Genus 2 Curves
With Several Points
Contained in an Arithmetic Progression

Michael Stoll
Universität Bayreuth

Arithmetic Geometry, Number Theory, and Computation

MIT

August 24, 2018

Preliminary Remarks

- This is an ongoing project
  and still somewhat rough around the edges.
- This talk is light on theorems and heavy on computational results.
- Everything is based on ideas of Noam Elkies from ca. 2000.

The Setting

Let C be a curve of genus 2, with (non-Weierstrass) points $P_1, \ldots, P_r$ in distinct orbits under the hyperelliptic involution ι.
We set $P_{-j} = \iota(P_j)$.

Then we can ask for all the points $P_{-r}, \ldots, P_{-1}, P_1, \ldots, P_r$ to be contained in an "arithmetic progression", in the sense that all differences $[P_j - P_k]$ are contained in a cyclic subgroup $\langle G \rangle$ of the Jacobian J of C.

There are then integers n_j, for $j \in R = \{-n_r, \ldots, -n_1, n_1, \ldots, n_r\}$, with $n_{-j} = -n_j$, such that

$$\forall j, k \in R: \qquad \frac{n_j - n_k}{\gamma} \cdot G = [P_j - P_k],$$

where γ is the gcd of all $n_j - n_k$ (and we choose $\langle G \rangle$ minimally).

We can normalize the n_j to be positive and coprime; then $\gamma = 1$ or $\gamma = 2$.

Some Observations

- The generator G is uniquely determined and can be represented by a divisor supported in the marked points.
- If $\gamma = 1$, then $P_0 = [P_j] - n_j \cdot G \in \mathrm{Pic}^1_C$ does not depend on j; P_0 is a theta characteristic and can be odd or even.
- In the odd case, P_0 is a Weierstrass point on C; in the even case, it corresponds to a $\{3, 3\}$-partition of the W. points.

This leads to three types of moduli spaces:

- $\mathcal{M}(0, n_1, \ldots, n_r)$ (with $\gamma = 1$, $P_0 \in C$; we include 0 in R)
- $\mathcal{M}(*, n_1, \ldots, n_r)$ (with $\gamma = 1$, $P_0 \notin C$)
- $\mathcal{M}(n_1, \ldots, n_r)$ (with $\gamma = 2 \iff$ all n_j odd)

We also write $\mathcal{M}(R)$ to denote any of these.

Why Interesting?

- Obviously interesting if you like genus 2 curves!
- Noam Elkies has looked at it (Oberwolfach 2001):

```
*32. N. ELKIES (15.15-16.00): Progress report on genus 2
[...]

A novel class of moduli problems.
[...]
```

  This talk got me started on the project.

- Can hope to find interesting (families of) genus 2 curves.
- Can hope to find interesting varieties among the moduli spaces. (But not in this talk!)

Admissibility

There is a necessary condition that R has to satisfy for $\mathcal{M}(R)$ to be non-empty.

A point $0 \neq Q \in J$ has a unique representation $Q = [P + P'] - K$, where K is the canonical class and $P, P' \in C$.

This implies that all non-zero sums $n + n'$ for $n, n' \in R$ have to be distinct.

Example. $\mathcal{M}(*, 1, 2, 4) = \emptyset$, since $4 - 2 = 1 + 1$.

We say that R is admissible if it satisfies this condition.

Expected Dimension

The moduli space $\mathcal{M}_{2,r}$ of genus 2 curves with r marked points has dimension $3 + r$.

Adding G to the data, we have dimension $r + 5$.

The points have to satisfy r relations in the Jacobian, so we expect

$$\dim \mathcal{M}(R) = r + 5 - 2r = 5 - r\,.$$

In any case, this consideration shows that either $\mathcal{M}(R)$ is empty, or else $\dim \mathcal{M}(R) \geq 5 - r$.

Computations

- NDE did some computations ca. 2000 (see his Oberwolfach talk).
- I did similar computations after learning about his.
- My student Andreas Kühn computed many $\mathcal{M}(R)$'s in the early 2010s.
- Recently, I picked this up again and computed even more $\mathcal{M}(R)$'s (using a compute cluster in Bayreuth).

Main Methods:

- Deduce low-weight relations supported on the P_j, set up a system of algebraic equations and solve using Gröbner bases.
- Use forgetful maps $\mathcal{M}(R) \to \mathcal{M}(R')$ (where $R' \subsetneq R$), when $\mathcal{M}(R')$ has already been computed.

Example 1

For $\mathcal{M}(*, 1, 2, 7)$, we have relations

$$3P_1 + 2P_2 + P_{-3} \sim 4P_1 + 2P_{-2} \sim 3K$$

where K is the canonical divisor $\infty_+ + \infty_-$.

We set $C\colon y^2 = x^6 + f_5 x^5 + \ldots + f_0$ with $P_1 = \infty_+$, $P_2 = (0, y_2)$ and $P_3 = (1, y_3)$.

The relations imply the existence of cubics $h_1(x), h_2(x)$ such that

$$\operatorname{div}(y - h_1(x)) = 3P_1 + 2P_2 + P_{-3} - 3K \quad \text{and} \quad \operatorname{div}(y - h_2(x)) = 4P_1 + 2P_{-2} - 3K\,.$$

This translates into equations that are linear in the coefficients of h_i.
Elimination leaves us with equations in $f_0, \ldots, f_5, y_2, y_3$.
Setting $u = y_2$ and $v = -y_3 - y_2 - 1$, this gives $\mathcal{M}(*, 1, 2, 7)$
as a subset of the affine plane, with universal curve

$$C_{*,1,2,7}\colon y^2 = x^6 + 2vx^5 + v^2x^4 - 2ux^3 + 2u(v+2)x^2 + u^2$$

and points $P_1 = \infty_+$, $P_2 = (0, u)$, $P_3 = (1, -u - v - 1)$.

Example 2

To compute $\mathcal{M}(*, 1, 2, 7, 14)$, we use that $\mathcal{M}(*, 1, 2, 7, 14) \hookrightarrow \mathcal{M}(*, 1, 2, 7)$.

We have that $G = [P_2 - P_1]$ in the Jacobian of $C_{*,1,2,7}$; we compute

$$7G = \left(x^2 + (v+1)x + u, (u+v+1)x\right).$$

We want $7G = [P_4 - P_3]$ for some $P_4 = (x_4, y_4) \in C$. This means that

$$x^2 + (v+1)x + u = (x-1)(x-x_4) \quad \text{and} \quad y_4 = (u+v+1)x_4\,,$$

leading to $\qquad u + v + 2 = 0 \qquad$ with $\qquad x_4 = u \qquad$ and $\qquad y_4 = -u$.

So $\mathcal{M}(*, 1, 2, 7, 14)$ is an open subset of the affine line,

$$C_{*,1,2,7,14} \colon y^2 = x^6 - 2(u+2)x^5 + (u+2)^2 x^4 - 2ux^3 - 2u^2x^2 + u^2\,,$$

and $P_1 = \infty_+$, $P_2 = (0, u)$, $P_3 = (1, 1)$, $P_4 = (u, -u)$.

$r = 3$

We computed > 30 $r = 3$ moduli spaces with their universal curves.
They are all rational surfaces.

Still, we formulate the following expectation ($\#R = 6$ or 7):

- If R is admissible, then $\dim \mathcal{M}(R) = 2$ and $\mathcal{M}(R)$ is geometrically irreducible.
- $\mathcal{M}(R)$ is rational (or Fano) for finitely many R.
- $\mathcal{M}(R)$ is of general type for all but finitely many R.

$r = 4$

We computed many (> 1500) $r = 4$ moduli spaces
(and their universal curves in most cases when $\mathcal{M}(R) \subset \mathbb{P}^1$).
Some unexpected phenomena occur.

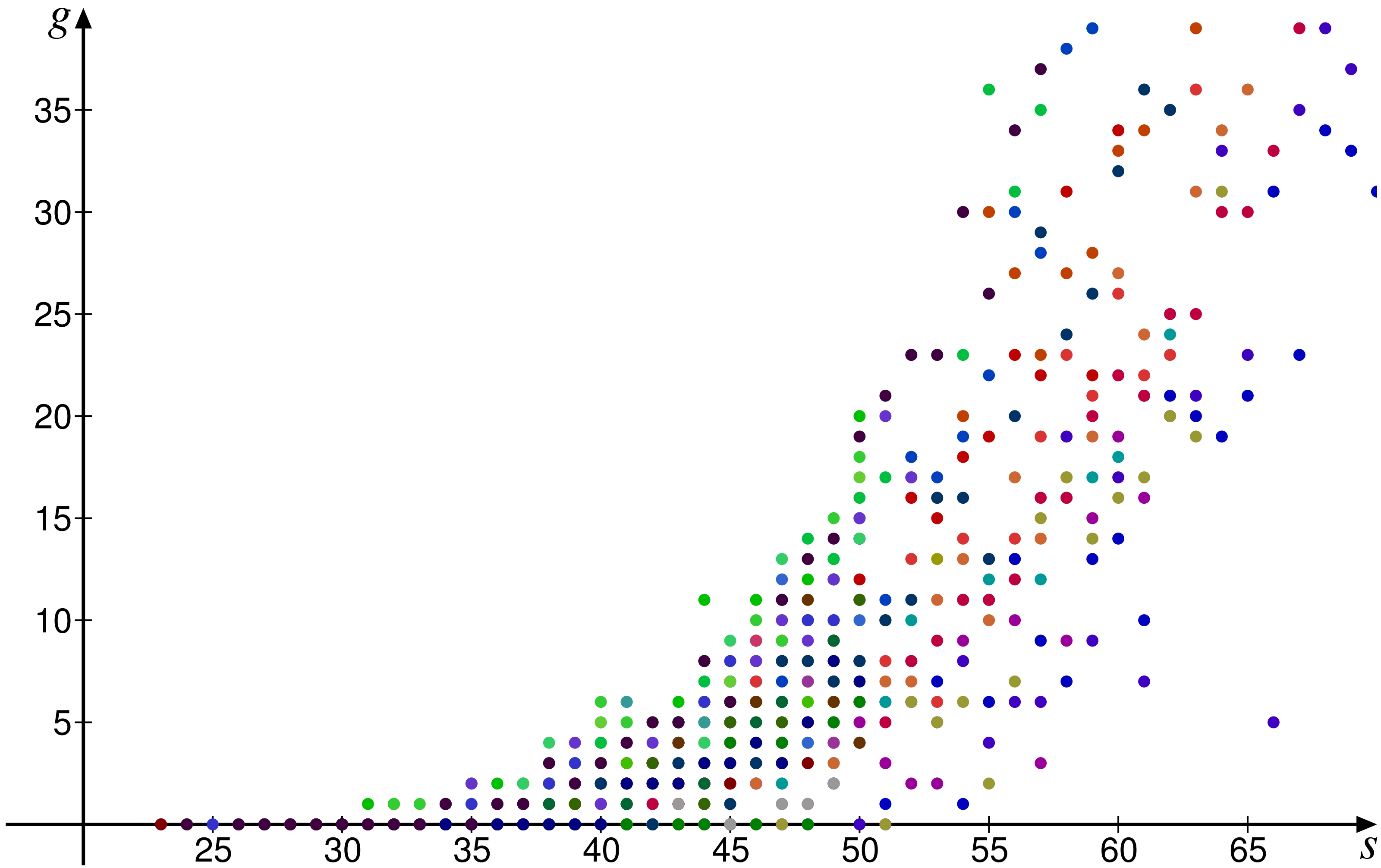
- We found four empty $\mathcal{M}(R)$ with R admissible:
$\mathcal{M}(0, 4, 6, 7, 26)$, $\mathcal{M}(0, 4, 6, 9, 26)$, $\mathcal{M}(*, 1, 5, 8, 13)$, $\mathcal{M}(*, 2, 4, 5, 16)$.
- We found nine $\mathcal{M}(R)$ that have actually $r = 5$:
$\mathcal{M}(0, 1, 9, 12, 16, 39)$, $\mathcal{M}(0, 7, 9, 12, 13, 48)$, $\mathcal{M}(0, 3, 11, 12, 16, 45)$,
$\mathcal{M}(0, 7, 8, 13, 17, 48)$, $\mathcal{M}(0, 3, 12, 16, 17, 39)$, $\mathcal{M}(*, 2, 5, 10, 11, 37)$,
$\mathcal{M}(7, 11, 17, 19, 61)$, $\mathcal{M}(1, 13, 17, 23, 55)$, $\mathcal{M}(1, 13, 19, 23, 71)$.
- If non-empty, the smooth projective model of $\mathcal{M}(R)$ is either
$\mathbb{P}^1$, several (2–4) $\mathbb{P}^1$'s permuted transitively by Galois,
an elliptic curve, or a nice curve of genus ≥ 2.

Conjectures for $r = 4$

Based on the data, we conjecture the following for admissible R ($\#R = 8$ or 9).

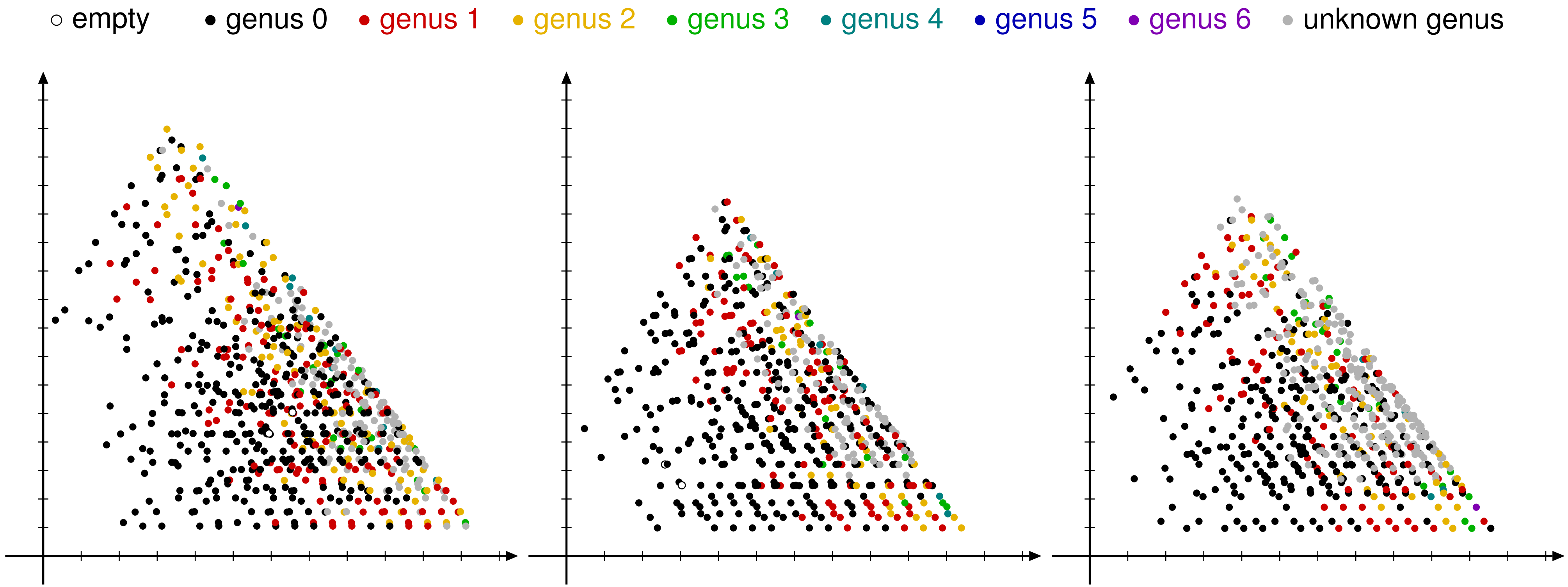
- The smooth projective model of $\mathcal{M}(R)$ is one of the following: (1) empty, (2) $\mathbb{P}^1$, (3) several conjugate $\mathbb{P}^1$'s, (4) an elliptic curve, or (5) a nice curve with $g \geq 2$.
- Each of the first four possibilities occurs finitely many times.
- For each $g \geq 2$, there are finitely many R such that $\mathcal{M}(R)$ has genus g.

Some Evidence



$s = (n_1 + \ldots + n_4)/\gamma$, $g = \text{genus}(\mathcal{M}(R))$, 33 families with fixed (n_1, n_2, n_3).

More Evidence



Projections of genus data for

$\mathcal{M}(0, n_1, \ldots, n_4)$ (left), $\mathcal{M}(*, n_1, \ldots, n_4)$ (middle), $\mathcal{M}(n_1, \ldots, n_4)$ (odd) (right).

$r = 5$

We computed lots ($> 100\,000$) of $r = 5$ moduli spaces
(and their associated curves).

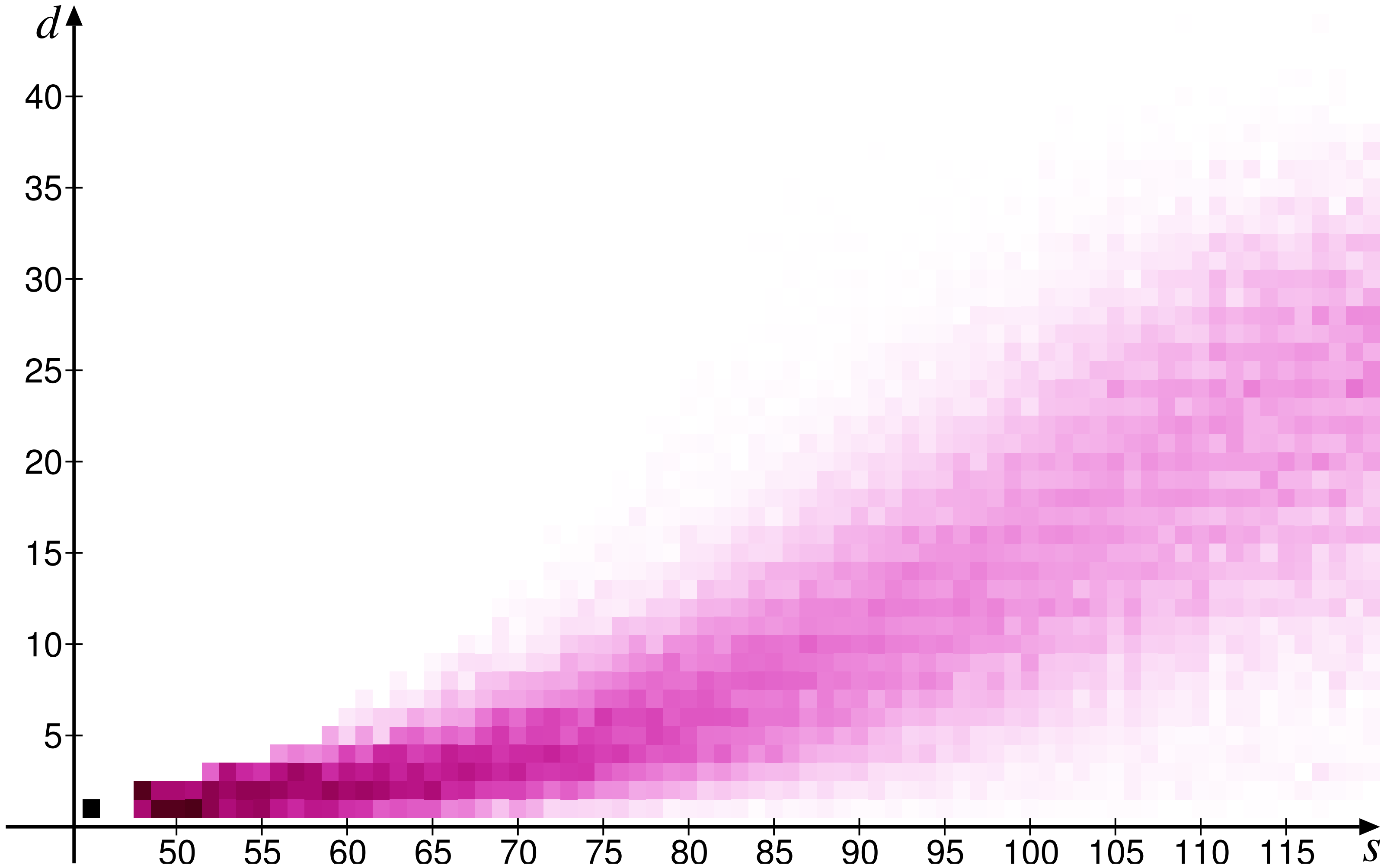
Conjecture for $\#R = 10$ or 11.

- With finitely many exceptions, $\mathcal{M}(R)$ is empty or of dimension 0.
- For fixed degree d, among the non-exceptional $\mathcal{M}(R)$,
  there are only finitely many irreducible components of degree d.
- Among the non-exceptional $\mathcal{M}(R)$,
  there are only finitely many components that extend to larger R
  (plus a similar statement for the exceptional ones).

This would imply an upper bound for $\#R$ such that $\mathcal{M}(R) \neq \emptyset$.

Over $\mathbb{Q}$, the maximum we found is 15 (twice);
the overall maximum is 17 for $R = \{0, \pm 4, \pm 5, \pm 16, \pm 23, \pm 29, \pm 59, \pm 76, \pm 90\}$.

Evidence



Relative distribution of component degrees d when $n_1 + \ldots + n_5 = s$, for $\mathcal{M}(*, n_1, n_2, n_3, n_4, n_5)$.

Small Canonical Height

Heuristic.

If $G \in J$ has small (positive) canonical height $\hat{h}(G)$,
then for many multiples $nG = (a_n x^2 + b_n x + c_n, \dots)$,
the coefficients a_n, b_n, c_n will be small,
and so the quadratic is likely to split;
then $nG = [P - P']$, and we get points with difference in $\langle G \rangle$.

So we expect the associated curves to show up in $\mathcal{M}(R)$
with (reasonably) large R.

In this way, we (hope to) find examples of curves over $\mathbb{Q}$ and over $\mathbb{Q}(t)$
with points on J of particularly small canonical height.

Small Height Examples

Over $\mathbb{Q}$, the record small height is obtained from

$$C_{*,3,19,20,29,31,44,49}: \quad y^2 = 25x^6 + 20x^5 - 76x^4 - 134x^3 + 124x^2 + 96x + 9$$

with $\hat{h}(G) = 0.00029824708304560637074732219128$.

Over a number field, the best so far is over $K = \mathbb{Q}(\zeta_{12})$:
$C_{0,4,5,16,23,29,59,76,90}$ gives $\hat{h}(G) \approx 0.0001913$.

Over $\mathbb{Q}(t)$, our record example is

$$\begin{aligned} C_{*,1,6,9,15}: \quad y^2 &= 9(4t+1)^2x^6 - 24(4t+1)(t+2)x^4 - 48(4t+1)(t-1)x^3 \\ &\quad + 16(t-2)^2x^2 + 64(t+1)(t-2)x + 64(t+1)^2 \end{aligned}$$

with $\hat{h}(G) = \frac{1}{840}$.

Torsion

A similar argument applies when G is torsion (i.e., $\hat{h}(G) = 0$).
We can add the condition $nG = 0$; this reduces the dimension by 2.

We indeed find examples for all known torsion orders > 20 over $\mathbb{Q}$
except 45, 60 and 63,
but (unfortunately) no examples with new torsion orders.

We do find orders 31, 37, 47 over quadratic fields
and 41 over cubic fields.

Torsion Examples

$\mathcal{M}(*, 3, 14, 18, 26, 27)$: The curve

$$y^2 = 4x^6 + 12x^5 + 13x^4 + 6x^3 + 7x^2 + 6x + 9$$

has $J(\mathbb{Q}) = \langle G \rangle = \mathbb{Z}/30\mathbb{Z}$.
Over $\mathbb{Q}(\sqrt{5})$, G is divisible by 4, and $J(\mathbb{Q}(\sqrt{5})) = \mathbb{Z}/120\mathbb{Z}$.

$\mathcal{M}(*, 2, 4, 5, 19, 32, 58)$ gives a pair of curves over $K = \mathbb{Q}(\sqrt{3})$ with a point of order 168 in $J(K)$.

$\mathcal{M}(*, 12, 14, 15, 28, 49, 66)$: The curve

$$y^2 = 4x^6 - 12x^5 - 3x^4 + 46x^3 - 15x^2 - 24x + 40$$

has $J(\mathbb{Q}) = \mathbb{Z}/27\mathbb{Z}$.
Over $\mathbb{Q}(\zeta_9)^+$, it acquires a point of order 7, so that $J(\mathbb{Q}(\zeta_9)^+) = \mathbb{Z}/189\mathbb{Z}$.

Thank You!