Arithmetic applications of Prym varieties in low genus

Nils Bruin (Simon Fraser University),

Tübingen, September 28, 2018

SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

Background: classifying rational point sets of curves

Typical arithmetic geometry problem:
Difference in point sets:

$$x^2 + y^2 = 1$$

$$x^2 + y^2 = -1$$

$$x^2 + y^2 = 5$$

$$x^2 + y^2 = 3$$

Topological trichotomy for point sets of curves:
Let C be smooth projective curve over a number field k (e.g. $k = \mathbb{Q}$). As a simple case: $C \subset \mathbb{P}^2$ of degree d.

d	genus	point set
≤ 2	0	$C(k) = \emptyset$ or $C \sim \mathbb{P}^1$
$= 3$	1	$C(k) = \emptyset$ or $C(k)$ is a finitely generated abelian group (Mordell-Weil)
≥ 4	> 1	$C(k)$ is a finite (Faltings)

Explicit computational question; elementary approaches

Explicit computational/theoretical problem: Given a projective, nonsingular curve C over a number field k, determine its set of k-rational points.

Basic observation I: local obstructions

If for a metric completion k_v of k (for $k = \mathbb{Q}$, this means $k_v = \mathbb{Q}_p$ or $k_v = \mathbb{R}$) we have $C(k_v) = \emptyset$, then we say that C has a *local obstruction* to having rational points:

$$C(k) \subset C(k_v) \text{ means } C(k_v) = \emptyset \implies C(k) = \emptyset$$

Basic observation II: *going down*

If $\phi : C \to D$ is a finite cover of curves over k, then $\phi(C(k)) \subset D(k)$, so if $D(k)$ is known and finite then $C(k) \subset \phi^{-1}(D(k))$ is easily computed.

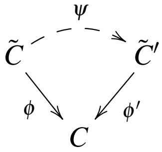
Example:

$$\begin{array}{ccc} C : y^2 = x^6 - 4x^4 + 16 & \to & D : y^2 = u^3 - 4u^2 + 16 \\ (x,y) & \mapsto & (x^2,y) = (u,y) \end{array}$$

$$D(\mathbb{Q}) = \{(0,\pm 4),(4,\pm 4),\infty\}, \text{ so } C(\mathbb{Q}) = \{(0,\pm 4),(\pm 2,\pm 4),\infty^{\pm}\}$$

Chevalley-Weil (Going up)

Definition: Let $\phi\colon \tilde{C} \to C$ and $\phi'\colon \tilde{C}' \to C$ be covers of projective curves over k. We say ϕ, ϕ' are *twists* if there is an isomorphism $\psi\colon \tilde{C} \to \tilde{C}'$ over k^{sep} such that $\phi = \phi' \circ \psi$:



Chevalley-Weil: *going up*

If $\phi\colon \tilde{C} \to C$ is unramified then there is a *finite* collection Σ of twists such that

$$\bigcup_{\xi \in \Sigma} \phi_\xi(\tilde{C}_\xi(k)) = C(k)$$

Key fact: The curves $\tilde{C}_\xi$ may be amenable to other approaches (such as local obstructions and going down).

Explicit unramified covers

Reminder: A curve is *hyperelliptic* if it admits a degree 2 map to a genus 0 curve. If it does not have a local obstruction, then it admits a model:

$$C\colon y^2 = f(x)$$

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:

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

- Careful consideration: WLOG $\xi \in \{1, 2, 3, 6, 11, 22, 33, 66\}$
- For each ξ we have $\tilde{C}_\xi(\mathbb{Q}_p) = \emptyset$ for some p.

General results

Two-covers (B.-Stoll, 2009): For hyperelliptic curves $C\colon y^2 = f(x)$ of genus g, there are two-covers for which the Chevalley-Weil set Σ is explicitly computable.

Theorem (Poonen-Stoll, 1999): Most hyperelliptic curves $y^2 = f(x)$ over $\mathbb{Q}$ do not have local obstructions.

Theorem (Bhargava, 2013): Most hyperelliptic curves over $\mathbb{Q}$ have only two-covers that have local obstructions.

Theorem (Bogomolov-Tschinkel, 2002): Any hyperelliptic curve admits an unramified cover $\tilde{C}$ that (over k^{sep}) covers $C_0\colon y^2 = x^6 + 1$.

Corollary: If for any number field L, you can compute $C_0(L)$ then, via going-up and going-down, you can compute the rational points on any hyperelliptic curve.

Subvarieties of Abelian varieties

Advanced: Determine $C(k)$ via embedding $C \hookrightarrow A$ into an Abelian variety A.

Obstruction to embedding: Note that $C(k) \subset \mathrm{Pic}^1(C/k)$, so either $C(k) = \emptyset$ or there is a $\mathfrak{d} \in \mathrm{Pic}^1(C/k)$:

$$C \hookrightarrow \mathrm{Jac}(C);\ \ P \mapsto [P] - \mathfrak{d}$$

Theorem (Mordell-Weil): $A(k)$ is finitely generated.

Chabauty's method: If $\mathrm{rk} A(k) = r < \dim(A)$:

$$\begin{array}{ccccc} C(k) & \longrightarrow & A(k) & \longrightarrow & \overline{A(k)} \\ \downarrow & & & & \downarrow \\ C(k_v) & & \longrightarrow & & A(k_v) \end{array}$$

v-adic analytic intersection:

$$C(k) \subset C(k_v) \cap \overline{A(k)}$$

- Higher dimension of A allows for larger r
- Lower dimension of A makes computation easier.
- If $A = \mathrm{Jac}(X)$, computing is easier still.

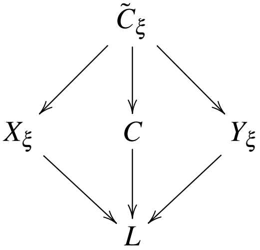
Prym varieties

Let C be of genus g and let $\phi : \tilde{C} \to C$ be an unramified double cover. Then $\ker(\phi_* : \mathrm{Jac}(\tilde{C}) \to \mathrm{Jac}(C))$ is of dimension $g-1$ and has two components.

Definition: $\mathrm{Prym}(\tilde{C}/C)$ is the maximal connected subgroup of $\ker \phi_*$.

Proposition: The principal polarization of $\mathrm{Jac}(\tilde{C})$ induces one on $\mathrm{Prym}(\tilde{C}/C)$.

Example (Hyperelliptic curves):



$C : y^2 = f_1(x) f_2(x)$ where $\deg(f_1), \deg(f_2)$ are even

$X_\xi : y_1^2 = \xi f_1(x)$

$Y_\xi : y_1^2 = \xi f_2(x)$

$\tilde{C}_\xi = X_\xi \times_L Y_\xi$

Description of Prym variety: $\mathrm{Prym}(\tilde{C}_\xi / C) = \mathrm{Jac}(X_\xi) \times \mathrm{Jac}(Y_\xi)$

Prym varieties as Jacobians

- As we have seen, Prym varieties of hyperelliptic curves can be described in terms of Jacobians. The cover $\tilde{C}$ maps to those curves.
- For C of genus 3, $\dim \mathrm{Prym}(\tilde{C}/C) = 2$. These are all Jacobians.
- For C of genus 4, $\dim \mathrm{Prym}(\tilde{C}/C) = 3$. These are *twists* of Jacobians.
- For C of genus ≥ 5 we do not expect $\mathrm{Prym}(\tilde{C}/C)$ to be a Jacobian.

Big question: For sufficiently general non-hyperelliptic C of genus $3, 4$ we have $\mathrm{Prym}(\tilde{C}/C) = \mathrm{Jac}(X)$ for some curve X (for a specific twist of $\tilde{C}$ for genus 4).

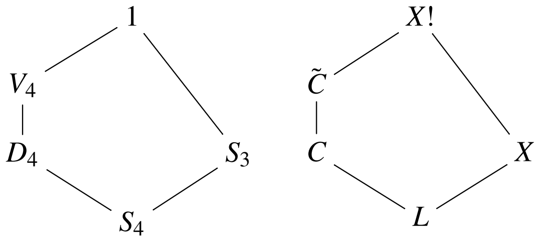
How do we construct this *Prym curve* X?

Description of canonical models of curves:

- Nonhyperelliptic genus 3 curve is a smooth plane quartic.
- Nonhyperelliptic genus 4 is an intersection of a quadric Q and a cubic Γ in $\mathbb{P}^3$.

Trigonal construction – Recillas

Galois theory:



Theorem: $\mathrm{Jac}(X) = \mathrm{Prym}(\tilde{C}/C)$, so Jacobians of tetragonal curves are Pryms.

In the opposite direction: Let $C \to L$ be trigonal; let $\tilde{C} \to C$ be an unramified double cover.

- Galois closure $\tilde{C}!$ of $\tilde{C} \to L$ generically has group $(C_2)^3 \rtimes S_3 = C_2 \times S_4$;
- Center interchanges geometric components.

Theorem: Given C trigonal and $\tilde{C} \to C$ unramified of degree 2, then there is a *twist* such that $\mathrm{Prym}(\tilde{C}/C) = \mathrm{Jac}(X)$.

Double covers of smooth plane quartics

Smooth plane quartic:

$$C\colon Q_1(x,y,z)Q_3(x,y,z) = Q_2(x,y,z)^2$$

Double cover:

$$\tilde{C}\colon \begin{cases} Q_1(x,y,z) = u^2 \\ Q_2(x,y,z) = uv \\ Q_3(x,y,z) = v^2 \end{cases}$$

Special divisor classes

$$X \subset W_4^1 \subset \mathrm{Pic}^4(\tilde{C})$$

Model:

$$X\colon t^2 = -\det(Q_1 + 2sQ_2 + s^2Q_3)$$

Mapping $\tilde{C}$ into the Prym

Given $\phi^* \colon \tilde{C} \to C$ unramified double cover of a genus 3 curve:

$$\begin{array}{ccc} \tilde{C} & \xrightarrow{2(\phi_* - \mathrm{id}_*)} & \mathrm{Jac}(X) \\ \downarrow & & \downarrow \\ C & \longrightarrow & \mathrm{Jac}(X)/\langle -1 \rangle \end{array}$$

Gives C as a subvariety of a Kummer surface, with the rational points of $\tilde{C}$ lifting to $\mathrm{Jac}(X)$. Gives C as an intersection of two quartic equations.

Example: $C : (2z^2 - 2x^2 - 2yz)(x^2 + 2xy + 2y^2) = (z^2 - x^2 + xz - 2yz)^2$ has $C(\mathbb{Q}) = \{(0:1:0)\}$.

Example: $C\colon (y^2 + yz - z^2)(z^2 + xy) = (x^2 - y^2 - z^2)^2$ has no local obstructions and yet, no rational points. The same holds for $\tilde{C}$.

Corollary: Every sextic polynomial can be expressed as $\det(M_0 + 2xM_1 + x^2M_2)$, where the M_i are 3×3 symmetric matrices (i.e., every $\mathrm{Jac}(X)$ is a Prym over k).

Pryms of genus 4 curves

Joint work with Emre Can Sertöz (MPI Leipzig)

Reminder: Non-hyperelliptic genus 4 curves have a canonical model in $\mathbb{P}^3$ $\Gamma = Q = 0$, where $\deg(\Gamma) = 3$, $\deg(Q) = 2$.

- Rulings on Q give trigonal maps $C \to L$,
- If Q is nonsingular, then C has two trigonal maps
- If Q is singular then C is uniquely trigonal (vanishing theta null)
- Cubic surfaces containing C: $\operatorname{span}\langle \Gamma, xQ, yQ, zQ, wQ \rangle$.

Cayley cubic: Four nodes; admits a *symmetric* presentation:

$$\Gamma_\varepsilon : xyz + xyw + xzw + yzw = \det \begin{pmatrix} x+w & w & w \\ w & y+w & w \\ w & w & z+w \end{pmatrix}$$

Points on Γ_ε parametrize singular plane conics, so pairs of lines.

Double cover: $\tilde{\Gamma} \to \Gamma$ Splits these pairs.

Double covers of genus 4 curves

Theorem (Catanese, B-Sertöz): The double covers of C (modulo twists) correspond exactly to symmetrized cubics containing C:

$$\varepsilon \in \mathrm{Pic}^0(C)[2] \setminus \{0\} \longleftrightarrow \{\text{Symmetrized cubics } \Gamma_\varepsilon \supset C\}$$

Warning: If $C \to E$ is bielliptic, then double covers of E (three in total) pull back to double covers of C. Then Γ_ε is a cone over E with three possible symmetrizations.

Parametrization: Symmetrization induces a birational map

$$\mathbb{P}^2 \to \Gamma_\varepsilon$$

Distinguished double cover:

$$\begin{array}{ccc} \tilde{C}_\varepsilon & \longrightarrow & \tilde{\Gamma}_\varepsilon \\ \downarrow & & \downarrow \\ C & \longrightarrow & \Gamma_\varepsilon \end{array}$$

Question: Do we have $\mathrm{Prym}(\tilde{C}/C) = \mathrm{Jac}(X_\varepsilon)$ and if so, how do we construct X_ε?

Dual varieties

Recall: Given a surface $V : f(x,y,z,w) = 0$, we have a rational map:

$$\mathbb{P}^3 \to \widehat{\mathbb{P}}^3; \quad (x:y:z:w) \mapsto (\frac{\partial f}{\partial x} : \frac{\partial f}{\partial y} : \frac{\partial f}{\partial z} : \frac{\partial f}{\partial w})$$

Dual variety: Image $\widehat{V}$ under this map.

- If Γ_ε is a Cayley cubic then $\widehat{\Gamma}_\varepsilon$ is a quartic surface.
- For a nonsingular quadric Q, we have that $\widehat{Q}$ is an isomorphic quadric.

Theorem: $X_\varepsilon = \widehat{\Gamma}_\varepsilon \cap \widehat{Q}$ yields $\mathrm{Jac}(X_\varepsilon) = \mathrm{Prym}(\tilde{C}_\varepsilon / C)$.

Additionally, the pull-back of X_ε along $\mathbb{P}^2 \to \Gamma_\varepsilon \to \widehat{\Gamma}_\varepsilon$ gives a smooth plane quartic.

Indication of proof: We have that $C \subset Q$ makes C trigonal in two ways. Similarly, $X_\varepsilon \subset \widehat{Q}$ makes X_ε tetragonal in two ways. This fits in Recillas' trigonal construction.

Defining data

Equivalent defining data for Prym construction

- C, together with $\varepsilon \in \mathrm{Pic}^0(C)[2]$
- X, together with two tetragonal pencils $\mathscr{L}_1, \mathscr{L}_2$, with $\mathscr{L}_1 \otimes \mathscr{L}_2$ bicanonical

Note: $\mathscr{L}_1$ is either part of a canonical linear system, or $\mathscr{L}_1$ is complete.

Special cases:

- C may have a vanishing theta null θ_0: Q is a cone.
- ε may be bielliptic: Γ_ε is a cone
- $\mathscr{L}_1, \mathscr{L}_2$ may be canonical themselves
- $\mathscr{L}_1$ may be linear equivalent to $\mathscr{L}_2$ (self-residual)

$$\varepsilon \text{ bielliptic} \longleftrightarrow \mathscr{L}_1 \text{ self-residual}$$
$$\ell(\varepsilon+\theta_0) \text{ even} \longleftrightarrow C \text{ hyperelliptic}$$
$$\ell(\varepsilon+\theta_0) \text{ odd} \longleftrightarrow \mathscr{L}_1 \text{ canonical}$$

Note: $\ell(\varepsilon+\theta_0)$ odd and ε bielliptic does not happen.

Realizing a quartic as a prym curve

Required data: X: smooth plane quartic, and one of:

(a) Point in $\mathbb{P}^2$ to project from to get $X \to \mathbb{P}^1$

(b) $\{\mathscr{L}_1, \mathscr{L}_2\}$ Galois-stable as a set; equivalently:
$\{\mathscr{L}_1 - \kappa_C, \mathscr{L}_2 - \kappa_C\}$; a point on $\mathrm{Kum}(X) = \mathrm{Jac}(X)/\langle \pm 1 \rangle$.

(Indeed, the ”Fibre” of the Prym map $\tilde{C}/C \mapsto X$ is known to be the Kummer variety blown up at the origin)

With (b) we can construct Q and Γ_ε.

For (a) one can use link with degree 2 and 1 del Pezzo surfaces to construct C.

Software needs

- For determining $\mathrm{Jac}(C)(k)$: p-adic computations; S-units in number fields
- For computing X from C etc.: basic commutative algebra; elimination (images of maps)
- For experimental checking: period matrices of algebraic curves.
- For Chabauty computations: Computing with divisor classes over $\mathbb{Q}_p$ and $\mathbb{F}_p$.