Computational aspects of nonabelian Chabauty Lecture I
September 12, 2023

Recall:

Thm (Coleman, 1985, "Effective Chabauty") Let $X/\mathbb{Q}$ a nice curve of genus $g \geq 2$. Suppose the Mordell-Weil rank of the Jacobian $J(\mathbb{Q})$ is less than g. If $p > 2g$ is a prime of good reduction for X,

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

Rmk. This upper bound comes from bounding the number of zeros of a p-adic (Coleman) integral.

Rmk. In general, very difficult to compute (or bound) $\mathrm{rk}\, J(\mathbb{Q})$ unless we're in some special cases:
- X hyperelliptic curve, via 2-descent (Magma) · RankBounds
- More generally, X cyclic cover of $\mathbb{P}^1$ (Magma)
- X is a modular curve, use analytic information to compute rank

How do we use Coleman's theorem ("Chabauty-Coleman method")?

A few different ways:

1) Directly, i.e., one has a good small prime p s.t.
$$\#X(\mathbb{Q})_{\text{known}} = \#X(\mathbb{F}_p) + 2g - 2$$

2) Do a bit more work: one computes an annihilating differential (or several annihilating differentials) and explicitly bound the number of zeros of its Coleman integral in each residue disk of the curve. This yields a finite set of points $X(\mathbb{Q}_p)_1$.
   A) This may work and give $X(\mathbb{Q})_{\text{known}} = X(\mathbb{Q}_p)_1$.
      $\Rightarrow$ This yields $X(\mathbb{Q})$.
   B) But it may be the case that $\#X(\mathbb{Q}_p)_1$ is strictly larger than $\#X(\mathbb{Q})_{\text{known}}$. What can be done?

In this case, we say that we have mock rational points in the Selmer set $X(\mathbb{Q}_p)_1$. Two possibilities:

- Can recognize mock rational points as algebraic ☺
- ?? — we combine with other strategies, e.g. the Mordell-Weil sieve

---

Some examples:

Ex 1. $X: y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16$

The Jacobian of X has $\mathrm{rk}\, J(\mathbb{Q}) = 1$ (Magma)

X has good reduction at $p=5$ and

$X(\mathbb{F}_5) = \{\infty^{\pm}, (0,\pm 1), (1,\pm 1), (2,\pm 2)\}$. So $\#X(\mathbb{F}_5) = 8$.

Coleman's theorem tells us $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_5) + 2g - 2$

$= 8 + 2\cdot 2 - 2$

$= 10$.

We search for rational points in a box and find

$X(\mathbb{Q})_{\text{known}} = \{\infty^{\pm}, (0,\pm 4), (1,\pm 1), (2,\pm 8), (\frac{13}{11}, \pm\frac{868}{113})\}$

So $X(\mathbb{Q}) = X(\mathbb{Q})_{\text{known}}$.

(This example is not quite the generic outcome of the Chabauty-Coleman method ... cf. the next example)

Ex. 2 $X: y^2 = x^5 - 2x^3 + x + \frac{1}{4}$, LMFDB 971.a.971.1

(L-Functions and Modular Forms Database - lmfdb.org)

DB of genus 2 curves

- $J(\mathbb{Q}) \cong \mathbb{Z}$ and $[(-1,-1/2) - (0,1/2)] \in J(\mathbb{Q})$ is a point of infinite order (Magma)
- We can for rational points in a box and find $X(\mathbb{Q})_{\text{known}} = \{\infty, (0,\pm 1/2), (-1,\pm 1/2), (1,\pm 1/2)\}$. ← $\#X(\mathbb{Q})_{\text{known}} = 7$
- X has good reduction at $p=3$, and $\#X(\mathbb{F}_3) = 7$.

Stoll's refinement of Chabauty-Coleman bound for $p=3$:

$(7 \leq)\ \#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r + \left\lfloor \frac{2r}{p-2} \right\rfloor$

$7 + 2 + 2 = 11$

So we need to do more work to determine $X(\mathbb{Q})$.

We construct a 3-adic annihilating differential η and compute its Coleman integral.

Crash course on Coleman integration:

Thm (Coleman, 1980s) Let $X/\mathbb{Q}_p$ be a nice curve with good reduction at p. The p-adic integral $\int_P^Q \omega \in \overline{\mathbb{Q}}_p$ defined for $P, Q \in X(\overline{\mathbb{Q}}_p)$ and $\omega \in H^0(X, \Omega^1)$ satisfies the following:

1) the integral is $\overline{\mathbb{Q}}_p$-linear.
2) If P, Q reduce to the same point $\bar{P} \in X(\overline{\mathbb{F}}_p)$, then we call the integral a <u>tiny integral</u> (Evaluate it via a local coordinate in the residue disk + formal integration.)
3) We have $\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega$

$\Rightarrow$ can define $\int_D \omega$ for $D = \sum_{j=1}^{n} ((Q_j) - (P_j)) \in \mathrm{Div}_X^0(\overline{\mathbb{Q}}_p)$

as $\int_D \omega = \sum_{j=1}^{n} \int_{P_j}^{Q_j} \omega$.

4) D principal $\Rightarrow$ $\int_D \omega = 0$

5) The integral is compatible with $\mathrm{Gal}(\overline{\mathbb{Q}}_p / \mathbb{Q}_p)$-action.
6) Fix $P_0 \in X(\overline{\mathbb{Q}}_p)$. If $0 \neq \omega \in H^0(X, \Omega^1)$ then the set of points $P \in X(\overline{\mathbb{Q}}_p)$ reducing to a fixed point in $X(\overline{\mathbb{F}}_p)$ s.t. $\int_{P_0}^{P} \omega = 0$ is finite.

This is the Coleman integral.

Def. Let $A = \{\omega \in H^0(X, \Omega^1) : \text{for all } P \in J(\mathbb{Q}),\ \int_0^P \omega = 0\}$ be the subspace of annihilating differentials.

By "computing rational points via the Chabauty-Coleman method. we mean that we compute the finite set of p-adic points

$$X(\mathbb{Q}_p)_1 = \{z \in X(\mathbb{Q}_p) : \int_1^z \omega = 0 \text{ for all } \omega \in A\}$$

for a fixed basepoint $b \in X(\mathbb{Q})$.

Back to our example:

Recall that we wanted to construct a 3-adic annihilating differential η on our genus 2 curve $X: y^2 = x^5 - 2x^3 + x + \frac{1}{4}$. Basis of $H^0(X_{\mathbb{Q}_3}, \Omega^1)$ is $\{\omega_i = \frac{x^i dx}{y}\}, i = 0, 1$. So η is a linear combination of ω_0 and ω_1. We use the values of

$$\alpha := \int_{(0,1/2)}^{(-1,-1/2)} \omega_0 \quad \text{and} \quad \beta := \int_{(0,1/2)}^{(-1,-1/2)} \omega_1$$

(recall: $[(-1,-1/2) - (0,1/2)] \in J(\mathbb{Q})$ is of infinite order)

to compute η.

SageMath can compute α, β:

$$\alpha = 3 + 3^2 + 3^4 + \cdots$$

$$\beta = 2 + 2\cdot 3 + 2\cdot 3^3 + \cdots$$

We take $\eta = \beta\omega_0 - \alpha\omega_1$ as our annihilating differential and run Chabauty-Coleman method.

Where do these numbers come from?

Explicit Coleman integration (Implementations: • SageMath for hyperell. curves (Sage library) • Julia for superell. curves (Alex Best's Github) • Magma for plane curves (Jan Tuitman's Github))

One approach:
Compute the action of Frobenius on p-adic cohomology of curve
(Alternate approach: work in the Jacobian, via kernel of reduction, but there's no obvious nonabelian generalization)

Let X^{an} denote the rigid analytic space over $\mathbb{Q}_p$ associated to $X/\mathbb{Q}_p$.
A wide open subspace of X^{an} is the complement in X^{an} of

the union of a finite collection of disjoint closed disks of radius $\lambda_i < 1$.

Thm (Coleman) Let η, ξ be 1-forms on a wide open subspace V of X^{an} and $P, Q, R \in V(\overline{\mathbb{Q}}_p)$. Let $a, b \in \overline{\mathbb{Q}}_p$. Then we have

1) linearity in the integrand
2) additivity in endpoints $\left(\int_P^Q \eta + \int_Q^R \eta = \int_P^R \eta\right)$
3) Change of variables under rigid analytic maps
4) Fundamental Theorem of Calculus
5) Galois compatibility.

Aim: first integrate $\int_P^Q \omega$ for ω a 1-form of the second kind (residue 0 everywhere), $P, Q \in V(\overline{\mathbb{Q}}_p)$.

We'll discuss the case of X hyperelliptic curve first.