Explicit Motivic Chabauty-Kim Method

D. Corwin

September 21, 2023

Talk Overview

Table of Contents

Part I: Higher Nonabelian Chabauty

Hyperbolic Curves and Siegel-Faltings

Faltings' Theorem is best explained as part of a general statement that includes Siegel's Theorem:

Theorem: Siegel-Faltings

If X is a smooth *hyperbolic* curve over $R = \mathcal{O}_K[1/S]$ for a number field K and finite set of places S, then $X(R)$ is finite.

Remark: If X is proper, then $X(R) = X(K)$

Definition: Hyperbolic Curve

An algebraic curve X over a subring R of $\mathbb{C}$ is *hyperbolic* if the manifold $X(\mathbb{C})$ has negative Euler characteristic
Equivalently: iff its fundamental group is non-abelian

- Open problem (Effective Faltings): compute $X(R)$ given X and R

Nonabelian Chabauty

- For X hyperbolic, Kim defines a series

$$\mathcal{I}^R_{CK,1} \subseteq \mathcal{I}^R_{CK,2} \subseteq \mathcal{I}^R_{CK,3} \subseteq \cdots$$ [i]

of sets of p-adic analytic functions on $X(\mathbb{Q}_p)$ with

$$X(R) \subseteq \cdots \subseteq Z(\mathcal{I}^R_{CK,2}) \subseteq Z(\mathcal{I}^R_{CK,1}) \subseteq X(\mathbb{Z}_p)$$

- If ranks of certain "generalized Selmer groups" (depending on n) are not too large, then $\mathcal{I}^R_{CK,n} \neq \{0\}$ (and hence $\#Z(\mathcal{I}^R_{CK,n}) < \infty$)
- Conjectures on Galois cohomology imply that $\mathcal{I}^R_{CK,n} \neq \{0\}$ for $n >> 0$
- The Quadratic Chabauty method of Balakrishnan et al computes $\mathcal{I}_{CK,2}$ in many cases by relating the functions to p-adic heights.

Overarching Goal

Compute $\mathcal{I}^R_{CK,n}$ for a general hyperbolic curve X, integer n (and S-integer ring R)

[i] We suppress R if X is proper.

Kim's Conjecture

Conjecture (Kim et al., 2014)

Let $K = \mathbb{Q}$. For sufficiently large n, the set[a] $Z(\mathcal{I}^R_{CK,n})$ of common zeroes of functions in $\mathcal{I}^R_{CK,n}$ is precisely $X(R)$.

[a] In fact, one really wants the (not necessarily reduced) analytic subspace.

Kim's conjecture reduces effective Faltings over $\mathbb{Q}$ to the problem of computing $\mathcal{I}_{CK,n}$ as follows:

- Given a proper hyperbolic curve X, we embed it into projective space $\mathbb{P}^n$
- By night, we search points of $\mathbb{P}^n(\mathbb{Q})$of larger and larger height, creating a list of elements of $X(\mathbb{Q})$
- By day, we compute $\mathcal{I}_{CK,n}$ for larger and larger n and use Newton polygons to bound the size of $Z(\mathcal{I}_{CK,n})$
- If our list has the same size as our bound for $Z(\mathcal{I}_{CK,n})$, we are done

Part II: Results of C–Dan-Cohen–Wewers

The case of $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$

Observation

The following sets are naturally in bijection for a ring R

- $x, w \in R^\times$ such that $x + w = 1$ (the "Unit Equation")
- $x, y \in R$ such that $x(1-x)y = 1$ (via $y = \frac{1}{xw}$)
- $X(R)$ with $X = \mathbb{P}^1 \setminus \{0, 1, \infty\} = \operatorname{Spec} \mathbb{Z}\left[x, \frac{1}{x(1-x)}\right]$

- Proven finite for $R = \mathcal{O}_K[1/S]$ by Siegel in 1929
- Reproven by Minhyong Kim in 2004 for $K = \mathbb{Q}$ (aka $R = \mathbb{Z}[1/N]$) $\Rightarrow$ first test case of Kim's method!
- The Galois representations/motives are mixed Tate; this is the **Mixed Tate case**

Recent Explicit Results

p-adic iterated integrals on X include p-adic polylogarithms $\mathrm{Li}_k^p(z)$

Theorem (Dan-Cohen–Wewers, 2013)

- For $R = \mathbb{Z}[1/\ell]$ and all $p \neq \ell$, the following Coleman function is in $\mathcal{I}^R_{CK,2}$:

$$2\mathrm{Li}_2^p(z) - \log^p(z)\mathrm{Li}_1^p(z)$$

- For $R = \mathbb{Z}[1/2]$ and $p \neq 2$, the following Coleman function is in $\mathcal{I}^R_{CK,4}$:

$$24\log^p(2)\zeta^p(3)\mathrm{Li}_4^p(z) + \frac{8}{7}\left(\log^p(2)^4 + 24\mathrm{Li}_4^p(\frac{1}{2})\right)\log^p(z)\mathrm{Li}_3^p(z)$$
$$+\left(\frac{4}{21}\log^p(2)^4 + \frac{32}{7}\mathrm{Li}_4^p(\frac{1}{2}) + \log^p(2)\zeta^p(3)\right)\log^p(z)^3\log^p(1-z)$$

Recent Results, cont.

- In 2015, Dan-Cohen posted a preprint[ii] showing that this could be made into an algorithm, whose halting is conditional on refinements of conjectures due to Kim and Goncharov.

Theorem (C–Dan-Cohen, 2017)

For $R = \mathbb{Z}[1/3]$ and $p \neq 2, 3$, the following Coleman function is in $\mathcal{I}^R_{CK,4}$:

$$\zeta^p(3)\log^p(3)\mathrm{Li}^p_4(z) - \left(\frac{18}{13}\mathrm{Li}^p_4(3) - \frac{3}{52}\mathrm{Li}^p_4(9)\right)\log^p(z)\mathrm{Li}^p_3(z)$$
$$-\frac{(\log^p(z))^3\mathrm{Li}^p_1(z)}{24}\left(\zeta^p(3)\log^p(3) - 4\left(\frac{18}{13}\mathrm{Li}^p_4(3) - \frac{3}{52}\mathrm{Li}^p_4(9)\right)\right),$$

13 in denominator related to "$\mathcal{L}_3(\xi_2) = \frac{13}{6}\zeta(3)$" on p.6 of *Classical and Elliptic Polylogarithms and Special Values of L-Series* by Zagier and Gangl

[ii] Now published in Algebra and Number Theory

Recent results, cont.

- Dan-Cohen–Wewers and C–Dan-Cohen have used these functions to verify[iii] a version of Kim's Conjecture for integral points in special cases:

Conjecture (Kim et al., 2014)

The space of common zeroes of elements of $\mathcal{I}^R_{CK,n}$ is precisely $X(R)$ for sufficiently large n.

- Another article of C–Dan-Cohen presents an improved algorithm
- Kim's conjecture and some standard conjectures about mixed motives imply the algorithm halts
- If the algorithm halts, then it provably gives the correct answer

[iii] In C–Dan-Cohen, we actually showed that one needs multiple polylogarithms (not just polylogarithms) to make the conjecture work, yet all our functions above involve only polylogarithms. However, one may bring multiple polylogarithms into the picture using the S_3-action on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Punctured Elliptic Curve $X = E'$

Let $X = E' = E \setminus \{O\}$ for some elliptic curve $E/\mathbb{Q}$ (given by $y^2 = x^3 + ax + b$) for which $4a^3 + 27b^2$ is a unit in $R = \mathcal{O}_K[1/S]$

Theorem (Siegel)

$|E'(R)| < \infty$; i.e., $y^2 = x^3 + ax + b$ has finitely many solutions for $x, y \in R$

- Also proven by Siegel; re-proven when E is CM by Kim.
- Simplest *non-rational* and non-mixed-Tate case of Chabauty-Kim

Chabauty-Kim for a Punctured Elliptic Curve

- Set $\eta_0 := \frac{dx}{y}$ and $\eta_1 = \frac{xdx}{y}$
- Set $J_1 := \int \eta_0$, $J_2 := \int \eta_0\eta_1$, $J_3 := \int \eta_0\eta_1\eta_0$, and $J_4 := \int \eta_0\eta_1\eta_1 + 2\int \eta_1$

Theorem (C, 2021)+(C–Dan-Cohen, 2023)

If $\ell \neq p$ are primes and E is an elliptic curve over $\mathbb{Q}$ of p-Selmer rank 1 with good ordinary reduction at p and $\mathcal{L}_p(E,2) \neq 0$, then there is a function of the form

$$c_1 J_4 + c_2 J_3 + c_3 J_1 J_2 + c_4 J_1^3 + c_5 J_1$$

in $\mathcal{I}_{CK,3}^{\mathbb{Z}[1/\ell]}$, with $c_i \in \mathbb{Q}_p$.

In progress: computing for specific elliptic curves, projective examples

Can say more about the c_i:

Bonus Slide: What the Function *Actually* Looks Like

$$(-2f_{\pi_0}f_\tau f_{\sigma_0})J_4 + (f_{\pi_0}f_\tau f_{\sigma_1})J_3 - (f_{\sigma_1}(f_{\tau\pi_0} - f_{\pi_0\tau}) - 2f_{\sigma_0}f_{\pi_1\tau})J_1J_2$$
$$- \left(\frac{f_{\pi_0}f_\tau(f_{\sigma_1}f_{\pi_0\pi_1\pi_0} - 2f_{\sigma_0}f_{\pi_0\pi_1^2}) - (f_{\sigma_1}(f_{\tau\pi_0} - f_{\pi_0\tau}) - 2f_{\sigma_0}f_{\pi_1\tau})(f_{\pi_0}f_{\pi_0\pi_1})}{f_{\pi_0}^3} \right) J_1^3$$
$$+(4f_{\pi_1}f_\tau f_{\sigma_0})J_1$$

with

- $f_{\pi_i} = \int_b^z \eta_i$ for z a generator of $E(\mathbb{Q})$ [iv]
- $f_\tau = \log^p(\ell)$ [v]
- f_{σ_i} related to syntomic regulator from $K_2(E)^{(2)}_{\text{odd}}$
- Combinations are Tannakian periods satisfying "shuffle relations"

[iv] aka syntomic regulator applied to $z \in K_0(E)$

[v] aka syntomic regulator applied to $\ell \in K_1(R)$

Explaining the p-adic L-Function

- The condition $\mathcal{L}_p(E,2) \neq 0$ is used to show that $H^1_f(G_{\mathbb{Q}}; V_p(E)^\vee) = 0$
- Here H^1_f is a Bloch-Kato Selmer group, and $V_p(E)^\vee = V_p(E)(-1)$ is the dual of the p-adic Tate module
- The implication $\mathcal{L}_p(E,2) \neq 0 \Rightarrow H^1_f(G_{\mathbb{Q}}; V_p(E)^\vee) = 0$ uses modularity of E and Kato's Iwasawa Main Conjecture
- To check $\mathcal{L}_p(E,2) \neq 0$, we may approximate it using Manin symbols:

$$\mathcal{L}_p(E,2) = \lim_{n\to\infty} \sum_{1\leq a<p^n} \left(\frac{a}{\alpha^n} \left[\frac{a}{p^n}\right]^+ - \frac{a}{\alpha^{n+1}} \left[\frac{a}{p^{n-1}}\right]^+ \right)$$

where α is the unit root of $T^2 - a_p(E)T + p$ and

$$[r]^+ = \frac{1}{\Omega_E} \operatorname{Re}\left(2\pi i \int_{i\infty}^{r} f(z)\,dz\right)$$

is a Manin symbol, with f the modular form associated to E.

- Manin symbols are rational numbers and are implemented in SageMath!

Part III: Tannakian Selmer Varieties

What's hard about computing $\mathcal{I}_{CK,n}$?

Let $X/\mathbb{Q}$ be proper hyperbolic (good reduction outside S). Recall Kim's cutter:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) \\ \Big\downarrow{\scriptstyle \kappa} & & \Big\downarrow{\scriptstyle \kappa_p} \\ H^1_{f,S}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}); U_n) & \xrightarrow{\mathrm{loc}_n} & U_n^{\mathrm{dR}}/F^0 U_n^{\mathrm{dR}} \end{array}$$

- $\mathcal{I}_{CK,n}$ is the pullback under κ_p of the ideal of functions vanishing on the image of loc_n
- Goal: compute loc_n (in coordinates we know κ_p)

Two problems:

1. $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is really big and complicated
2. f is defined by B_{cris}, which is really big and complicated

The Tannakian Formalism

- Idea: consider the category of all relevant $G_{\mathbb{Q}}$-representations (depends on $J = \mathrm{Jac}(X)$ and $R = \mathbb{Z}[1/S]$)

Definition

$\mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{sf,S}}(G_{\mathbb{Q}}, J)$ is the category of geometric Galois representations with a weight filtration whose graded pieces in $\langle V_p(J)\rangle^{\otimes}$ and extension structure unramified outside S.

This category is not as hard to describe:

- Its semisimple objects form the category of representations of the p-adic monodromy group $\mathbb{G}$ of J (close to Mumford-Tate group $\mathrm{MT}(J)$)
- $\mathrm{Ext}^1(\mathbb{Q}_p, V) \cong H^1_{f,S}(G_{\mathbb{Q}}; V)$ for V of negative weight
- Ext^i (conjecturally) vanishes for $i \geq 2$

The Tannakian Selmer Variety

- We use the 'de Rham' fiber functor sending V to $\mathrm{D}_{\mathrm{cris}}(V)$
- By the Tannakian formalism,

$$\mathrm{Rep}^{\mathrm{sf,S}}_{\mathbb{Q}_p}(G_{\mathbb{Q}}, J) \cong \mathrm{Rep}^{\mathrm{alg}}(\pi_1^{\mathrm{MA}}(R, J))$$

  for a pro-algebraic group $\pi_1^{\mathrm{MA}}(R, J)$ - an extension of $\mathbb{G}$ by a pro-unipotent group $U(R, J)$
- By the description of the category, $U(R, J)$ is a free unipotent group on the product of the vector spaces $H^1_{f,S}(G_{\mathbb{Q}}; V)$ for $V \in \mathrm{Rep}^{\mathrm{alg}}(\mathbb{G})$ irreducible of negative weight
- Key Upshot:

$$H^1_{f,S}(G_{\mathbb{Q}}; U_n) \cong H^1(\pi_1^{\mathrm{MA}}(R, J); U_n^{\mathrm{dR}})$$

- The RHS[vi] is a *Tannakian Selmer Variety*

[vi] or disjoint unions of it à la Betts–Dogra

Computing the Tannakian Selmer Variety

- Once we know $\pi_1^{\mathrm{MA}}(R, J)$, we can compute $H^1(\pi_1^{\mathrm{MA}}(R, J); U_n^{\mathrm{dR}})$ using

Theorem (C, 2021)

[a] For a pro-unipotent group Π with action of $\pi_1^{\mathrm{MA}}(R, J)$, we have

$$H^1(\pi_1^{\mathrm{MA}}(R, J); \Pi) \cong Z^1(U(R, J); \Pi)^{\mathbb{G}}.$$

[a] Generalizing Dan-Cohen–Wewers for $\mathbb{G} = \mathbb{G}_m$)

- The latter is the space of $\mathbb{G}$-equivariant cocycles and can be computed by knowing the abstract structure of $U(R, J)$ and its $\mathbb{G}$-action
- More specifically, for each V irreducible, we get $d_S(V) := \dim H^1_{f,S}(G_{\mathbb{Q}}; V)$ coordinates on $H^1(\pi_1^{\mathrm{MA}}(R, J); U_n^{\mathrm{dR}})$ for each copy of V in U_n
- The Bloch-Kato Conjectures give a conjectural computation of $d_S(V)$
- Remark: For given n, we need only V appearing in $V_p(J)^{\otimes m}$ for $1 \leq m \leq n$

Part IV: Localization and p-adic periods

joint with Ishai Dan-Cohen

Localization and Universal Cocycle Evaluation

The approach of C–Dan-Cohen in the mixed Tate case suggests that loc_n is the base-change along a special point $\mathrm{per}_p\colon \operatorname{Spec}\mathbb{Q}_p \to U(R,J)$ of the *universal cocycle evaluation map*

$$\mathfrak{ev}_{U_n,F_{\mathbb{Q}},S,J}\colon Z^1(U(R,J);U_n^{\mathrm{dR}})^{\mathbb{G}} \times U(R,J) \to U_n^{\mathrm{dR}} \times U(R,J)^{\text{vii}}$$

- This map sends $c \in Z^1(U(R,J);U_n^{\mathrm{dR}})^{\mathbb{G}}$ and $u \in \times U(R,J)$ to $(c(u),u) \in U_n^{\mathrm{dR}} \times U(R,J)$.
- The map $\mathrm{per}_p\colon \operatorname{Spec}\mathbb{Q}_p \to U(R,J)$ was defined in the mixed Tate case by Chatzistamatiou–Ünver
- Soon forthcoming work of C–Dan-Cohen defines per_p in general (more details ahead)

[vii] composed with the projection $U_n^{\mathrm{dR}} \to U_n^{\mathrm{dR}}/F^0U_n^{\mathrm{dR}}$

The p-adic period map

- The coordinate ring of the pro-unipotent part is a Hopf algebra we call

$$A(R, J)$$

- For $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, is it graded; for $X = E'$, it has a GL_2-action; more generally, an action of $\mathbb{G}$
- The map per_p is equivalently a ring homomorphism $\mathrm{per}_p \colon A(R, J) \to \mathbb{Q}_p$
- Elements of $A(R, J)$ can be seen as *motivic periods* (sense of Grothendieck, Kontsevich–Zagier, Brown), and per_p sends them to their p-adic (Coleman) period
- In fact, the elements $f_\tau, f_{\tau\pi_0}, f_{\sigma_0}, f_{\pi_0\pi_1}$, etc from Slide 14 are p-adic periods of an abstract basis of $A(R, J)$!
- Our result in fact relates per_p not only to loc_n but to κ_p in Kim's cutter:

Theorem of C–Dan-Cohen

Theorem (C–Dan-Cohen, 2023)

There is a point

$$\mathrm{per}_p \colon \operatorname{Spec} \mathbb{Q}_p \to U(R, J),$$

satisfying the following property:
For all

$$c \in Z^1(U(R, J), U_n^{\mathrm{dR}})^{\mathbb{G}}(\mathbb{Q}_p),$$

the composition

$$c/F^0 \circ \mathrm{per}_p \colon \operatorname{Spec} \mathbb{Q}_p \xrightarrow{\mathrm{per}_p} U(R, J) \xrightarrow{c} U_n^{\mathrm{dR}} \twoheadrightarrow U_n^{\mathrm{dR}}/F^0 U_n^{\mathrm{dR}}$$

is $\mathrm{loc}_n(c) \in U_n^{\mathrm{dR}}/F^0 U_n^{\mathrm{dR}}(\mathbb{Q}_p)$.

The explicit result of (C, 2021) on Slide 13 depends on this theorem.

Consequences and Future Work

- The result of Slide 24 reduces computation of $\mathcal{I}^R_{CK,n}$ to computing a basis of $A(R,J)$ on which we know per_p
- We can actually the theorem to do this: given $z \in X$ and $\omega \in \mathcal{O}(U_n^{\mathrm{dR}}/F^0 U_n^{\mathrm{dR}})$, we can pull back ω along $\kappa(z)$ to get an element of $A(R,J)$ denoted $I^{\mathfrak{m}}(b:\omega:z)$ known as a *motivic iterated integral*
- We then have
$$\mathrm{per}_p(I^{\mathfrak{m}}(b:\omega:z)) = \int_b^z \omega,$$
an iterated Coleman integral.
- More generally, if we replace X by any variety whose unipotent étale fundamental group lies in $\mathrm{Rep}^{\mathrm{sf,S}}_{\mathbb{Q}_p}(G_{\mathbb{Q}}, J)$, we get more motivic iterated integrals
- More work must also be done to understand the action of $U(R,J)$ on U_n
- The eventual goal is an algorithm depending on the Bloch-Kato conjectures with halting like the one before for any hyperbolic curve X

Useful References/Credits

- Explicit Motivic Mixed Elliptic Chabauty-Kim, David Corwin, arXiv
- Tannakian Selmer Varieties, David Corwin, website (`math.bgu.ac.il/~corwind`)
- p-Adic Periods and Selmer Scheme Images, David Corwin and Ishai Dan-Cohen, soon to appear on arXiv

Published:

- Mixed Tate Motives and the Unit Equation, Ishai Dan-Cohen and Stefan Wewers
- Mixed Tate Motives and the Unit Equation II, Ishai Dan-Cohen
- The polylog quotient and the Goncharov quotient in computational Chabauty-Kim theory I, David Corwin and Ishai Dan-Cohen
- The polylog quotient and the Goncharov quotient in computational Chabauty-Kim theory II, David Corwin and Ishai Dan-Cohen

Thank You!