{F}_2^g$, so we typically have

$$\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) \subset \mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap S = \varnothing$$

# Selmer-group Chabauty (cont.)

**Condition 2:** $\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) = \varnothing$

- Consider the subfamily of curves $C$ with special fiber at 2 given by $y^2 + y = x^{2g+1} + x + 1$ if $g \equiv 1 \pmod 3$ and $y^2 + y = x^{2g+1} + x^3 + 1$ otherwise. (This happens a fraction of $\gg 16^{-g}$ of the time)
- $C(\mathbb{F}_2) = \{\infty\}$ and $C(\mathbb{F}_4) = \{\infty, (0,\alpha), (0, \alpha+1), (1,\alpha), (1,\alpha+1)\}$
- Compute log explicitly in terms of power series on the residue disks lying above these points, and then use this explicit formula for log to compute a fixed subset $S \subset \mathbb{P}^{g-1}(\mathbb{F}_2)$ such that $\#S = 5$ and $\rho \log(X(\mathbb{Q}_2)) \subset S$ for every curve $C$ in the subfamily
- On the other hand, $\#\mathbb{P}\sigma(\mathrm{Sel}_2 J) \leq 3$ and equidistributes among elements of $\mathbb{F}_2^g$, so we typically have

$$\mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap \rho \log(X(\mathbb{Q}_2)) \subset \mathbb{P}\sigma(\mathrm{Sel}_2 J) \cap S = \varnothing$$

# 2-Selmer groups of even-degree hyperelliptic Jacobians

- Let $f(x,y) \in \mathbb{Z}[x,y]$ be a separable form of degree $n = 2g+2 \geq 4$; consider hyperelliptic curve $C_f : z^2 = f(x,y)$ with Jacobian $\mathrm{J}(C_f)$
- Objective: apply "parametrize-and-count strategy" to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as $f$ varies among:
  - Non-monic binary $n$-ic forms with fixed leading coefficient; or
  - Among the family of all binary $n$-ic forms

**Conjecture (Poonen and Rains, 2010)**

*Let $n \geq 6$ with $n \equiv 2 \pmod 4$. When binary $n$-ic forms $f$ are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) = 6$.

# 2-Selmer groups of even-degree hyperelliptic Jacobians

- Let $f(x, y) \in \mathbb{Z}[x, y]$ be a separable form of degree $n = 2g + 2 \geq 4$; consider hyperelliptic curve $C_f : z^2 = f(x, y)$ with Jacobian $\mathrm{J}(C_f)$
- Objective: apply "parametrize-and-count strategy" to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as $f$ varies among:
  - Non-monic binary $n$-ic forms with fixed leading coefficient; or
  - Among the family of all binary $n$-ic forms

**Conjecture (Poonen and Rains, 2010)**

*Let $n \geq 6$ with $n \equiv 2 \pmod 4$. When binary $n$-ic forms $f$ are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) = 6$.

# 2-Selmer groups of even-degree hyperelliptic Jacobians

- Let $f(x, y) \in \mathbb{Z}[x, y]$ be a separable form of degree $n = 2g + 2 \geq 4$; consider hyperelliptic curve $C_f : z^2 = f(x, y)$ with Jacobian $\mathrm{J}(C_f)$
- Objective: apply "parametrize-and-count strategy" to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as $f$ varies among:
  - Non-monic binary $n$-ic forms with fixed leading coefficient; or
  - Among the family of all binary $n$-ic forms

**Conjecture (Poonen and Rains, 2010)**

*Let $n \geq 6$ with $n \equiv 2 \pmod 4$. When binary $n$-ic forms $f$ are ordered by the max norm on their coefficients, we have $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) = 6$.*

# 2-Selmer groups of even-degree hyperelliptic Jacobians

- Let $f(x, y) \in \mathbb{Z}[x, y]$ be a separable form of degree $n = 2g + 2 \geq 4$; consider hyperelliptic curve $C_f \colon z^2 = f(x, y)$ with Jacobian $\mathrm{J}(C_f)$
- Objective: apply "parametrize-and-count strategy" to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as $f$ varies among:
  - Non-monic binary $n$-ic forms with fixed leading coefficient; or
  - Among the family of all binary $n$-ic forms

**Conjecture (Poonen and Rains, 2010)**

*Let $n \geq 6$ with $n \equiv 2 \pmod 4$. When binary $n$-ic forms $f$ are ordered by the max norm on their coefficients, we have $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) = 6$.*

# 2-Selmer groups of even-degree hyperelliptic Jacobians

- Let $f(x, y) \in \mathbb{Z}[x, y]$ be a separable form of degree $n = 2g + 2 \geq 4$; consider hyperelliptic curve $C_f \colon z^2 = f(x, y)$ with Jacobian $\mathrm{J}(C_f)$
- Objective: apply "parametrize-and-count strategy" to study the distribution of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ as $f$ varies among:
  - Non-monic binary $n$-ic forms with fixed leading coefficient; or
  - Among the family of all binary $n$-ic forms

**Conjecture (Poonen and Rains, 2010)**

*Let $n \geq 6$ with $n \equiv 2 \pmod 4$. When binary $n$-ic forms $f$ are ordered by the max norm on their coefficients, we have $\operatorname{Avg} \# \mathrm{Sel}_2(\mathrm{J}(C_f)) = 6$.*

# Primer on parametrize-and-count strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J\rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

# Primer on parametrize-and-count strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J\rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

# Primer on parametrize-and-count strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J\rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

# Primer on parametrize-and-count strategy

- **Step 1** (algebraic): Parametrize arithmetic objects of interest in terms of integral/rational orbits of a coregular representation $G \curvearrowright V$; if rational, check that these orbits have integral representatives
- E.g., let $V = \{\text{binary quartic forms}\}$ and $G = \mathrm{PGL}_2$; $\mathrm{PGL}_2 \curvearrowright V$, with ring of invariants $= \mathbb{Z}\langle I, J\rangle$
- **Step 2** (analytic): Use geometry-of-numbers methods and sieve techniques to count integral representatives

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{\begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array}\right\} \hookrightarrow \left\{\begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array}\right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x, y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x, y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\,\mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2\,\mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x, y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x, y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x, y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x, y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \ \textit{s.t.} \\ \det(xA + yB) = f(x, y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x, y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

  $$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x, y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x, y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization of $\mathrm{Sel}_2(\mathrm{J}(C_f))$

- Warmup case: $C_f(\mathbb{Q}) \neq \varnothing$. Then pullback via isomorphism $\mathrm{Pic}^1(C_f) \simeq \mathrm{Pic}^0(C_f) = \mathrm{J}(C_f)$ induces

$$\{\text{loc. sol. 2-covers of } \mathrm{J}(C_f)\} \leftrightarrow \{\text{loc. sol. 2-covers of } \mathrm{Pic}^1(C_f)\}$$

**Theorem (Bhargava–Gross–Wang, 2017 (via Wood, 2010))**

$$\left\{ \begin{array}{c} \textit{loc. sol. 2-cover} \\ \textit{of } \mathrm{Pic}^1(C_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n \textit{ s.t.} \\ \det(xA + yB) = f(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

- Serious problem: If $C_f(\mathbb{Q}) = \varnothing$, there may *not* exist $(A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^n$ with $\det(xA + yB) = f(x,y)$!
- Solution: Create $\mathbb{Q}$-point by replacing $f$ with $f^{\mathrm{mon}} := f_0^{-1} \times f(x, f_0 y)$
- $C_{f^{\mathrm{mon}}}(\mathbb{Q}) \neq \varnothing$, twist of $C_f$ by $\mathbb{Q}(\sqrt{f_0})$
- $\mathrm{J}(C_f)[2] \simeq \mathrm{J}(C_{f^{\mathrm{mon}}})[2]$, induces $H^1(\mathbb{Q}, \mathrm{J}(C_f)[2]) \simeq H^1(\mathbb{Q}, \mathrm{J}(C_{f^{\mathrm{mon}}})[2])$, which identifies elts of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ with certain 2-covers of $\mathrm{J}(C_{f^{\mathrm{mon}}})$

# Parametrization (cont'd.)

- Let $R_f := H^0\big(\operatorname{Proj} \frac{\mathbb{Z}[x,y]}{(f(x,y))}\big)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- $I$ = *ideal class of* $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$
- $I^2 \subset \alpha \times D_f$ *and* $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different($R_f$) in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\left(\text{Proj}\,\frac{\mathbb{Z}[x,y]}{(f(x,y))}\right)$, $K_f := \text{Frac}(R_f)$, $D_f := (\text{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\text{Sel}_2(\text{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- *$I$ = ideal class of $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$*
- *$I^2 \subset \alpha \times D_f$ and $\text{N}(I)^2 = \text{N}(\alpha) \times \text{N}(D_f)$*

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different$(R_f)$ in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\big(\operatorname{Proj} \frac{\mathbb{Z}[x,y]}{(f(x,y))}\big)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- $I$ = *ideal class of* $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$
- $I^2 \subset \alpha \times D_f$ *and* $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different($R_f$) in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\left(\operatorname{Proj} \frac{\mathbb{Z}[x,y]}{(f(x,y))}\right)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- *$I$ = ideal class of $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$*
- *$I^2 \subset \alpha \times D_f$ and $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$*

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different$(R_f)$ in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\big(\operatorname{Proj}\frac{\mathbb{Z}[x,y]}{(f(x,y))}\big)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- *$I$ = ideal class of $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$*
- *$I^2 \subset \alpha \times D_f$ and $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$*

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different($R_f$) in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\big(\operatorname{Proj} \frac{\mathbb{Z}[x,y]}{(f(x,y))}\big)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- $I =$ *ideal class of* $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$
- $I^2 \subset \alpha \times D_f$ *and* $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different$(R_f)$ in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\left(\operatorname{Proj}\frac{\mathbb{Z}[x,y]}{(f(x,y))}\right)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- *$I$ = ideal class of $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$*
- *$I^2 \subset \alpha \times D_f$ and $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$*

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different$(R_f)$ in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\left(\operatorname{Proj} \frac{\mathbb{Z}[x,y]}{(f(x,y))}\right)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\operatorname{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- $I$ = *ideal class of* $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$
- $I^2 \subset \alpha \times D_f$ *and* $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different($R_f$) in terms of orbits of a representation?

# Parametrization (cont'd.)

- Let $R_f := H^0\big(\operatorname{Proj}\frac{\mathbb{Z}[x,y]}{(f(x,y))}\big)$, $K_f := \operatorname{Frac}(R_f)$, $D_f := (\operatorname{different}(R_f))^{-1}$

**Theorem (Bhargava, Shankar, and S., 2021)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary form of even degree $n \geq 4$, and suppose $C_f$ loc. sol. if $n \equiv 0 \pmod 4$. Elements of $\mathrm{Sel}_2(\mathrm{J}(C_f))$ correspond to certain pairs $(I, \alpha)$, where:*

- *$I$ = ideal class of $R_f$; $\alpha \in K_f^\times / K_f^{\times 2}$*
- *$I^2 \subset \alpha \times D_f$ and $\mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f)$*

- Ellenberg on *MathOverflow* in 2011: Can one parametrize square roots of class of different$(R_f)$ in terms of orbits of a representation?

# Parametrization (cont'd.)

**Theorem (S., 2020)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary n-ic form with leading coefficient $f(1,0) = f_0 \neq 0$. Then we have an injection:*

$$\left\{ \begin{array}{c} (I,\alpha) \text{ s.t. } I^2 \subset \alpha \times D_f, \\ \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{mon}(x,y) \end{array} \right\} \Big/ \mathrm{SL}_n^{\pm}(\mathbb{Z})$$

*The image is defined by congruence conditions mod $f_0^{n-1}$.*

- Combining yields parametrization of 2-Selmer elements:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

# Parametrization (cont'd.)

**Theorem (S., 2020)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary n-ic form with leading coefficient $f(1,0) = f_0 \neq 0$. Then we have an injection:*

$$\left\{ \begin{array}{c} (I,\alpha) \text{ s.t. } I^2 \subset \alpha \times D_f, \\ \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{mon}(x,y) \end{array} \right\} \Big/ \mathrm{SL}_n^{\pm}(\mathbb{Z})$$

*The image is defined by congruence conditions mod $f_0^{n-1}$.*

- Combining yields parametrization of 2-Selmer elements:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

# Parametrization (cont'd.)

**Theorem (S., 2020)**

*Let $f \in \mathbb{Z}[x,y]$ be a binary n-ic form with leading coefficient $f(1,0) = f_0 \neq 0$. Then we have an injection:*

$$\left\{ \begin{array}{c} (I,\alpha) \text{ s.t. } I^2 \subset \alpha \times D_f, \\ \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{mon}(x,y) \end{array} \right\} \Big/ \mathrm{SL}_n^{\pm}(\mathbb{Z})$$

*The image is defined by congruence conditions mod $f_0^{n-1}$.*

- Combining yields parametrization of 2-Selmer elements:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A,B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x,y) \end{array} \right\} \Big/ (\mathrm{SL}_n/\mu_2)(\mathbb{Z})$$

# Parametrization (cont'd.)

**Theorem (S., 2020)**

*Let $f \in \mathbb{Z}[x, y]$ be a binary n-ic form with leading coefficient $f(1,0) = f_0 \neq 0$. Then we have an injection:*

$$\left\{ \begin{array}{c} (I, \alpha) \text{ s.t. } I^2 \subset \alpha \times D_f, \\ \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{mon}(x, y) \end{array} \right\} \Big/ \operatorname{SL}_n^{\pm}(\mathbb{Z})$$

*The image is defined by congruence conditions mod $f_0^{n-1}$.*

- Combining yields parametrization of 2-Selmer elements:

$$\operatorname{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x, y) \end{array} \right\} \Big/ (\operatorname{SL}_n / \mu_2)(\mathbb{Z})$$

# Parametrization (cont'd.)

**Theorem (S., 2020)**

*Let $f \in \mathbb{Z}[x, y]$ be a binary n-ic form with leading coefficient $f(1,0) = f_0 \neq 0$. Then we have an injection:*

$$\left\{ \begin{array}{c} (I, \alpha) \text{ s.t. } I^2 \subset \alpha \times D_f, \\ \mathrm{N}(I)^2 = \mathrm{N}(\alpha) \times \mathrm{N}(D_f) \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{mon}(x, y) \end{array} \right\} \Big/ \mathrm{SL}_n^{\pm}(\mathbb{Z})$$

*The image is defined by congruence conditions mod $f_0^{n-1}$.*

- Combining yields parametrization of 2-Selmer elements:

$$\mathrm{Sel}_2(\mathrm{J}(C_f)) \hookrightarrow \left\{ \begin{array}{c} (A, B) \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}^2 \mathbb{Z}^n \text{ s.t.} \\ \det(xA + yB) = f^{\mathrm{mon}}(x, y) \end{array} \right\} \Big/ (\mathrm{SL}_n / \mu_2)(\mathbb{Z})$$

# Main result: fixed leading coefficient

- Construction seems leading-coefficient dependent, so natural to apply it to families of binary forms with fixed leading coefficient

**Theorem (Bhargava, Shankar, and S., 2022)**

*Let $n \geq 4$ be even. Consider binary $n$-ic forms $f$ with fixed nonzero leading coefficient such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by "height," we have* $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^* 6$.

- Shows robustness of Poonen–Rains conjecture — average remains 6 even on thin families of curves with fixed leading coefficient
- Previously proven by Shankar and Wang (2018) for leading coefficient 1 (marked rational non-Weierstrass points at $\infty$)
- Analogous result proven by Bhargava and Gross (2013) for leading coefficient 0 (marked rational Weierstrass point at $\infty$)

# Main result: fixed leading coefficient

- Construction seems leading-coefficient dependent, so natural to apply it to families of binary forms with fixed leading coefficient

**Theorem (Bhargava, Shankar, and S., 2022)**

*Let $n \geq 4$ be even. Consider binary $n$-ic forms $f$ with fixed nonzero leading coefficient such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by "height," we have* $\operatorname{Avg} \# \mathrm{Sel}_2(J(C_f)) \leq^* 6$.

- Shows robustness of Poonen–Rains conjecture — average remains 6 even on thin families of curves with fixed leading coefficient
- Previously proven by Shankar and Wang (2018) for leading coefficient 1 (marked rational non-Weierstrass points at $\infty$)
- Analogous result proven by Bhargava and Gross (2013) for leading coefficient 0 (marked rational Weierstrass point at $\infty$)

# Main result: fixed leading coefficient

- Construction seems leading-coefficient dependent, so natural to apply it to families of binary forms with fixed leading coefficient

**Theorem (Bhargava, Shankar, and S., 2022)**

*Let $n \geq 4$ be even. Consider binary $n$-ic forms $f$ with fixed nonzero leading coefficient such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by "height," we have $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^* 6$.*

- Shows robustness of Poonen–Rains conjecture — average remains 6 even on thin families of curves with fixed leading coefficient
- Previously proven by Shankar and Wang (2018) for leading coefficient 1 (marked rational non-Weierstrass points at $\infty$)
- Analogous result proven by Bhargava and Gross (2013) for leading coefficient 0 (marked rational Weierstrass point at $\infty$)

# Main result: fixed leading coefficient

- Construction seems leading-coefficient dependent, so natural to apply it to families of binary forms with fixed leading coefficient

**Theorem (Bhargava, Shankar, and S., 2022)**

*Let $n \geq 4$ be even. Consider binary $n$-ic forms $f$ with fixed nonzero leading coefficient such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by "height," we have $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^* 6$.*

- Shows robustness of Poonen–Rains conjecture — average remains 6 even on thin families of curves with fixed leading coefficient
- Previously proven by Shankar and Wang (2018) for leading coefficient 1 (marked rational non-Weierstrass points at $\infty$)
- Analogous result proven by Bhargava and Gross (2013) for leading coefficient 0 (marked rational Weierstrass point at $\infty$)

# Main result: fixed leading coefficient

- Construction seems leading-coefficient dependent, so natural to apply it to families of binary forms with fixed leading coefficient

**Theorem (Bhargava, Shankar, and S., 2022)**

*Let $n \geq 4$ be even. Consider binary $n$-ic forms $f$ with fixed nonzero leading coefficient such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by "height," we have* $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^* 6$.

- Shows robustness of Poonen–Rains conjecture — average remains 6 even on thin families of curves with fixed leading coefficient
- Previously proven by Shankar and Wang (2018) for leading coefficient 1 (marked rational non-Weierstrass points at $\infty$)
- Analogous result proven by Bhargava and Gross (2013) for leading coefficient 0 (marked rational Weierstrass point at $\infty$)

# Main result: fixed leading coefficient

- Construction seems leading-coefficient dependent, so natural to apply it to families of binary forms with fixed leading coefficient

**Theorem (Bhargava, Shankar, and S., 2022)**

*Let $n \geq 4$ be even. Consider binary $n$-ic forms $f$ with fixed nonzero leading coefficient such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by "height," we have $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^* 6$.*

- Shows robustness of Poonen–Rains conjecture — average remains 6 even on thin families of curves with fixed leading coefficient
- Previously proven by Shankar and Wang (2018) for leading coefficient 1 (marked rational non-Weierstrass points at $\infty$)
- Analogous result proven by Bhargava and Gross (2013) for leading coefficient 0 (marked rational Weierstrass point at $\infty$)

# Main result: fixed leading coefficient

- Construction seems leading-coefficient dependent, so natural to apply it to families of binary forms with fixed leading coefficient

**Theorem (Bhargava, Shankar, and S., 2022)**

*Let $n \geq 4$ be even. Consider binary $n$-ic forms $f$ with fixed nonzero leading coefficient such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by "height," we have $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^* 6$.*

- Shows robustness of Poonen–Rains conjecture — average remains 6 even on thin families of curves with fixed leading coefficient
- Previously proven by Shankar and Wang (2018) for leading coefficient 1 (marked rational non-Weierstrass points at $\infty$)
- Analogous result proven by Bhargava and Gross (2013) for leading coefficient 0 (marked rational Weierstrass point at $\infty$)

# Varying the leading coefficient

- Goal: Compute $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all $f$ (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed $f_0$, and then simply sum over all possible values of $f_0$
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

# Varying the leading coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all $f$ (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed $f_0$, and then simply sum over all possible values of $f_0$
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

# Varying the leading coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all $f$ (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed $f_0$, and then simply sum over all possible values of $f_0$
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

# Varying the leading coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all $f$ (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed $f_0$, and then simply sum over all possible values of $f_0$
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i\{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

# Varying the leading coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all $f$ (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed $f_0$, and then simply sum over all possible values of $f_0$
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

# Varying the leading coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all $f$ (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed $f_0$, and then simply sum over all possible values of $f_0$
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i\{|f_0^{i-1} f_i|^{1/i}\}$$

  Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

# Varying the leading coefficient

- Goal: Compute Avg $\#\,\mathrm{Sel}_2(\mathrm{J}(C_f))$ over all $f$ (loc. sol. if $4 \mid n$)
- Naïve approach: Determine asymptotic count of Selmer elements for each fixed $f_0$, and then simply sum over all possible values of $f_0$
- Given $f_0 \in \mathbb{Z} \setminus \{0\}$, let $S_{f_0}(X) := \{f : \mathrm{H}^*(f) < X, f(1,0) = f_0\}$, where

$$\mathrm{H}^*(f) = \max_i \{|f_0^{i-1} f_i|^{1/i}\}$$

  Then we have

$$\sum_{f \in S_{f_0}(X)} \#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} + \text{error}$$

- Problem: natural height on binary forms is $\mathrm{H}(f) = \max_i\{|f_i|\}$
- $S_{f_0}(X) \not\approx \{f : \mathrm{H}(f) < X,\ f(1,0) = f_0\}$, unless $f_0 \asymp X$
- Turns out that contribution from $f_0 \not\asymp X$ is negligible

# Varying the leading coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \mathrm{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for $f_0$ close to $X$
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

# Varying the leading coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \mathrm{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for $f_0$ close to $X$
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

# Varying the leading coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \mathrm{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for $f_0$ close to $X$
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

# Varying the leading coefficient (cont'd.)

- Summing bound over $f_0 \asymp X$ and ignoring error term, we find that $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C_f)) \ll$

$$\frac{1}{\#\{f : \mathrm{H}(f) < X\}} \sum_{f_0 \asymp X} f_0^{-\frac{n(n-1)}{2}} X^{\frac{n(n+1)}{2}} \ll \frac{1}{X^{n+1}} \times X^{n+1} = 1$$

- Problem: Error term overtakes main term for $f_0$ close to $X$
- Multiple sources of error; worst is application of Davenport's Lemma: # of lattice points satisfying congruence conditions in a "round" region $\approx$ the volume of the region times the probability that the congruence conditions are satisfied

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \mathrm{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \dots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \operatorname{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4 / \mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \operatorname{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \mathrm{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4 / \mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \operatorname{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \operatorname{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \operatorname{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \operatorname{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

## Theorem (Bhargava, Shankar, S., 2021)

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \operatorname{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \operatorname{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

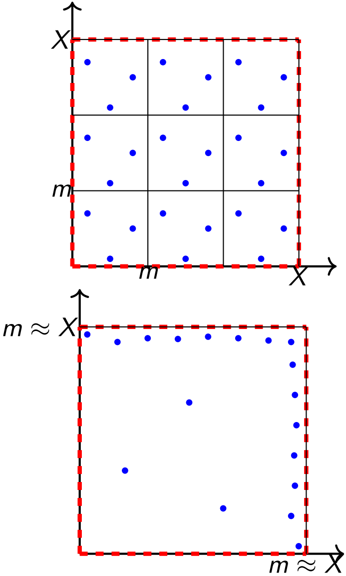
# Orbits of rk $\leq 1$ mod $f_0$

- To control error, need to understand image of parametrization better
- Recall that image *a priori* defined by congruence conditions mod $f_0^{n-1}$: $(A, B)$ arises if for each $i \in \{2, \ldots, n-1\}$ certain linear combinations of the $i \times i$ minors of $B$ vanish modulo $f_0^{i-1}$
- Helpful if image is defined mod $f_0$, rather than a higher power
- Say $B \in \mathrm{Sym}^2 \mathbb{Z}^n$ has rk $\leq 1$ mod $f_0$ if $B \propto (\text{linear form})^2 \pmod{f_0}$

**Theorem (Bhargava, Shankar, S., 2021)**

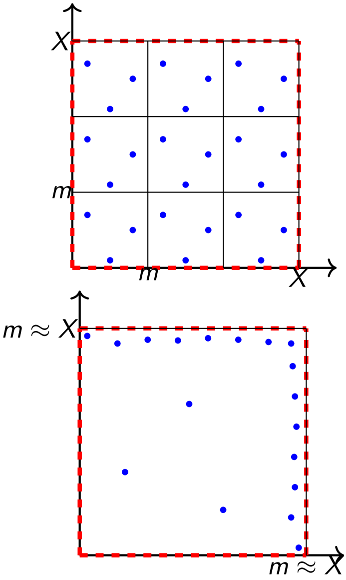
- *If $R_f = \mathcal{O}_{K_f}$ is the maximal order, or if first two coefficients of $f$ are coprime, then $B$ has rk $\leq 1$ mod $f_0$*
- *Let $n = 4$. If $(A, B)$ is not defined mod $f_0$, then $\exists$ $(\mathrm{SL}_4/\mu_2)(\mathbb{Q})$-translate $(A', B') \in \mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}_2 \mathbb{Z}^4$ such that $i \times i$ minors of $B'$ vanish modulo $f_0^{i-1}$ for each $i \in \{2, 3, 4\}$*

# Error from Davenport's lemma



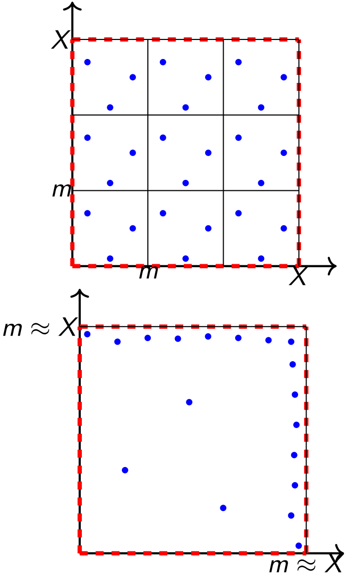

- Want to count lattice pts cut out by congruence conditions mod $m$ in box of sidelength $X$
- If $m/X$ is tiny, Davenport's lemma gives good estimate
- But *a priori*, orbits we want to count are defined by conditions mod $f_0$, and $f_0$ can be as big as $X$
- If $m \approx X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

# Error from Davenport's lemma



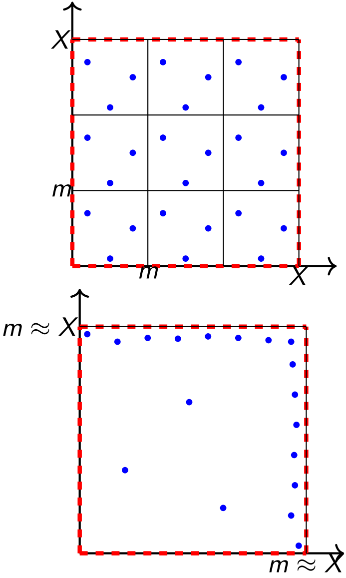

- Want to count lattice pts cut out by congruence conditions mod $m$ in box of sidelength $X$
- If $m/X$ is tiny, Davenport's lemma gives good estimate
- But *a priori*, orbits we want to count are defined by conditions mod $f_0$, and $f_0$ can be as big as $X$
- If $m \approx X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

# Error from Davenport's lemma



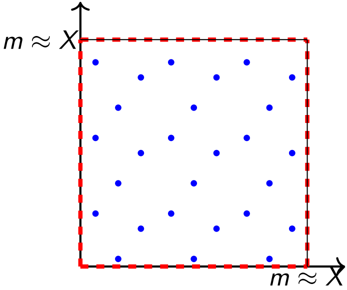

- Want to count lattice pts cut out by congruence conditions mod $m$ in box of sidelength $X$
- If $m/X$ is tiny, Davenport's lemma gives good estimate
- But *a priori*, orbits we want to count are defined by conditions mod $f_0$, and $f_0$ can be as big as $X$
- If $m \approx X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

# Error from Davenport's lemma




- Want to count lattice pts cut out by congruence conditions mod $m$ in box of sidelength $X$
- If $m/X$ is tiny, Davenport's lemma gives good estimate
- But *a priori*, orbits we want to count are defined by conditions mod $f_0$, and $f_0$ can be as big as $X$
- If $m \approx X$ and pts are sparse or concentrated near edges of box, error in Davenport's lemma will be huge

# Error from Davenport's lemma (cont'd.)

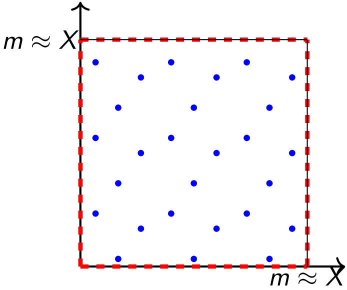



- Want to prove that orbits arising from construction are somewhat equidistributed in box, even when $m \approx f_0 \approx X$
- Let $\chi =$ indicator function mod $f_0$ of image of construction.

  proving pts somewhat equidistributed $\iff$ bounding $\sum_{B \neq 0} |\widehat{\chi}(B)|$

- Easy to show that mod prime $p$, e.g., we have $|\widehat{\chi}(B)| \ll p^{n - \frac{\operatorname{rk} B}{2}}$

# Error from Davenport's lemma (cont'd.)

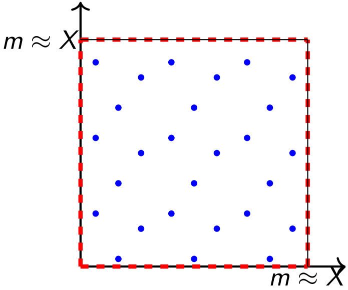



- Want to prove that orbits arising from construction are somewhat equidistributed in box, even when $m \approx f_0 \approx X$
- Let $\chi =$ indicator function mod $f_0$ of image of construction.

$$\text{proving pts somewhat equidistributed} \iff \text{bounding} \sum_{B \neq 0} |\widehat{\chi}(B)|$$

- Easy to show that mod prime $p$, e.g., we have $|\widehat{\chi}(B)| \ll p^{n - \frac{\text{rk}\, B}{2}}$

# Error from Davenport's lemma (cont'd.)

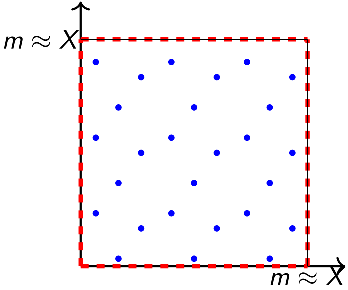



- Want to prove that orbits arising from construction are somewhat equidistributed in box, even when $m \approx f_0 \approx X$
- Let $\chi =$ indicator function mod $f_0$ of image of construction.

$$\text{proving pts somewhat equidistributed} \iff \text{bounding} \sum_{B \neq 0} |\widehat{\chi}(B)|$$

- Easy to show that mod prime $p$, e.g., we have $|\widehat{\chi}(B)| \ll p^{n - \frac{\text{rk}\, B}{2}}$

# Error from Davenport's lemma (cont'd.)




- Want to prove that orbits arising from construction are somewhat equidistributed in box, even when $m \approx f_0 \approx X$
- Let $\chi =$ indicator function mod $f_0$ of image of construction.

$$\text{proving pts somewhat equidistributed} \iff \text{bounding} \sum_{B \neq 0} |\widehat{\chi}(B)|$$

- Easy to show that mod prime $p$, e.g., we have $|\widehat{\chi}(B)| \ll p^{n - \frac{\mathrm{rk}\, B}{2}}$

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^{\star} 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0,1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J(C_f)) \leq^{*} 6$.

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^{\star} 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0,1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^{*} 6$.

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^\star 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0,1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J(C_f)) \leq^\star 6$.

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\operatorname{Avg} \# \operatorname{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^{\star} 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0,1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\operatorname{Avg} \# \operatorname{Sel}_2(J(C_f)) \leq^{*} 6$.

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^\star 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0,1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J(C_f)) \leq^* 6$.

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^{\star} 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^{\star} 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0, 1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J(C_f)) \leq^{*} 6$.

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^\star 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0,1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J(C_f)) \leq^* 6$.

# Main results: varying leading coefficient

**Theorem (Bhargava, Shankar, and S., 2021)**

*When binary quartic forms $f$ such that $C_f$ is loc. sol. are ordered by the max norm on their coefficients, we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(\mathrm{J}(C_f)) \leq^\star 6$.

- Family of curves $C_f$, where $f$ ranges over all binary quartic forms, has a lot of redundancies: If $f, f'$ are $\mathrm{PGL}_2(\mathbb{Q})$-equivalent, then $C_f \simeq C_{f'}$
- Average remains $\leq^\star 6$ even if quotient our family by the action of $\mathrm{PGL}_2(\mathbb{Q})$ (llows us to bound second moment of size of 2-Selmer group of elliptic curves!)

**Theorem (Bhargava, Laga, Shankar, and S., 2024)**

*Let $n \geq 6$ be even, and let $\varepsilon \in (0,1)$. Consider binary $n$-ic forms $f$ such that $C_f$ is loc. sol. if $n \equiv 0 \pmod 4$. When such $f$ are ordered by the max norm on their coefficients, there exists a density-$(1-\varepsilon)$ subset on which we have* $\mathrm{Avg}\,\#\,\mathrm{Sel}_2(J(C_f)) \leq^* 6$.

**Thank You!!**