Computational aspects of nonabelian Chabauty
Lecture 2, September 13, 2023

Goal: integrate $\int_P^Q \omega$ for ω a 1-form of the second kind.

Suppose X is a hyperelliptic curve (general case in a bit).
Sketch of explicit Coleman integration (B.–Bradshaw–Kedlaya '10):

1) Take a lift ϕ of p-power Frobenius from the special fiber
2) Compute a basis $\{\omega_i\}$ of 1-forms of the second kind
3) Compute $\phi^*\omega_i$ via Kedlaya's zeta function algorithm and use properties of Coleman integrals to relate $\int_P^Q \phi^*\omega_i$ to $\int_P^Q \omega_i$, as well as other terms we can compute.
4) Use linear algebra to solve for $\{\int_P^Q \omega_i\}$.

Kedlaya's algorithm (sketch). Let $X: y^2 = P(x)$ be a hyperell. curve

- Work in an affine $Y \subset X$, given by deleting Weierstrass points
- Take ϕ to be the following lift of Frobenius:

$$x \mapsto x^p$$
$$y \mapsto y^p \sum_{j=0}^{\infty} \binom{1/2}{j} \left(\frac{P(x^p) - P(x)^p}{y^{2p}} \right)^j$$

- Compute the action of Frobenius on a basis elt of $H^1_{dR}(X)$, and reduce the pole order of each resulting differential using relations in cohomology.

e.g. let $\omega_i = \frac{x^i\,dx}{y}$.

Kedlaya's work tells us — see Prop 1.33 from Aws lecture notes.

$$\phi^*\omega_i = \phi^*\left(\frac{x^i\,dx}{y}\right) = \frac{x^{pi}\,d(x^p)}{\phi(y)} = \frac{p\,x^{pi+p-1}\,dx}{y^p} \sum_{j=0}^{\cancel{\infty}\,N} \binom{-1/2}{j} \left(\frac{P(x^p) - P(x)^p}{y^{2p}}\right)^j$$

$\rightsquigarrow$ after reducing using various relations in cohomology, get

$$\phi^*\omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ji}\,\omega_j$$

How does this allow us to compute Coleman integrals?

If we can compute h_i and M_{ji}, then we have

$$\begin{pmatrix} \vdots \\ \int_Q^P \omega_i \\ \vdots \end{pmatrix} = (M^t - I)^{-1} \begin{pmatrix} \vdots \\ h_i(P) - h_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^{Q} \omega_i \\ \vdots \end{pmatrix} \quad (*)$$

Note that eigenvalues of M have norm $\sqrt{p}$ by the pf. of Weil conjectures.

Finishing the example with the 3-adic integral on $y^2 = x^5 - 2x^3 + x + \frac{1}{4}$:

- We constructed $\eta = \beta\omega_0 - \alpha\omega_1$, where α, β are computed using the linear system $(*)$.
- We want to compute
$$X(\mathbb{Q}_3)_1 := \{ z \in X(\mathbb{Q}_3) : \int_{(0,1/2)}^{z} \eta = 0 \} \supset X(\mathbb{Q})$$
- Do the above by computing power series expansions of the collection of Coleman integrals $\left\{ \int_{(0,1/2)}^{P_t} \eta \right\}$ where P_t ranges over all residue disks.

In particular, can take

$$(\star) \int_{(0,1/2)}^{P_t} \eta = \underbrace{\int_{(0,1/2)}^{P_0} \eta}_{(**)} + \underbrace{\int_{P_0}^{P_t} \eta}_{(***)}$$

$(**)$ is a 3-adic #
$(***)$ is a tiny integral

Lucky fact: for each residue disk, $\exists$ $P_0 \in X(\mathbb{Q})$! So take P_0 to be this point. Then $(**)$ is simply 0 and the computation is purely local now.

- Computing the power series $(\star)$ in each residue disk, we find each has a simple zero at the known rational point.
- This proves $X(\mathbb{Q}) = \{ \infty, (0, \pm 1/2), (-1, \pm 1/2), (1, \pm 1/2) \}$.

Ex 3. $X_0(37)$: $y^2 = -x^6 - 9x^4 - 11x^2 + 37$

$\operatorname{rk} J_0(37)(\mathbb{Q}) = 1$

Carry out Chabauty – Coleman using $\frac{dx}{y}$ as our annihilating differential.
We find $X_0(37)(\mathbb{Q}_3)_1 = \{(\pm 1, \pm 4), P, \iota(P)\}$
where $P, \iota(P)$ are mock rational points.
It turns out that $\{P, \iota(P)\} = \{(0, \pm\sqrt{37})\}$.
$\Rightarrow$ So we can deduce that $X_0(37)(\mathbb{Q}) = \{(\pm 1, \pm 4)\}$.

elliptic curves

Note that $J_0(37) \sim E_0 \times E_1$, where

LMFDB labels

E_0 : 37.b2 $\qquad E_0(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$
E_1 : 37.a1 $\qquad E_1(\mathbb{Q}) \cong \mathbb{Z}$

So can alternatively compute rational points on $X_0(37)$ by the "rank 0" strategy.

Rmk. There are generalizations of Chabauty – Coleman in a few different directions:
1) Combining w/ restriction-of-scalars (Siksek)
Chabauty over number fields K (?? $r \leq [K:\mathbb{Q}](g-1)$)
2) Chabauty for symmetric powers of curves (Siksek, Box, Box – Gajović – Goodman): used to find all quadratic points (and indeed cubic or quartic points) on certain modular curves
3) Chabauty – Coleman for surfaces
Thm (Caro – Pasten, simplified version) Let X be a surface in A an abelian 3-fold $/\mathbb{Q}$. Suppose $\mathrm{rk}\, A(\mathbb{Q}) \leq 1$, p is a prime of good reduction sufficiently large, $X/\mathbb{F}_p$ contains no ell. curves. Then

$$\# X(\mathbb{Q}) \leq \# X(\mathbb{F}_p) + 4p\, c_1^2(X)$$

See paper for their actual bound, which is better!

where $c_1^2(X)$ is the 1st Chern number of the surface.

(cf. $\# C(\mathbb{Q}) \leq \# C(\mathbb{F}_p) + c_1(X)$)
for a curve $C/\mathbb{Q}$ w/ Jacobian rank $< g$.

Coleman integration from Kedlaya to Tuitman
(hyperelliptic) (plane)

Let $X/\mathbb{Q}$ be a nice curve of genus g:
$Q(x,y) = y^{d_x} + Q_{d_x-1}\, y^{d_x-1} + \cdots + Q_0 = 0$ s.t. $Q(x,y)$ is irred, $Q_i(x) \in \mathbb{Z}[x]$

1) Consider the map $x : X \to \mathbb{P}^1$ and remove the ramification locus $r(x)$ of the map x (the analogue of removing Weierstrass points in Kedlaya's algorithm)
2) Choose a lift of Frobenius $x \mapsto x^p$, compute image of y via Hensel lifting.
3) Compute action of Frobenius on differentials and reduce pole orders using Lauder's fibration algorithm.

In the same way as before, this gives "analytic continuation along Frobenius" and a linear system to produce $\left(\int_Q^P \omega_i\right)_{i=0,\ldots,2g-1}$

for $\{\omega_i\}$ a basis of $H^1_{dR}(X)$.

These p-adic integrals can be viewed as solutions to p-adic differential equations. For nonabelian Chabauty, will need to solve p-adic differential equations whose solutions are iterated Coleman integrals.

By work of Coleman ('82) and Coleman-de Shalit ('88), have a theory of iterated p-adic integrals on X (p-adic analogue of Chen's iterated integrals '71): these are iterated path integrals

$$\int_P^Q \eta_n \cdots \eta_1 = \int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1)\, dt_n \cdots dt_1 .$$

In quadratic Chabauty, the relevant objects are the double Coleman integrals

$$\int_P^Q \eta_2 \eta_1 := \int_P^Q \eta_2(R) \underbrace{\int_P^R \eta_1}_{=I(R)}$$
$$= \int_P^Q \eta_2(R)\, I(R)$$

n-fold

These iterated integrals are computed using:

- an algorithm for computing of Frobenius on p-adic cohomology (e.g. Kedlaya, Tuitman) to produce $\phi^* \omega_i = dh_i + \sum M_{ji} \omega_j$ for a bas $\{\omega_i\}$ of $H^1_{dR}(\mathcal{X})$
- Observe that the eigenvalues of $M^{\otimes n}$ are not 1, and reduce the computation of n-fold iterated integrals to (n-1) fold iterated integrals.

Application (Quadratic Chabauty for rank 1 elliptic curve, special case) Let $\mathcal{E}/\mathbb{Z}$ be the minimal regular model of an elliptic curve. Let $\mathcal{X} = \mathcal{E} \setminus \mathcal{O}$. Let $\omega_0 = \frac{dx}{2y + a_1 x + a_3}$, $\omega_1 = x\omega_0$.

Let b be a tangential basepoint at $\mathcal{O}$ or an integral 2-torsion point. Let p be a prime of good reduction. Suppose $\mathcal{E}$ has analytic rank 1 and Tamagawa product 1. Let

$$\log(z) = \int_b^z \omega_0, \quad D_2(z) = \int_b^z \omega_0 \omega_1$$

Thm (Kim, B.-Kedlaya-Kim) Suppose P a point of infinite order in $\mathcal{E}(\mathbb{Z})$. Then $\mathcal{X}(\mathbb{Z}) \subset \mathcal{E}(\mathbb{Z})$ is in the zero set of

$$f(z) := (\log(P))^2 D_2(z) - (\log(z))^2 D_2(P).$$

Observation (Kim) This D_2 is closely related to the p-adic height on $\mathcal{E}$.