Chabauty for Symmetric Powers of Curves

Samir Siksek
University of Warwick

$C/\mathbb{Q}$ curve $\qquad C(\mathbb{Q}) \neq \emptyset$

$g \geq 2$ genus

J Jacobian

Basic Problem: Compute $C(\mathbb{Q})$

One approach: Chabauty — need to know a basis for $J(\mathbb{Q})$.

Choose a prime $p \geq 3$ of good reduction.

$\Omega/\mathbb{Q}_p$ holomorphic differentials on $C/\mathbb{Q}_p$

$$\dim_{\mathbb{Q}_p} \Omega = g$$

[Example: $y^2 = x^5 + 1$

$$\Omega = \mathbb{Q}_p \frac{dx}{y} \oplus \mathbb{Q}_p \frac{x\,dx}{y}$$]

(Classical stuff) — Coleman, Wetherell, Flynn, ... ②

<u>Bilinear Pairing</u>

$$\Omega \times J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

$$\left(\omega, \left[\sum P_i - Q_i\right]\right) \longmapsto \sum \int_{Q_i}^{P_i} \omega$$

$$\Omega_0 = J(\mathbb{Q})^{\perp}$$

[Think of J as degree 0 divisors / lin. equiv.]

Let $\Omega_0 \subseteq \Omega$ be <u>annihilator</u> of $J(\mathbb{Q}) \subseteq J(\mathbb{Q}_p)$.

$$\boxed{\therefore \quad \omega \in \Omega_0, \quad P, Q \in C(\mathbb{Q}) \Longrightarrow \int_Q^P \omega = 0}$$

<u>Note</u> $\dim \Omega_0 \geq \dim \Omega - \operatorname{rank} J(\mathbb{Q})$
$= g - \operatorname{rank} J(\mathbb{Q})$

<u>Chabauty Assumption</u> $\operatorname{rank} J(\mathbb{Q}) \leq g-1$.

$\therefore \dim \Omega_0 \geq 1.$

Fix $\omega \in \Omega_0 \setminus \{0\}$ i.e. differential that kills $J(\mathbb{Q})$

Residue Classes These are the fibres of

$$\text{red} : C(\mathbb{Q}_p) \longrightarrow C(\mathbb{F}_p)$$

i.e. if $Q \in C(\mathbb{Q}_p)$, the residue class of Q is $\{P \in C(\mathbb{Q}_p) : P \equiv Q \bmod p\}$

Fix $Q \in C(\mathbb{Q})$.

Question Are there any $P \in C(\mathbb{Q})$ sharing the same residue class as ~~P~~ Q?

Suppose so.

Let $t \in \mathbb{Q}(C)$ uniformizer at Q, $\tilde{Q} \leftarrow \text{red}(Q)$.

Then $0 = \int_Q^P \omega$ $\qquad \omega = (a_0 + a_1 t + \cdots\cdots)\,dt$

by scaling $a_i \in \mathbb{Z}_p$

$$= \int_{t(Q)}^{t(P)} (a_0 + a_1 t + \cdots)\,dt$$

Recall $t(Q) = 0$ $\quad t(\tilde{Q}) \equiv 0 \pmod p$

and $\tilde{Q} \equiv \tilde{P} \pmod p$ so

$\widetilde{t(P)} = t(\tilde{P}) \equiv t(\tilde{Q}) \equiv 0 \pmod p$.

Let $z = t(P)$ $\quad z \equiv 0 \pmod p$

Then
$$0 = \int_Q^P \omega$$
$$= \int_{\underbrace{t(Q)}_{=0}}^{\overbrace{t(P)}^{=z}} (a_0 + a_1 t + \cdots)\, dt$$
$$= a_0 z + \frac{a_1}{2} z^2 + \cdots$$
$$= z\left(a_0 + \frac{a_1}{2} z + \cdots\right)$$

If $a_0 \not\equiv 0 \bmod p$ then
$$\left(a_0 + \frac{a_1}{2} z + \cdots\right) \equiv a_0 \not\equiv 0 \pmod p$$
(Recall $p \geq 3$)

$\therefore$ $a_0 + \frac{a_1}{2} z + \cdots \neq 0$

$\therefore$ $t(P) = z = 0$ $\quad \therefore$ $P = Q$

Chabauty Criterion If $a_0(\omega) \not\equiv 0 \pmod{p}$ then Q is the unique rational point in its residue class.

How to get $C(\mathbb{Q})$?

Let $K \subseteq C(\mathbb{Q})$ subset of known points.

$$S_p = \{ \tilde{Q} : Q \in K \text{ \& by Chabauty I know there is no other rational point sharing its residue class} \}$$

$S_p \subseteq C(\mathbb{F}_p)$

Let $R_p = C(\mathbb{F}_p) \setminus S_p$

Suppose $\exists\, Q \in C(\mathbb{Q}) \setminus K$ want contradiction.

Clearly $\tilde{Q} \in R_p$.

Now let $p_1, \ldots, p_n$ be primes of good reduction.

unknown point Albanese map

$$\begin{tikzcd}
Q \arrow[r, phantom, "\in"] \arrow[dd, dashed] & C(\mathbb{Q}) \arrow[r, "\phi"] \arrow[d, "\mathrm{red}"] & J(\mathbb{Q}) \arrow[d, "\mathrm{red}"] \\
 & \prod C(\mathbb{F}_{p_i}) \arrow[r, "\phi"] & \prod J(\mathbb{F}_{p_i}) \\
\prod \mathcal{R}_{p_i} \arrow[ur, phantom, "\subseteq" sloped] & &
\end{tikzcd}$$

Clearly $\phi(\tilde{Q}) \in \underbrace{\phi\left(\prod \mathcal{R}_{p_i}\right) \cap \mathrm{red}(J(\mathbb{Q}))}_{\text{finite \& computable}}$

Contradiction if

$$\phi\left(\prod \mathcal{R}_{p_i}\right) \cap \mathrm{red}(J(\mathbb{Q})) = \emptyset,$$

Then $C(\mathbb{Q}) = K$. (i.e. known points are only ones)

Example (Flynn, Poonen & Schaeffer)

$$C: \ y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$$

$$C(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 1), (-3, \pm 1)\}$$

Can we use Chabauty for varieties of dim ≥ 2?

$$X \xrightarrow{i} \mathrm{Alb}(X) = A$$

Albanese variety of X

X: variety

i: Albanese morphism

Have pairing:

$$\Omega \times A(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

In general: don't know how to compute $A(\mathbb{Q})$ etc.

Look for a situation where we understand A & i.

First Attempt: Symmetric powers of curves

$$C^{(d)} := S_d \backslash C^d$$

$C^{(d)}$: d-th symmetric power

S_d: symmetric group

$\left[\mathrm{Alb}(C^{(d)}) = J \right.$

J: Jacobian of C

(suppose $C(\mathbb{Q}) \neq \phi$)

Note ① $\{P_1, \dots, P_d\} \in C^{(d)}(\mathbb{Q})$

$\iff$ $P_i \in C(\overline{\mathbb{Q}})$, $\{P_1, \dots, P_d\}$ fixed by $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

$\iff$ $\sum P_i$ is a +ve rational divisor of degree d.

② Knowing $C^{(d)}(\mathbb{Q})$ means knowing $C(K)$ for all $K/\mathbb{Q}$ with $[K:\mathbb{Q}] \leq d$.

Suppose $\mathcal{Q} = \{Q_1, Q_2\} \in C^{(2)}(\mathbb{Q})$ known

$\mathcal{P} = \{P_1, P_2\} \in C^{(2)}(\mathbb{Q})$ unknown

and $\mathcal{P} \equiv \mathcal{Q} \pmod{p}$.

Choose p prime ≥ 5

$\omega \in \Omega_0 \leftarrow$ annihilator of $J(\mathbb{Q})$

Choose t_i uniformizer at $Q_i, \tilde{Q}_i$.

Then

$$0 = \int_{Q_1}^{P_1} \omega + \int_{Q_2}^{P_2} \omega \qquad \begin{aligned} \omega &= (a_1 + b_1 t_1 + \cdots)\, dt_1 \\ \omega &= (a_2 + b_2 t_2 + \cdots)\, dt_2 \end{aligned}$$

$$= \int_0^{z_1} (a_1 + \cdots)\, dt_1 + \int_0^{z_2} (a_2 + \cdots)\, dt_2$$

where $z_i = t_i(P_i)$

$$= a_1 z_1 + a_2 z_2 + (\text{higher powers})$$

Suppose $\omega_1, \omega_2 \in \Omega_0$ are linearly independent. Get

$$a_{11} z_1 + a_{12} z_2 + (\text{higher powers}) = 0$$

$$a_{21} z_1 + a_{22} z_2 + (\text{higher powers}) = 0$$

Chabauty Criterion

If $\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \not\equiv 0 \pmod{\pi}$, $\pi \mid p$

then $Q = \{Q_1, Q_2\}$ is the unique rational point in its residue class.

Note: for Chabauty to succeed for $C^{(d)}$ need

$$\dim \Omega_0 \geq d$$

Enough to have $\operatorname{rank}(J(\mathbb{Q})) \leq g-d$.

Usually need Chabauty criterion and several primes as before to show that

$$C^{(d)}(\mathbb{Q}) = \text{known rational points.}$$

Example 1 (non-hyperelliptic genus 3)

$C \quad x^4 + (y^2+1)(x+y) = 0$

Schaefer & Wetherell:

$J(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$

$C(\mathbb{Q}) = \{(0,0), (-1,0), \infty\}$

Our method shows $C^{(2)}(\mathbb{Q}) =$

$\Big\{ \{(0,0),(0,0)\}, \{(0,0),(-1,0)\}, \{(0,0),\infty\}$

$\{(-1,0),(-1,0)\}, \{(-1,0),\infty\}, \{\infty,\infty\},$

$\{(0,i),(0,-i)\}, \left\{\left(\frac{1+\sqrt{-3}}{2},0\right),\left(\frac{1-\sqrt{-3}}{2},0\right)\right\},$

$\left\{\left(-1,\frac{1+\sqrt{-3}}{2}\right),\left(-1,\frac{1-\sqrt{-3}}{2}\right)\right\},$

$\left\{\left(-17+\sqrt{259},\ -48+3\sqrt{259}\right), \text{conj}\right\} \Big\}$

Used Mordell–Weil sieve first with

$p = 3, 5, 7, \ldots, 23$

and then lazy Chabauty with $p=5$.

[For now assuming

$J(\mathbb{Q}) = \mathbb{Z}\cdot((-1,0)-\infty) + \mathbb{Z}/4\mathbb{Z}\,((0,0)-\infty)$]

Example 2 (hyperelliptic genus 3)

$C: \quad y^2 = x(x^2+2)(x^2+43)(x^2+8x-6)$

Magma $\Longrightarrow$ $J(\mathbb{Q})$ has rank 1

Let $\pi : C \longrightarrow \mathbb{P}^1$ $\quad (x,y) \longmapsto x$, $\infty \longmapsto \infty$.

Using Chabauty with $p = 5, 7, 13$ we get

$$C^{(2)}(\mathbb{Q}) = \pi^{-1}\mathbb{P}^1(\mathbb{Q}) \cup \{Q_1, \ldots, Q_{10}\}$$

where

$$\pi^{-1}\mathbb{P}^1(\mathbb{Q}) = \{\{\infty,\infty\}\} \cup \{\{(x,y),(x,-y)\} : x \in \mathbb{Q}\}$$

$Q_1 = \{(0,0), \infty\}$, $\quad Q_2 = \{(\sqrt{-2},0), (-\sqrt{-2},0)\}$

$Q_3 = \{(\sqrt{43},0), \text{conj}\}$, $\quad Q_4 = \{(-4+\sqrt{22},0), \text{conj}\}$

$Q_5 = \{(\sqrt{6}, 56\sqrt{6}), \text{conj}\}$, $\quad Q_6 = Q_5'$

$Q_7 = \left\{\left(\frac{41+\sqrt{1509}}{2}, -222999 - 5740\sqrt{1509}\right), \text{conj}\right\}$ $\quad Q_8 = Q_7'$

$Q_9 = \left\{\left(\frac{-164+\sqrt{22094}}{49}, \frac{257704352 - 1648200\sqrt{22094}}{823543}\right), \text{conj}\right\}$ $\quad Q_{10} = Q_9'$