Computational aspects of nonabelian Chabauty
Lecture 3, September 14, 2023

In the previous lecture, we saw a prototype of a quadratic Chabauty theorem: that, for a rank 1 elliptic curve $E/\mathbb{Q}$ with Tamagawa product 1 has integral points contained in the set

$$\{z \in E(\mathbb{Q}_p) : p(z) := D_2(z) - \frac{D_2(P)}{(\log(P))^2}(\log(z))^2 = 0\}$$ for a fixed $P \in E(\mathbb{Q})$ of infinite order.

- $D_2(z)$: ~ local height function
- $\frac{D_2(P)}{(\log(P))^2}$: constant relating global ht to the basis.
- $(\log(z))^2$: global height via choice of basis of quadratic forms
- $= 0$: local height away from p, given the Tamagawa hypothesis
- underbrace: global height

This is the general shape of a quadratic Chabauty function:

$$\text{QC function} = h_p - h = \sum : \leftarrow \text{values of possible loc. hts away from } p.$$

(h_p: loc. ht at p; h: global ht)

This comes from a global p-adic height

$$h = h_p + \sum_{q \neq p} h_q$$

that is the sum of local heights and is a bilinear pairing (cf. Mazur–Tate, Coleman–Gross, Nekovář, ...)

Thm (B.–Dogra) Let $X/\mathbb{Q}$ be a nice curve of genus $g > 1$, let J be the Jacobian of X, assume $\operatorname{rk} J(\mathbb{Q}) = g$, $\operatorname{rk} NS(J) > 1$. Let p be a prime of good reduction for X s.t. $\log : J(\mathbb{Q}) \otimes \mathbb{Q}_p \to H^0(X, \Omega^1)^*$ is an isomorphism. Choose a nice correspondence Z on X. Fix a basis $\{\tau_i\}$ of the space $(H^1(X_{\mathbb{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbb{Q}_p}, \Omega^1)^*)^*$ of $\mathbb{Q}_p$-valued bilinear forms on $H^1(X_{\mathbb{Q}_p}, \Omega^1)^*$. Then there exist constants $a_i \in \mathbb{Q}_p$ s.t.

$$\rho : \begin{array}{ccc} X(\mathbb{Q}_p) & \to & \mathbb{Q}_p \\ x & \mapsto & h_p(A(x)) - \sum \alpha_i \varphi_i \circ (\pi_1, \pi_2)(A(x)) \end{array}$$

has finitely many zeros and takes values in a finite set S for points in the quadratic Chabauty set.

To "compute rational points via quadratic Chabauty", we'd like to compute this function and the finite set S.

Algorithm (QC for Modular Curves, B-Dogra-Müller-Tuitman-Vonk)

Input:
- A modular curve $X/\mathbb{Q}$ with Mordell-Weil rank $r = g$ and $\mathrm{rk}\, NS(J) > 1$, a point $b \in X(\mathbb{Q})$, and a prime p of good reduction for which the image of $J(\mathbb{Q})$ in $H^0(X, \Omega^1)^*$ has rk g.
- A covering of X by affine opens birational to a plane curve cut out by an equation satisfying Tuitman's "Assumption 1" ← (see Aws notes)
- The action of a nice correspondence Z on $H^1_{dR}(X)$.

Output:
- The quadratic Chabauty set (wrt Z above)

Steps:
1) Write the local height function $x \mapsto h_p(A(x))$ as a convergent p-adic power series on each residue disk in $X(\mathbb{Q}_p)$ by computing the relevant Hodge filtration and Frobenius structure (solve p-adic differential equation)
2) Compute the finite set S of local height values the QC function takes (in certain cases, the set $S = \{0\}$, but this is difficult in general: cf. Betts-Dogra, forthcoming work of Betts-Duque Rosero-Hashimoto-Spelier for hyperell. curves).
3) Compute the constants α_i in some way - either via

a supply of rational points on the curve or on the Jacobian (in particular, computing the p-adic heights of these points) to "fit" the height pairing, i.e., to rewrite the height pairing in terms of the basis $\{\gamma_i\}$ of the space of bilinear pairings on $H^0(X, \Omega^1)^*$.

4) Use the above to write down a convergent power series on every residue disk D and solve for all points $z \in D(\mathbb{Q}_p)$ s.t. $p(z) \in S$. Return the union of these points.

Package for applying this:

github.com/steffenmueller/QCMod (with examples)

Ex. Let X: $X_0^+(N) := X_0(N)/\langle w_N \rangle$, N prime
The non-cuspidal points on X classify unordered pairs of elliptic curves $\{E_1, E_2\}$ with an N-isogeny between them.

Let $N = 167$.
Galbraith showed that X has genus 2 and that a model for it is $y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$
We have $X(\mathbb{Q})_{\text{known}} = \{\infty^{\pm}, (-1, \pm 1)\}$.
We have $\text{rk } J(\mathbb{Q}) = 2$, $\text{rk NS } J_{\mathbb{Q}} = 2$.
Do a change of variables to move ratl points away from $\infty^{\pm}$ $\rightsquigarrow$ upshot is that we then only need to work in one affine curve. The new model has known ratl pts $(0, \pm 1), (1/2, \pm 1/8)$.
Can do in 2 different ways in Magma:
1) via 2-descent in Magma
2) By computing that the analytic rank of the unique (up to conj.) newform of level 167 and wt 2 invariant under w_{167} is equal to 1, and applying Gross-Zagier and Kolyvagin-Logachev

Fix $p = 7$ of good (and ordinary) reduction.
The Hecke operator T_7 generates the Hecke algebra.

The bulk of the computation is then computing local heights:

- fix a symplectic basis $\{\omega_0, \dots, \omega_3\}$ of $H^1_{dR}(X)$
  ↳ cup product is the standard symplectic form $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$.
- Use Tuitman's algorithm for the matrix F of Frobenius on $H^1_{dR}(X)$
- Use Eichler-Shimura to compute the matrix of the Hecke Operator T_7 on $H^1_{dR}(X)$:
$$T_7 = F^T + 7(F^T)^{-1}$$
- This gives the matrix Z representing the endomorphism on $H^1_{dR}(X)$ of a nice correspondence:
$$Z := (\mathrm{Tr}(T_7) I_4 - 4T_7) C^{-1} \qquad C = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$
- Compute the Hodge filtration (essentially principal parts of Laurent series expansions around $\infty^{\pm}$, defined over a quadratic field) and Frobenius structure (solving p-adic differential eqns using Tuitman's algorithm).
- Expand the function $x \mapsto h_7(A(x))$ as a 7-adic power series: e.g. in the residue disk of $(0,-1)$:
$$h_7(A(x)) = t - 5t^2 - 24t^3 + O(t^4, 7^2).$$
- Compute that the set of local heights away from 7 is $\{0\}$.
- Determine the global height pairing as a bilinear pairing by computing global heights on the Jacobian using Coleman-Gross heights and relate them to a basis of bilinear forms ($\sum \int \omega_i \int \omega_j$ for holomorphic ω_i, ω_j)

So in the disk of $(0,-1)$:
$$p(x(t)) = h_7(A(x)) - (-10t + \tfrac{5}{7}t^2 - 12t^3) + O(t^4, 7^2)$$
$$= 17t + {}^{9}/_{7}t^2 - 12t^3 + O(t^4, 7^2)$$

In this residue disk, p has two zeros:
1) the zero at $t=0 \Rightarrow$ recovers the rat'l point $(0,-1)$
2) another zero that gives the 7-adic point $(2\cdot 7 + O(7^2), -(1+6\cdot 7 + O(7^2)))$.

Going through all the residue disks (non-bad, non-infinite) in this way, find:
p vanishes on the 4 known rational points, as well as 4

pairs of 7-adic points in non-bad, non-infinite disks.
- use the Mordell-Weil sieve to rule out these extra points
- use the MW sieve to show that the bad disk corresponding to $\overline{(1,0)}$ and the disks at infinity do not have any rat'l points.

Thm (BDMTV) $\#X_0^+(167)(\mathbb{Q}) = 4$ and they are all cusps or CM points.

Thm (Many, including Adzaga-Arul-Beneish-Chen-Chidambaram-Keller-Ulmer): If $2 \leq g(X_0^+(N)) \leq 5$, then $X_0^+(N)(\mathbb{Q})$ contain exceptional rational points iff

$$N \in \{73, 91, 103, 125, 137, 191, 311\}.$$

This settles a 2002 conjecture of Galbraith.