An update on effective Chabauty

Jan Tuitman

KU Leuven

November 3, 2017

Rational points

$X/\mathbf{Q}$ a smooth projective curve of genus $g > 1$.

Given by (singular) plane model $f(x, y) = 0$.

$X(\mathbf{Q})$ is finite by Faltings's theorem.

Usually points are easily found by a search (if they exist).

Example ($g = 4$)

$$f(x, y) = y^3 - (x^5 - 2x^4 - 2x^3 - 2x^2 - 3x)$$
$$X(\mathbf{Q}) \supset \{(1, -2), (0, 0), (-1, 0), (3, 0), \infty\}$$

Problem

How to prove that these are all points?

Coleman integrals

Let:

- p a prime of good reduction,
- $P, Q \in X(\mathbf{Q}_p)$,
- $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

In the 80's Coleman defined path independent line integrals

$$\int_P^Q \omega$$

which can be extended to integrate over $D \in J(\mathbf{Q}_p)$, where J is the Jacobian of X (above: $D = (Q) - (P)$).

Chabauty-Coleman

Assume at least one point $b \in X(\mathbf{Q})$ is known and embed $X \hookrightarrow J$ by $P \mapsto (P) - (b)$.

Theorem (Chabauty-Coleman)

Let r denote the Mordell-Weil rank of J and suppose that $r < g$. Then there exists $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$ such that $\int_b^P \omega = 0$ for all $P \in X(\mathbf{Q})$.

Sketch of proof.

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r] \arrow[d] & X(\mathbf{Q}_p) \arrow[d] \arrow[dr, "AJ_b"] & \\
J(\mathbf{Q}) \arrow[r] & J(\mathbf{Q}_p) \arrow[r, "D \mapsto \int_D"] & H^0(X_{\mathbf{Q}_p}, \Omega^1)^*
\end{tikzcd}$$

$X(\mathbf{Q})$ lands in a subspace of $H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$ of dimension at most r. □

Effective Chabauty

A residue disk on $X_{\mathbf{Q}_p}$ is the inverse image under reduction mod p of a single point.

The integral $\int_b^P \omega$ can be expanded in a power series with a finite number of zeros on every residue disk.

This proves Mordell's conjecture in the case $r < g$ as already noted by Chabauty.

Since Coleman integrals can (in principle) be computed, this gives an algorithm to find a finite subset

$$X(\mathbf{Q}_p)_1 \subset X(\mathbf{Q}_p)$$

which contains $X(\mathbf{Q})$.

Tiny integrals

Let: $P, Q \in X(\mathbf{Q}_p)$ points in the same residue disk, $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

Then $\int_P^Q \omega$ can be computed by expanding ω in a local coordinate t on the disk:

$$\omega = \sum_{i \geq 0} c_i t^i dt$$

and integrating as usual

$$\int_{t(P)}^{t(Q)} \sum_{i \geq 0} c_i t^i dt = \sum_{i \geq 0} \frac{c_i}{i+1} (t(Q)^{i+1} - t(P)^{i+1}).$$

When P and Q not in the same residue disk, does not work: series do not converge.

Analytic continuation fails over $\mathbf{Q}_p$. Coleman: use Frobenius action on p-adic cohomology.

p-adic cohomology

Can construct p-adic cohomology space $H^1_{rig}(X_{\mathbf{Q}_p})$:

- a vector space over $\mathbf{Q}_p$ isomorphic to $H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$,
- with action F_p^* of p-th power Frobenius F_p on $X_{\mathbf{F}_p}$.

Let $\omega_1, \ldots, \omega_{2g} \in \Omega^1(X_{\mathbf{Q}_p})$ form a basis for $H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$.

Then there exist:

- a matrix $\Phi \in M_{2g \times 2g}(\mathbf{Q}_p)$,
- (overconvergent) functions $f_1, \ldots, f_{2g}$ on some open of $X_{\mathbf{Q}_p}$,

such that

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_{j=1}^{2g} \Phi_{ij} \omega_j \qquad \text{for } i = 1, \ldots, 2g.$$

We can take $\omega_1, \ldots, \omega_g$ to be a basis for $H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

General integrals

Recall that

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_{j=1}^{2g} \Phi_{ij}\omega_j \qquad \text{for } i = 1, \ldots, 2g.$$

Assume that $\mathrm{F}_p(P) = P$ and $\mathrm{F}_p(Q) = Q$ (Teichmüller points). No loss of generality, can correct with tiny integrals. Integrating, we find

$$\int_P^Q \omega_i = \int_{\mathrm{F}_p(P)}^{\mathrm{F}_p(Q)} \omega_i = \int_P^Q \mathrm{F}_p^*(\omega_i) = f_i(Q) - f_i(P) + \sum_j \Phi_{ij} \int_P^Q \omega_j.$$

So we can determine the $\int_P^Q \omega_i$ by solving the linear system

$$(\Phi - I) \int_P^Q \omega_i = f_i(P) - f_i(Q) \qquad \text{for } i = 1, \ldots, 2g.$$

Implementation

We have developed and implemented (in Magma) an algorithm to compute the action F_p^* on $H_{\mathrm{rig}}(X_{\mathbf{Q}_p})$ for any X for almost all p. The application we had in mind was computing the zeta function $Z(X_{\mathbf{F}_p}, T)$.

The package is called *pcc* and can be found on our website and GitHub. It comes with Magma since v2.23, the commands are: *ZetaFunction* and *LPolynomial*.

In joint work with Balakrishnan we have extended this to an algorithm and implementation for computing (single) Coleman integrals on arbitrary curves.

The package is called *Coleman* and can again be found on our website and GitHub.

Explicit effective Chabauty

1. Suppose an upper bound $R < g$ is known on the rank r of J.
2. Take as input points $P_1, \ldots, P_k \in X(\mathbf{Q})$.
3. Determine the subspace S of $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$ such that

$$\int_{P_1}^{P_i} \omega = 0 \qquad \text{for } i = 1, \ldots, k.$$

4. If $\dim S \leq g - R$ then for all $\omega \in S$ and $P \in X(\mathbf{Q})$

$$\int_{P_1}^{P} \omega = 0 \qquad \text{for } i = 1, \ldots, k.$$

5. Expand these conditions in power series and find the candidate points on every residue disk of $X_{\mathbf{Q}_p}$.

Example

Let us return to the example $f(x,y) = y^3 - (x^5 - 2x^4 - 2x^3 - 2x^2 - 3x)$. The Magma function *RankBounds()* proves that the rank of J is 1. This uses work of Poonen-Schaefer ('97). Now we call:

```
> load "coleman.m";
> Q:=y^3 - (x^5 - 2*x^4 - 2*x^3 - 2*x^2 - 3*x);
> p:=7;
> N:=15;
> data:=coleman_data(Q,p,N);
> Qpoints:=Q_points(data,1000); // PointSearch
> #vanishing_differentials(Qpoints,data:e:=50);
3
> #effective_chabauty(data,1000:e:=50),#Qpoints;
5 5
```

This proves that our list of rational points is complete.

Problems

Some examples of what can go wrong:

- No upper bound on rank r. Assume some conjectures?
- $(P) - (Q)$ with $P, Q \in X(\mathbf{Q})$ do not generate full rank subgroup of $J(\mathbf{Q})$. Then $\dim S \leq g - R$ is never satisfied. Use more general $D \in J(\mathbf{Q})$? Currently, only points in $X(\mathbf{Q}_p)$ allowed.
- Too many points found: $X(\mathbf{Q}_p)_1$ strictly larger than $X(\mathbf{Q})$. Use other prime p, combine with Mordell-Weil sieving?
- Rank r known but $r \geq g$. Method as explained so far breaks down. However, recently some succes with non-abelian effective Chabauty.

What is non-abelian Chabauty? Let's see an example.

The cursed curve

Split Cartan modular curve of level 13:

$$X_s(13) = X(13)/C_s(13)^+$$

where $C_s(13)^+$ is the normaliser of a split Cartan subgroup of $GL_2(\mathbf{F}_{13})$.

Baran '14 found a defining equation, which we can rewrite as

$$f(x, y) = y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y.$$

The closure in $\mathbf{P}^2_{\mathbf{Q}}$ is a smooth plane quartic, so $g = 3$.

Jacobian simple and by known instance of BSD one finds $r = 3$.

What about the rational points?

Rational points

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk)

The rational points on $X_s(13)$ are the seven known ones (six CM points and one cusp).

Paper 'Explicit Chabauty-Kim for the split Cartan modular curve of level 13' should be on arxiv very soon.

Corollary

There does not exist an elliptic curve $E/\mathbf{Q}$ without CM such that the image of its mod ℓ Galois representation is contained in the normalizer of a split Cartan subgroup of $GL_2(\mathbf{F}_\ell)$ for $\ell = 13$.

For all $\ell \neq 13$ it was already known (Bilu-Parent-Rebolledo '11) whether such elliptic curves exist or not (for $\ell \leq 7$ yes, otherwise no).

Non-abelian Chabauty

Here $D \to \int_D$ gives an isomorphism

$$J(\mathbf{Q}) \otimes \mathbf{Q}_p \to H^1_{\mathrm{rig}}(X_{\mathbf{Q}_p})^*.$$

Therefore, we cannot find the global points among the local ones using linear relations in the Abel-Jacobi map.

The idea of Kim's non-abelian Chabauty program is to refine the Abel-Jacobi map, by replacing linear relations by higher degree ones.

$$X(\mathbf{Q}_p) \supset X(\mathbf{Q}_p)_1 \supset X(\mathbf{Q}_p)_2 \supset \ldots \supset X(\mathbf{Q})$$

In our case it turns out that $X(\mathbf{Q}_p)_2 = X(\mathbf{Q})$.

Quadratic Chabauty pairs

Fix $b \in X(\mathbf{Q})$. A quadratic Chabauty pair is

- a function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$,
- a finite set $\Upsilon \subset \mathbf{Q}_p$,

satisfying the following conditions:

1. On each residue disk, the map
$$(AJ_b, \theta) : X(\mathbf{Q}_p) \to H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \times \mathbf{Q}_p$$
has Zariski dense image and is given by a power series.
2. There exist
    - an endomorphism E of $H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$,
    - a functional $c \in H^0(X_{\mathbf{Q}_p}, \Omega^1)^*$,
    - a bilinear form $B : H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes H^0(X_{\mathbf{Q}_p}, \Omega^1)^* \to \mathbf{Q}_p$,

   such that, for all $x \in X(\mathbf{Q})$:
$$\theta(x) - B\left(AJ_b(x), E(AJ_b(x)) + c\right) \in \Upsilon.$$

Nice correspondences

We will construct θ from a nice correspondence.

Let Z be a correspondence on X, i.e. a divisor on $X \times X$.

We denote:

- τ the involution $(x_1, x_2) \mapsto (x_2, x_1)$ on $X \times X$,
- $\pi_1, \pi_2 : X \times X \to X$ the canonical projections.

Z is symmetric if there exist $Z_1, Z_2 \in Pic(X)$ such that

$$\tau_* Z = Z + \pi_1^*(Z_1) + \pi_2^*(Z_2).$$

Induces endomorphism ξ_Z of $H^1_{\mathrm{dR}}(X)$ and class in $H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) \otimes H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$.

Z is nice if nontrivial, symmetric and $\mathrm{Tr}(\xi_Z) = 0$.

Unipotent overconvergent F-isocrystals

Let $Y = X - x^{-1}(\infty)$. Take $\vec{\omega} = \{\omega_1, \ldots \omega_6\}$ to be a basis of $H^1_{\mathrm{dR}}(X)$.

Put the connection $\nabla = d - \Lambda$ on $\mathcal{A}_{Z,b} = \mathcal{O}_Y \oplus \mathcal{O}_Y^{\oplus 6} \oplus \mathcal{O}_Y$:

$$\Lambda = \begin{pmatrix} 0 & 0 & 0 \\ \vec{\omega} & 0 & 0 \\ \eta & \vec{\omega}^t Z & 0 \end{pmatrix}$$

η is determined by: 1) is logarithmic 2) ∇ extends to a holomorphic connection on X.

By a crystalline comparison theorem $A_{Z,b}$ admits a Frobenius structure, i.e. an isomorphism

$$F : \mathrm{F}_p^* \mathcal{A}_{Z,b} \to \mathcal{A}_{Z,b}$$

horizontal w.r.t ∇, turning $(\mathcal{A}_{Z,b}, \nabla)$ into a unipotent overconvergent F-isocrystal.

Frobenius structure

Let $\tilde{b}$ be the Teichmüller lift in the residue disk of b (i.e. $\mathrm{F}_p(\tilde{b}) = \tilde{b}$).

The matrix of the Frobenius structure F is given by

$$G = \begin{pmatrix} 1 & 0 & 0 \\ \vec{f} & \Phi & 0 \\ h & \vec{g}^t & p \end{pmatrix}$$

where:

$$\begin{aligned} \mathrm{F}_p^* \vec{\omega} &= d\vec{f} + \Phi \vec{\omega} & f(\tilde{b}) &= 0 \\ d\vec{g}^t &= d\vec{f}^t Z \Phi & & \\ dh &= \vec{\omega}^t \Phi^t Z \vec{f} + d\vec{f}^t Z \vec{f} - \vec{g}^t \vec{\omega} + \mathrm{F}_p^* \eta - p\eta & h(\tilde{b}) &= 0 \end{aligned}$$

This can be solved using our algorithms!

Construct θ_Z

For any $x \in X(\mathbf{Q}_p)$ can pull back $A_Z(b)$:

$$A_Z(b,x) = x^*(A_Z(b)).$$

This is a ϕ-module in the sense of p-adic Hodge theory. Note that ϕ is G evaluated at x.

$A_Z(b)$ is an extension and carries a Hodge filtration compatible with ϕ.

For such extensions of filtered ϕ-modules, Nekovar has defined a p-adic height function $h_p()$. We set

$$\theta_Z(x) = h_p(A_Z(b,x)).$$

For any nice correspondence there is a finite set Υ such that (θ, Υ) is a quadratic Chabauty pair (with $E = \xi_Z$).

Some computational details

$$f(x,y) = y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y.$$

$$\vec{\omega} := \begin{pmatrix} 1 \\ x \\ y \\ -160x^4/3 + 736x^3/3 - 16x^2y/3 + 436x^2/3 - 440xy/3 + 68y^2/3 \\ -80x^3/3 + 44x^2 - 40xy/3 + 68y^2/3 - 32 \\ -16x^2y + 28x^2 + 72xy - 4y^2 - 160x/3 + 272/3 \end{pmatrix} dx/(\partial f/\partial y)$$

We use the correspondences Z with $\xi_Z = 6a_q - \mathrm{Tr}(a_q)Id$ for $q = 7, 11$:

$$Z_1 = \begin{pmatrix} 0 & 112 & -656 & -6 & 6 & 6 \\ -112 & 0 & -2576 & 15 & 9 & 27 \\ 656 & 2576 & 0 & 3 & 3 & -3 \\ 6 & -15 & -3 & 0 & 0 & 0 \\ -6 & -9 & -3 & 0 & 0 & 0 \\ -6 & -27 & 3 & 0 & 0 & 0 \end{pmatrix} Z_2 = \begin{pmatrix} 0 & -976 & -1104 & 10 & -6 & 18 \\ 976 & 0 & -816 & -3 & 1 & 3 \\ 1104 & 816 & 0 & -3 & 3 & -11 \\ -10 & 3 & 3 & 0 & 0 & 0 \\ 6 & -1 & -3 & 0 & 0 & 0 \\ -18 & -3 & 11 & 0 & 0 & 0 \end{pmatrix}$$