Two-cover descent on plane quartics with rational bitangents

Nils Bruin (Simon Fraser University) and
Daniel Lewis (University of Arizona)

Fourteenth Algorithmic Number Theory Symposium, ANTS-XIV,
University of Auckland, New Zealand
June 29 - July 4, 2020

Overview

Quick overview for experts;

Motivation and details in rest of presentation.

Main contribution: A practical method to decide if certain smooth plane quartics have rational points.

Restriction: *Certain* means all 28 bitangents rational

Examples: We use del Pezzo surfaces of degree 2 to generate plenty of examples

Success rate: Our method is successful on a sample of 150000 test cases. We expect failures do occur, although very rarely.

Bonus material

- Information on the Mordell-Weil groups of the Jacobians of these curves
- In particular, on their two-Selmer groups.
- Poonen-Rains (2012) heuristics: well-matched if shifted.
- Jacobians very often have an everywhere locally trivial torsor representing Pic^1.

Rational points on curves

Projective plane curve over a field k:

$$C : f(x, y, z) = 0$$

with $f \in k[x, y, z]$ irreducible homogeneous of degree d.

Rational point: $(x_0 : y_0 : z_0) \in C(k)$, with $f(x_0, y_0, z_0) = 0$.

Solvability: A curve is called *solvable* if $C(k) \neq \emptyset$. Examples:

- $C_{-1,1} : x^2 + y^2 - z^2 = 0$ ✓
- $C_{-1,-1} : x^2 + y^2 + z^2 = 0$ ✗
- $C_{-1,3} : x^2 + y^2 - 3z^2 = 0$ ✗

Proving solvability over number fields: Enumerate $(x_0, y_0, z_0) \in k^3$ until $f(x_0, y_0, z_0) = 0$.

Proving insolvability: Sometimes $C(\mathbb{R}) = \emptyset$ or $C(\mathbb{Q}_p) = \emptyset$.
Then $C(\mathbb{Q}) = \emptyset$ as well, since $\mathbb{Q} \subset \mathbb{R}$ and $\mathbb{Q} \subset \mathbb{Q}_p$.

Obstructions

Let C be a curve over a number field k.

Local obstruction: C has a *local obstruction* to having rational points if $C(k_v) = \emptyset$ for some completion k_v of k.

Insufficiency: For curves of degree $d \geq 3$, one may have $C(k) = \emptyset$ without having local obstructions:

$$3x^3 + 4y^3 + 5z^3 = 0 \text{ [Selmer, 1951]}$$

Chevalley–Weil: If $\phi\colon D \to C$ is an unramified cover then one can determine a *finite collection of twists* such that

$$\bigcup \phi_\xi(D_\xi(k)) = C(k)$$

Selmer set:

$$\mathrm{Sel}^{(\phi)}(C/k) = \{\xi \in \mathrm{Twists}(D/C) : D_\xi(k_v) \neq \emptyset \text{ for all } v\}$$

Observation: We can have $\mathrm{Sel}^{(\phi)}(C/k) = \emptyset$ even if $C(k_v) \neq \emptyset$ for all v.

Explicit Selmer set example

Example. The following (genus 1) curve has no local obstructions:

$$C\colon y^2 = 22x^4 + 65x^2 + 48 = (2x^2 + 3)(11x^2 + 16)$$

Construct a cover:

$$D_\xi = \begin{cases} 2x^2 + 3 = \xi y_1^2 \\ 11x^2 + 16 = \xi y_2^2 \\ y = \xi y_1 y_2 \end{cases}$$

- Careful consideration: WLOG $\xi \in \{1, 2\}$
- For each ξ we have $D_\xi(\mathbb{Q}_p) = \emptyset$ for some p.

Conclusion: $\mathrm{Sel}^{(\phi)}(C/\mathbb{Q}) = \emptyset$, but $C(\mathbb{Q}_v) \neq \emptyset$ for all v.

2-Selmer sets for hyperelliptic curves

Two-cover: Given a curve C of genus g, A *two-cover* is an unramified cover

$$\phi\colon D \longrightarrow C \text{ with } \mathrm{Aut}_{\bar{k}}(D/C) \simeq (\mathbb{Z}/2\mathbb{Z})^{2g}.$$

Hyperelliptic curve: $C\colon y^2 = f(x)$, with $\deg(f) = 2g + 2$.

Local solvability: [Poonen–Stoll, 1999] Most hyperelliptic curves have points everywhere locally.

Two-cover descent: [B.–Stoll, 2009] Efficient method for computing $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$.

Easy case: Rational Weierstrass points

$$C\colon y^2 = c(x - a_1)\cdots(x - a_{2g+2})$$

But then $(a_i, 0) \in C(k)$!

Average results: [Bhargava–Gross–Wang, 2017] Most hyperelliptic curves have $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$.

Question: How do these results generalize to non-hyperelliptic curves?

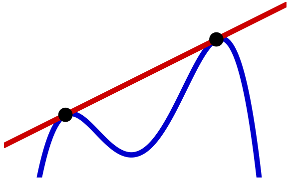
Plane quartic curves

Plane quartic: Non-hyperelliptic genus 3 curve:

$$C : f(x, y, z) = 0 \text{ smooth with } f \text{ homogeneous of degree } 4$$

Analogue of Weierstrass point: Bitangent line $\ell(x, y, z) = 0$.

- If ℓ is defined over k, contact points can still be quadratic!
- Quotient of bitangent lines $f = \ell_1/\ell_2$ yields function with $\mathrm{div}(f) \in 2\,\mathrm{Div}(C)$.
- Adjoining $\sqrt{f}$ yields an unramified cover $D \to C$.



Bitangent count: A smooth plane quartic has 28 bitangents

Relations: The 378 quotients have relations: adjoining all square roots yields an unramified cover of degree 2^6; a two-cover.

Description: If all 28 bitangents are defined over k, we get a good description of a two-cover $D \to C$ and its twists: gives an avenue to computing $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$.

Constructing examples

Degree 2 del Pezzo surfaces: two geometric descriptions:

- Blow-up of $\mathbb{P}^2$ in seven points $P_1, \dots, P_7$ in general position
- Double cover of $\mathbb{P}^2$ branched over a smooth plane quartic C

Relation with bitangents: If $P_1, \dots, P_7 \in \mathbb{P}^2(k)$, then bitangents of C are defined over k. Normalize points:

$$\begin{pmatrix} | & & | \\ P_1 & \cdots & P_7 \\ | & & | \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 & u_1 & u_2 & u_3 \\ 0 & 1 & 0 & 1 & v_1 & v_2 & v_3 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Amusing proposition: Over $\mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$ no such configurations exist. Over $\mathbb{F}_{11}$, only one isomorphism class occurs:

$$C_{11} : x^4 + y^4 + z^4 + x^2y^2 + x^2z^2 + y^2z^2 = 0, \text{ and } C_{11}(\mathbb{F}_{11}) = \emptyset.$$

Corollary: Every locally solvable example over $\mathbb{Q}$ has bad reduction at $3, 5, 7, 11$.

Example

$$\begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix} = \begin{pmatrix} 17 & -7 & -9 \\ 35 & 3 & 9 \end{pmatrix}.$$

We find

$$\begin{aligned} C\colon 9x^4 - 60x^3y + 357x^2y^2 + 246xy^3 + 16y^4 - 42x^3z + 259x^2yz - 168xy^2z \\ - 141y^3z + 31x^2z^2 - 492xyz^2 + 207y^2z^2 + 42xz^3 - 27yz^3 + 9z^4 = 0 \end{aligned}$$

- Discriminant $D_{27}(C) = 2^{34} \cdot 3^{20} \cdot 5^{10} \cdot 7^8 \cdot 11^2 \cdot 13^6 \cdot 17^4 \cdot 19^4 \cdot 29^2 \cdot 37^2 \cdot 41^2$.
- $C(\mathbb{Q}_v) \neq \emptyset$ for all places v
- Initial $\mathbb{F}_2$-vector space containing $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$ of dimension 72.
- Using linear algebra, reduced to dimension 9.
- Can prove $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$ by checking $D_\xi(\mathbb{Q}_p) = \emptyset$ for some $p \in \{2, 3, 5\}$ for each of the 2^9 values of ξ.

Systematic samples

A. $(u_1, \ldots, v_3) \in \{-6, \ldots, 6\}$ with $u_1 < u_2 < u_3$ and $u_1 < v_1$.

81070 configurations in general position; 33471 distinct discriminants.

B. $u_1, \ldots, v_3$ uniformly randomly chosen from $\{-40, \ldots, 40\}$

70000 curves; all with distinct discriminant values.

	$C(\mathbb{Q}_v) = \emptyset$	$\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$	rational bitangent contact point	other rational point	total
A	3654	42477	34025	4568	81070
	4.5%	52%	42%	5.6%	100%
B	521	63926	4830	1244	70000
	0.7%	91%	6.9%	1.8%	100%

- We were able to decide $C(\mathbb{Q}) = \emptyset$ or $C(\mathbb{Q}) \neq \emptyset$ in all cases.
- Only found local obstructions for $p = 2, 11$, and only when C has good reduction there.

BONUS: Selmer rank information

For a significant proportion of the curves in samples **A** and **B**, our information allows us to compute $\mathrm{Sel}^2(\mathrm{Jac}_C/\mathbb{Q})$ as well.

Prevalence of $\dim_2 \mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q})$

	6	7	8	9	10	11	12	13	
A	0.05%	18.7%	39.4%	29.1%	10.1%	2.28%	0.29%	0.006%	$(n = 31990)$
B	0	20.2%	41.8%	27.9%	8.71%	1.27%	0.10%	0.006%	$(n = 51685)$

Poonen–Rains (2012):

$$\mathrm{Prob}\Big(\dim_2 \mathrm{Sel}^{(2)}(\mathrm{Jac}_C/\mathbb{Q}) = c + d\Big) \sim \prod_{j=0}^{\infty} \frac{1}{1+2^{-j}} \cdot \prod_{j=1}^{d} \frac{2}{2^j - 1}$$

One should definitely expect $c = \dim_2 \mathrm{Jac}_C[2](\mathbb{Q}) = 6$, but we find an extra shift by 1

Observation: C has points everywhere locally, so $\mathrm{Pic}^1(C/\mathbb{Q}_v) \neq \emptyset$. The representing scheme provides an everywhere locally trivial Jac_C-torsor.