Chabauty for Symmetric Powers of Curves

Samir Siksek
University of Warwick

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

Defn d-th symmetric power of C is

$$C^{(d)} := \underset{\substack{\uparrow \\ \text{symmetric group}}}{S_d} \backslash C^d$$

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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

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

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

Aim Adapt Chabauty to compute $C^{(d)}(\mathbb{Q})$ in favourable circumstances.

Previous & current work on subject

(i) M. Klassen Arizona PhD (1993) (not very explicit)

(ii) J. Wetherell (circa 2000) computed some examples

(iii) "well-known" to the experts

(iv) S.S. "Chabauty for Symmetric Powers of Curves"

To simplify, focus on $C^{(2)}(\mathbb{Q})$.

Chabauty–Coleman

p prime of good reduction

$\Omega/\mathbb{Q}_p$ $\mathbb{Q}_p$ – vector space of holomorphic differentials

J Jacobian of C

There is a pairing

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

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

$\omega_1, \ldots, \omega_n$ basis for annihilator of $J(\mathbb{Q}) \subseteq J(\mathbb{Q}_p)$

$$n \geq g - \operatorname{rank} J(\mathbb{Q})$$

Residue classes fibres of map
$$C^{(2)}(\mathbb{Q}_p) \longrightarrow C^{(2)}(\mathbb{F}_p)$$

"Hardcore ~~Energetic~~ Chabauty": method for bounding number of rational points in each ~~fibre~~ residue class.

"Lazy Chabauty": start with $\mathcal{Q} = \{Q_1, Q_2\} \in C^{(2)}(\mathbb{Q})$ Show that it <u>doesn't</u> share its residue class with any other element of $C^{(2)}(\mathbb{Q})$.

<u>How</u>? $\mathcal{Q} = \{Q_1, Q_2\} \in C^{(2)}(\mathbb{Q})$, $\mathcal{Q}$ known

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

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

<u>Objective</u> Show $\mathcal{P} = \mathcal{Q}$

WLOG $P_1 \equiv Q_1$, $P_2 \equiv Q_2 \pmod{\pi}$ $(\pi | p)$

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

Let $\omega \in \{\omega_1, \dots, \omega_n\} \leftarrow$ diffs annihilating $J(\mathbb{Q})$

(4)

Then $[(P_1+P_2)-(Q_1+Q_2)] \in J(\mathbb{Q})$,

so $\int_{Q_1}^{P_1} \omega + \int_{Q_2}^{P_2} \omega = 0$.

Write $\omega = (\alpha + \alpha' t_1 + \alpha'' t_1^2 + \cdots) dt_1$ [scaling ω $\Downarrow$ coeffs $\in \mathcal{O}_\pi$]
$\omega = (\beta + \beta' t_2 + \beta'' t_2^2 + \cdots) dt_2$

Let $z_1 = t_1(P_1)$, $z_2 = t_2(P_2)$

(objective = show $z_1 = z_2 = 0$)

Then $0 = \int_0^{z_1} (\alpha + \alpha' t_1 + \cdots) dt_1 + \int_0^{z_2} (\beta + \beta' t_2 + \cdots) dt_2$

$= \alpha z_1 + \beta z_2 +$ (higher order terms)

Let $m = \min\{\mathrm{ord}_\pi z_1, \mathrm{ord}_\pi z_2\}$ [objective = show $m = \infty$]

Know $m \geq 1$. If $p >$ const

then $\alpha z_1 + \beta z_2 \equiv 0 \mod \pi^{m+1}$

Do this for each diff $\omega_1, \ldots, \omega_n$.

Get system $\left.\begin{array}{l} \alpha_1 z_1 + \beta_1 z_2 \equiv 0 \\ \vdots \\ \alpha_n z_1 + \beta_n z_2 \equiv 0 \end{array}\right\} \mod \pi^{m+1}$

If $\mathrm{rank}\begin{pmatrix} \bar{\alpha}_1 & \bar{\beta}_1 \\ \vdots & \vdots \\ \bar{\alpha}_n & \bar{\beta}_n \end{pmatrix} \geq 2$ then

$\leftarrow$ reduction mod π

$z_1 \equiv z_2 \equiv 0 \pmod{\pi^{m+1}} \Rightarrow m \geq m+1$

$\Rightarrow m = \infty \Rightarrow P = Q$.

Necessary condition for this to work is $r \geq 2$ i.e. g − Chabauty rank ≥ 2

(e.g. $g = 3$, rank $= 1$ should work)

[For $C^{(d)}(\mathbb{Q})$ want g − Chabauty rank $\geq d$]

Lazy Chabauty II How do we get $C^{(2)}(\mathbb{Q})$?

Let $\mathcal{L}$ known elts of $C^{(2)}(\mathbb{Q})$

Suppose $\exists\, \beta \in C^{(2)}(\mathbb{Q}) \setminus \mathcal{L}$

Objective Get a contradiction.

Fix $C^{(2)}(\mathbb{Q}) \xrightarrow{\phi} J(\mathbb{Q})$.

Pick a prime p of good reduction.

Let $S_p = \{\widetilde{Q} : Q \in \mathcal{L}$ & using Lazy Chabauty I know there is no other rational element sharing its residue class $\}$

$S_p \subseteq C^{(2)}(\mathbb{F}_p)$

Let $\mathfrak{R}_p = C^{(2)}(\mathbb{F}_p) \setminus S_p$.

Clearly $\tilde{\mathfrak{P}} \in \mathfrak{R}_p$.

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

$$
\begin{tikzcd}
\mathfrak{P} \in C^{(2)}(\mathbb{Q}) \arrow[r, "\phi"] \arrow[d, "\mathrm{red}"] \arrow[dd, dashed, bend right] & J(\mathbb{Q}) \arrow[d, "\mathrm{red}"] \\
\prod C^{(2)}(\mathbb{F}_{p_i}) \arrow[r, "\phi"] \arrow[d, phantom, sloped, "\supseteq"] & \prod J(\mathbb{F}_{p_i}) \\
\prod \mathfrak{R}_{p_i} &
\end{tikzcd}
$$

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

Contradiction if

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

Then $C^{(2)}(\mathbb{Q}) = \mathcal{L}$. (i.e. known points are only ones)

~~Example 2~~

Rewards of laziness I

(non-hyperelliptic genus 3)

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

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

$$\Big\{ \{(0,0),(0,0)\},\ \{(0,0),(-1,0)\},\ \{(0,0),\infty\},$$
$$\{(-1,0),(-1,0)\},\ \{(-1,0),\infty\},\ \{\infty,\infty\},$$
$$\{(0,i),(0,-i)\},\ \left\{\left(\tfrac{1+\sqrt{-3}}{2},0\right),\left(\tfrac{1-\sqrt{-3}}{2},0\right)\right\},$$
$$\left\{\left(-1,\tfrac{1+\sqrt{-3}}{2}\right),\left(-1,\tfrac{1-\sqrt{-3}}{2}\right)\right\},$$
$$\left\{\left(-17+\sqrt{259},\ -48+3\sqrt{259}\right),\ \text{conj}\right\} \Big\}$$

Used Mordell–Weil sieve first with

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

and then lazy Chabauty with $p=5$.

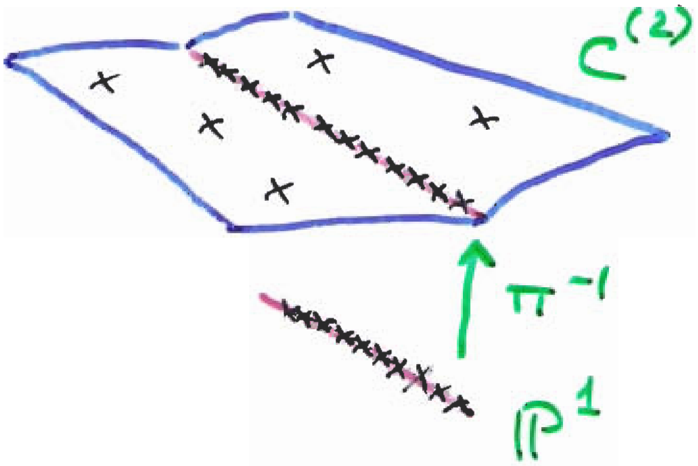
[For now assuming
$$J(\mathbb{Q}) = \mathbb{Z}\cdot((-1,0)-\infty) + \mathbb{Z}/4\mathbb{Z}\,((0,0)-\infty)$$
]

Problem If C is hyperelliptic

$C : y^2 = f(x)$ $\quad \pi : C \to \mathbb{P}^1$, $(x,y) \mapsto x$

Then $\pi^{-1} : \mathbb{P}^1 \to C^{(2)}$

$$\underbrace{\pi^{-1}\mathbb{P}^1(\mathbb{Q})}_{\text{infinite}} = \left\{ \{(x, \sqrt{f(x)}), (x, -\sqrt{f(x)})\} : x \in \mathbb{Q} \right\} \cup \{\infty, \infty\} \text{ or } \cup \{\infty^+, \infty^+\}$$



Lazy Chabauty fails for $\mathcal{Q} \in \pi^{-1}\mathbb{P}^1(\mathbb{Q})$

Call elements of $\pi^{-1}\mathbb{P}^1(\mathbb{Q})$ trivial.

Lazy Chabauty III Given $\mathcal{Q}$ trivial, p prime.

Suppose $\mathcal{P} \in C^{(2)}(\mathbb{Q})$ $\quad \mathcal{P} \equiv \mathcal{Q} \pmod p$

Objective Show $\mathcal{P}$ is trivial.

Let $\iota : C \longrightarrow C$ hyperelliptic inv. (9)

$(x,y) \longmapsto (x,-y)$

Then $\mathcal{Q} = \{Q, Q'\}$, $\iota Q' = Q$.

Write $\mathcal{P} = \{P, P'\}$ [objective = show $\iota P' = P$]

WLOG $P \equiv Q \pmod{\pi}$, $P' \equiv Q' \pmod{\pi}$

Let t be uniformizer at $Q, \tilde{Q}$.

Write $z = t(P)$, $z' = t(\iota P')$

[objective = show that $z = z'$].

Take ω holomorphic diff annihilating $J(\mathbb{Q})$

$$\omega = (\alpha + \beta t + \gamma t^2 + \cdots)\, dt \qquad \alpha, \beta, \ldots \in \mathcal{O}_\pi$$

(after scaling ω)

Then
$$0 = \int_Q^P \omega + \int_{Q'}^{P'} \omega$$

replace y by $-y$

$$= \int_Q^P \omega - \int_{\iota Q'}^{\iota P'} \omega$$

[ω is a lin. comb. of $\frac{dx}{y}, \ldots, x^{g-1}\frac{dx}{y}$,
so $y \mapsto -y$ sends $\omega \mapsto -\omega$]

So $\displaystyle 0 = \int_Q^P \omega - \int_Q^{\iota P'} \omega \qquad Q = \iota Q'$

$$= \left(\int_0^z - \int_0^{z'}\right)(\alpha + \beta t + \cdots)\,dt$$

$$= (z - z')\left(\alpha + \frac{\beta}{2}(z+z') + \cdots\right)$$

Note $z \equiv z' \equiv 0 \pmod{\pi}$.

If $\alpha \not\equiv 0 \bmod \pi$ and $p >$ constant

then $\alpha + \frac{\beta}{2}(z+z') + \cdots \equiv \alpha \bmod \pi$

so $\alpha + \frac{\beta}{2}(z+z') + \cdots \neq 0$

$\therefore\ z = z'$ objective achieved.

Can do the same for $C^{(d)}(\mathbb{Q})$ if $\pi : C \longrightarrow C'$ geometrically Galois of degree d.

Necessary condition: (??)

$$(g - g') - (r - r') \geq d - 1$$

g, g' genus of C, C' & r, r' Ch. ranks

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

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

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

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

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

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

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

$Q_8 = Q_7'$

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

$Q_{10} = Q_9'$