Rational points on curves via algebraic cycles on surfaces

March 12, 2025

. . . or . . .

Nonabelian Chabauty V: The Jacobian Strikes Back!

March 12, 2025

Two questions in nonabelian Chabauty

1. How do we prove that $X(\mathbb{Q}_p)_U$ is finite?
2. How do we compute $X(\mathbb{Q}_p)_U$?

- In this talk I want to explain *computational* approaches to these questions, and advertise exciting questions in computational number theory related to mixed motives and algebraic cycles.
- These subjects are ripe for computational experimentation!

Please contact aws@awsmath.org with any questions.

The topic for AWS 2026 will be *Computational aspects of arithmetic geometry and cryptography*

Funded by the National Science Foundation, and organized in partnership with the Clay Mathematics Insti

The Chabauty–Coleman method

The Chabauty–Coleman method gives an approach to determining the rational points of X using the Jacobian J of X. We have a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \to & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ X(\mathbb{Q}_p) & \to & J(\mathbb{Q}_p) \end{array}$$

We have $J(\mathbb{Q}_p) \approx \mathbb{Z}_p^g$. If $r < g$, then the topological closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ is $\approx \mathbb{Z}_p^{r'}$ where $r' \leq r$.

How does Chabauty–Coleman work?

Suppose someone gives you a hyperelliptic curve. How do you apply the Chabauty–Coleman method?

- Carry out a 2-descent to verify $r < g$.
- Find a set of divisors of degree zero generating a finite index subgroup of $J(\mathbb{Q})$.
- Some p-adic computations and Mordell–Weil sieving.

In this talk I want to talk about generalising the *first two* steps in the context of nonabelian Chabauty (the last step is better understood).

Motivation: the Chabauty–Coleman–Kim method

Let X be a smooth projective geometrically irreducible curve of genus $g > 1$ over $\mathbb{Q}$. The Chabauty–Coleman–Kim method produces a nested sequence

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

such that $X(\mathbb{Q}_p)_1$ is the usual Chabauty–Coleman set. This generalisation is obtained by "getting rid of the Jacobian".

Theorem (Kim)

$X(\mathbb{Q}_p)_2$ is finite whenever

$$\mathrm{rk} J(\mathbb{Q}) < \frac{1}{2}(3g-2)(g+1) - \mathrm{rk} H^1_f(G_{\mathbb{Q}}, \wedge^2 V_p J).$$

where $V_p(J) := T_p(J) \otimes \mathbb{Q}_p$.

In general, finiteness of $X(\mathbb{Q}_p)_n$ is implied by bounding the dimension of H^1_f of certain summands of $V_p J^{\otimes i}$, for $1 \leq i \leq n$.

Definition: 'Full-fat' versus 'diet' Quadratic Chabauty

- Recall that if $\mathrm{rk} J(\mathbb{Q}) < g + \rho(J) - 1$, then one can prove finiteness of $X(\mathbb{Q}_p)_2$, and can sometimes compute $X(\mathbb{Q}_p)_2$ using p-adic heights.
- In this talk I will mostly be interested in describing $X(\mathbb{Q}_p)_2$ when $\rho(J) = 1$.
- I will henceforth distinguish between 'full-fat quadratic Chabauty' (which works with the whole of $X(\mathbb{Q}_p)_2$) and 'diet quadratic Chabauty' which just use the part coming from p-adic heights.
- Although it is widely believed that diet quadratic Chabauty is better for you, some experts dispute this.

The Chabauty–Kim method in the best of all possible worlds

More generally, the Bloch–Kato conjectures give a precise prediction on an n (not necessarily optimal) such that $X(\mathbb{Q}_p)_n$ is finite.

n	Bloch–Kato $\implies$ $X(\mathbb{Q}_p)_n$ finite when
1	$r < g$
2	$r < g^2 + \rho(J) - 1$
3	$r < \frac{4g^3+3g^2-4g-3}{3} + \rho(J)$
4	$r < \frac{6g^4+4g^3-6g^2-4g}{3} + \rho(J)$
5	$r < \frac{48g^5+30g^4-40g^3-30g^2-8g}{15} + \rho(J)$

Here $\rho(J) := \mathrm{rk}\mathrm{NS}(J(\mathbb{Q}))$. Note that $X(\mathbb{Q}_p)_2$ is finite (unconditionally) when $r < g + \rho(J) - 1$. For example, for genus 2 curves we expect $X(\mathbb{Q}_p)_3$ is finite whenever $r < 12$, $X(\mathbb{Q}_p)_4$ is finite whenever $r < 33$, and $X(\mathbb{Q}_p)_5$ is finite whenever $r < 105$.

Part 1: how do we bound Bloch–Kato Selmer groups?

Given a continuous finite dimensional $\mathbb{Q}_p$ -representation V of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, define

$$H^1_f(G_{\mathbb{Q}}, V) := \cap_v \mathrm{Ker}(H^1(G_{\mathbb{Q}_v}, V) \to H^1(G_{\mathbb{Q}_v}, V)/H^1_f(G_{\mathbb{Q}_v}, V))$$

where the intersection is over all primes v, and

$$H^1_f(G_{\mathbb{Q}_v}, V) := \begin{cases} \mathrm{Ker}(H^1(G_{\mathbb{Q}_v}, V) \to H^1(G_{\mathbb{Q}_v}, V \otimes B_{\mathrm{cris}})), & v = p. \\ \mathrm{Ker}(H^1(G_{\mathbb{Q}_v}, V) \to H^1(I_v, V)), & v \neq p. \end{cases}$$

To verify this expectation in examples, we need *explicit methods* for BK Selmer groups.

Descent for Selmer groups of hyperelliptic curves

(Cassels, Schaefer, Bruin, Poonen–Schaefer, Stoll, ...)
Let X/K be a hyperelliptic curve given by a polynomial f of odd degree, where K is a field of characteristic different from 2. For simplicity, suppose f is irreducible and $\alpha \in K^{\mathrm{sep}}$ is a root.
Then we have an isomorphism

$$H^1(K, J[2]) \simeq \mathrm{Ker}(K(\alpha)^\times \otimes \mathbb{F}_2 \xrightarrow{\mathrm{Nm}} K^\times \otimes \mathbb{F}_2).$$

Under this isomorphism, for $z, w \in (X - W)(K)$ (where $W \subset X$ is the set of Weierstrass points), the 2-Kummer homomorphism is given by the "$(x - t)$ map"

$$z - w \mapsto (x(z) - \alpha)/(x(w) - \alpha) \in \mathrm{Ker}(K(\alpha)^\times \otimes \mathbb{F}_2 \xrightarrow{\mathrm{Nm}} K^\times \otimes \mathbb{F}_2).$$

These results were extended to the case of even degree polynomials (and more generally to cyclic covers of $\mathbb{P}^1$) by Poonen and Schaefer.

Results

Theorem (D.)

Let X be the curve $y^2 - y = x^5 - x$. Then $\mathrm{rk} J(\mathbb{Q}) = 3$, $\dim H^1_f(G_{\mathbb{Q}}, \wedge^2 V_2(J)/\mathbb{Q}_2(1)) = 2$ *and*

$$X(\mathbb{Q}) = \left\{ \begin{array}{c} \infty, (0,1), (\frac{1}{4}, \frac{15}{32}), (2,6), (3,-15), (1,1), (30,-4929), \\ (-1,1), (1,0), (30,4930), (3,16), (\frac{1}{4}, \frac{17}{32}), (2,-5), \\ (0,0), (-1,0), (-\frac{15}{16}, -\frac{185}{1024}), (-\frac{15}{16}, \frac{1209}{1024}) \end{array} \right\}$$

Theorem (D.)

Of the $7,224$ *rank 2 genus 2 curves with a rational Weierstrass point in the LMFDB, at least 3,323 satisfy* $\#X(\mathbb{Q}_2)_2 < \infty$.

Two-descent for BK Selmer groups

Given a lattice T in a nice $\mathbb{Q}_p$ Galois representation V, one might try to bound the rank of $H^1_f(G_\mathbb{Q}, V)$ by defining a $\mathbb{Z}_p$-module

$$H^1_f(G_\mathbb{Q}, T) \subset H^1(G_{\mathbb{Q},S}, T)$$

such that $H^1_f(G_\mathbb{Q}, T) \otimes \mathbb{Q}_p \simeq H^1_f(G_\mathbb{Q}, V)$, and an $\mathbb{F}_p$ subspace $H^1_f(G_\mathbb{Q}, T \otimes \mathbb{F}_p) \subset H^1_f(G_{\mathbb{Q},S}, T \otimes \mathbb{F}_p)$ giving a commutative diagram

$$\begin{array}{ccc} H^1_f(G_\mathbb{Q}, T) \otimes \mathbb{F}_p & \hookrightarrow & H^1_f(G_\mathbb{Q}, T \otimes \mathbb{F}_p) \\ \downarrow & & \downarrow \\ H^1(G_{\mathbb{Q},S}, T) \otimes \mathbb{F}_p & \hookrightarrow & H^1(G_{\mathbb{Q},S}, T \otimes \mathbb{F}_p) \end{array}$$

such that the top horizontal map is injective.

Two-descent for BK Selmer groups

In our case of interest, we give an upper bound on the dimension of $H^1_f(G_{\mathbb{Q}}, \wedge^2 V_2(J))$ by finding a subspace $H^1_f(G_{\mathbb{Q}}, \wedge^2 J[2]) \subset H^1(G_{\mathbb{Q}}, \wedge^2 J[2])$, such that

$$\dim_{\mathbb{F}_2} H^1_f(G_{\mathbb{Q}}, \wedge^2 J[2]) \geq \dim H^1_f(G_{\mathbb{Q}}, \wedge^2 V_2(J)).$$

A natural choice of lattice in $\wedge^2 V_2(J)$ is $\wedge^2 T_2(J)$. Its mod 2 quotient is isomorphic to $\wedge^2 J[2]$. Local conditions at primes of bad reduction are easy to understand if the reduction is stable. Understanding 'crystalline' conditions at 2 is not.

The field theoretic description of $H^1(K, \wedge^2 J[2])$

To ease notation, suppose $\mathrm{Gal}(K)$ acts 2-transitively on the roots of f. Let $\alpha, \beta \in K^{\mathrm{sep}}$ be distinct roots. Assume for simplicity that $[K(\alpha,\beta) : K(\alpha+\beta)] = 2$.

Lemma

Let J be the Jacobian of a hyperelliptic curve defined by an odd degree polynomial f. We have an isomorphism

$$H^1(K, \wedge^2 J[2]) \simeq \mathrm{Ker}(K(\alpha+\beta)^\times \otimes \mathbb{F}_2 \xrightarrow{\mathrm{Nm}} K(\alpha)^\times \otimes \mathbb{F}_2)$$

here Nm is the composite of the map $K(\alpha+\beta)^\times \otimes \mathbb{F}_2 \to K(\alpha,\beta)^\times \otimes \mathbb{F}_2$ and the norm map from $K(\alpha,\beta)^\times \otimes \mathbb{F}_2$ to $K(\alpha)^\times \otimes \mathbb{F}_2$.

There is also a 'nonabelian $(x - T)$ map' describing the elements of $K(\alpha+\beta)^\times \otimes \mathbb{F}_2$ you get from rational points.

Berry's work: even degree

- If X does not have a rational Weierstrass point, the description of $H^1(K, J[2])$ in terms of f is much more complicated (see Poonen–Schaefer).
- $\mathrm{Ker}(K(\alpha)^\times \otimes \mathbb{F}_2 \xrightarrow{\mathrm{Nm}} K^\times \otimes \mathbb{F}_2)$ is closely related to $\widetilde{J}[2]$, where $\widetilde{J}$ is an extension of J by a torus (which is split by the field of definition of the points at infinity).
- Recently, Lee Berry showed that one can get useful bounds on the dimension of $H^1_f(\mathbb{Q}, \wedge^2 V_2 J)$ by trying to working with $H^1(K, \wedge^2 \widetilde{J}[2])$.
- $\rightsquigarrow$ proofs of finiteness of $X(\mathbb{Q}_2)_2$ for hyperelliptic curves of genus 2 and 3 without a rational Weierstrass points when $r \geq g$.

Berry's work: ordinary curves are nice

If X has ordinary reduction at p, then

$$H^1_g(\mathbb{Q}_p, \wedge^2 V_p J) = \mathrm{Ker}(H^1(\mathbb{Q}_p, \wedge^2 V_p J) \xrightarrow{\pi_*} H^1(\mathbb{Q}_p, \wedge^2 V_p J_{\mathbb{F}_p})).$$

If X is a hyperelliptic curve with good ordinary reduction at 2, then it has a smooth model

$$y^2 + h_1(x)y = h_2(x)$$

where $h_1 \in \mathbb{Z}_2[x]$ is of degree $g+1$, with separable reduction mod 2. Berry shows that the map π_* can be described in terms of fields defined in terms of roots of h_1.

Theorem (Berry, 2025)

Of the 1,138 genus 2 curves with Mordell-Weil rank 2, good ordinary reduction at 2 and exactly one rational Weierstrass point on the LMFDB, at least 574 satisfy $\#X(\mathbb{Q}_2)_2 < \infty$.

Examples (Berry)

Theorem (Berry)

The genus 2, rank 3 curve
$X : y^2 + (x^2 + x + 1)y = x^5 - x^4 + 2x^3 + 6x^2 + 2x$ *satisfies* $\#X(\mathbb{Q}_2)_2$ *is finite.*

Theorem (Berry, 2025)

The genus 3 curve

$$X : y^2 + (x^4 + x + 1)y = -4x^6 - 7x^5 + 4x^4 + 14x^3 + 5x^2 - 2x$$

satisfies $\#X(\mathbb{Q}_2)_2 < \infty$.

In the last example, the Mordell–Weil group of the Jacobian has rank 3 or 4, and the curve does not have a rational Weierstrass point.

Part 2: How do we compute $X(\mathbb{Q}_p)_2$?

- Now suppose $\#X(\mathbb{Q}_2)_2 < \infty$. How do we find it?
- Recall what happens in 'diet' quadratic Chabauty, for integral points on a hyperelliptic curve (Balakrishnan–Besser–Müller):

$$X(\mathbb{Z}_p) \subset \{h_p(z) = \sum a_{ij}(\int_\infty^z \omega_i)(\int^z \omega_j) + c\}$$

  where the a_{ij} are essentially detemined by the p-adic height pairing.
- In full-fat quadratic Chabauty, the story is essentially the same, but the p-adic height pairing is replaced by a *generalised height* pairing.
- In the case of $y^2 - y = x^5 - x$, we can determine this pairing (and hence $X(\mathbb{Q})$) by evaluating on rational points.
- Is this enough in general?

Why are proofs of the Mordell conjecture ineffective?

- Given a curve X, suppose X has *tons* of rational points.
- If you have a ridiculously large number, they have to have all kinds of relations between one another, which eventually leads to a contradiction (e.g. violating Vojta's inequality).
- This means that if, after searching, you find that you have the largest possible 'legal' number of rational points, you've effectively computed all of them!
- But usually you won't find that many, so you have no way of verifying that you've found them all.
- Example: Chabauty–Coleman. If $\mathrm{rk} J(\mathbb{Q}) = r$, and you have $r+1$ points in $X(\mathbb{Q})$ 'in general position', you get an equation for $X(\mathbb{Q}_p)_1$.

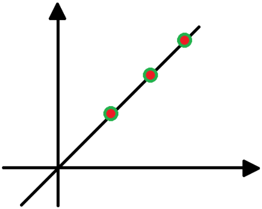
Why ((diet) quadratic) Chabauty is (typically) effective

- Chabauty–Coleman, when it applies, 'usually' does successfully determine the rational points.
- The reason is that, crucially, you don't need to find points in $X(\mathbb{Q})$ which generate (a finite index subgroup of) $J(\mathbb{Q})$. You just need to find them in $J(\mathbb{Q})$ (i.e. in $(\mathrm{Div}^0(X))(\mathbb{Q})$).
- To determine $X(\mathbb{Q}_p)_U$ in the context of usual diet quadratic Chabauty, this largely amounts to computing the p-adic height pairing, i.e. computing the $\mathbb{Q}_p$-valued matrix $h_p(P_i, P_j)$ for (P_i) a basis for a finite index subgroup of $J(\mathbb{Q})$.
- Example: $y^2 = -35x^6 + 310x^5 - 675x^4 + 750x^3 - 450x^2 + 140x - 15$ (Balakrishnan-D.-Müller-Tuitman-Vonk).

What about full fat quadratic Chabauty, or more general nonabelian Chabauty?

- Conjectures imply that when $\mathrm{rk} J(\mathbb{Q}) = r$, if you have about $r^{\log(r)/\log(g)}$ points 'in general position' you get some kind of equation for $X(\mathbb{Q}_p)_n$.
- Remark: This is quite a lot!
- What if we work over number fields (i.e. evalute on $\mathrm{Div}(X)(\mathbb{Q})$)?
- Unclear, e.g. if you do this for the p-adic height on a hyperelliptic curve, this factors through

$$\mathrm{Div}(X)(\mathbb{Q}) \to \mathrm{Sym}^2 J(\overline{\mathbb{Q}})^{G_{\mathbb{Q}}}$$
$$\sum n_i P_i \mapsto \sum n_i (P_i - \infty)^2$$

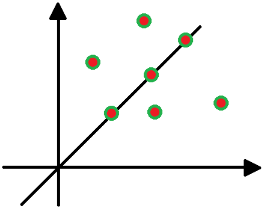


which has a target of infinite rank (I think?).

What about full fat quadratic Chabauty, or more general nonabelian Chabauty?

- Conjectures imply that when $\mathrm{rk} J(\mathbb{Q}) = r$, if you have about $r^{\log(r)/\log(g)}$ points 'in general position' you get some kind of equation for $X(\mathbb{Q}_p)_n$.
- Remark: This is quite a lot!
- What if we work over number fields (i.e. evalute on $\mathrm{Div}(X)(\mathbb{Q})$)?
- Unclear, e.g. if you do this for the p-adic height on a hyperelliptic curve, this factors through

$$\mathrm{Div}(X)(\mathbb{Q}) \to \mathrm{Sym}^2 J(\overline{\mathbb{Q}})^{G_{\mathbb{Q}}}$$
$$\sum n_i P_i \mapsto \sum n_i (P_i - \infty)^2$$



which has a target of infinite rank (I think?).

What is a nonabelian cohomology variety?

Here is a nice way to think about nonabelian cohomology varieties. Consider a collection $V_0, \ldots, V_n$ of representations of a group G. Define:

- $M(G; V_0, \ldots, V_n)$ to be the set of isomorphism classes of representations W, with a descending G-stable filtration W_i
- $U(V_0, \ldots, V_n)$ to be the group of block lower triangular matrices in $\mathrm{GL}(V_0 \oplus \ldots \oplus V_n)$.

Lemma

$$M(G; V_0, \ldots, V_n) \simeq H^1(G, U(V_0, \ldots, V_n)).$$

Any unipotent group maps into a group of the form $U(V_0, \ldots, V_n)$, so you can always map a nonabelian cohomology variety into something like this (analogy: mapping a reductive group G into GL_n to think of G-bundles on a variety as vector bundles).

Example: $n = 1$ and 2

$$U(V_0, V_1) = \mathrm{Hom}(V_0, V_1) = V_0^* \otimes V_1$$

$$M(G; V_0, V_1) \simeq H^1(G, V_0^* \otimes V_1) \simeq \mathrm{Ext}^1(G, V_0, V_1).$$

The case $n = 2$ is more interesting. What do representations with graded pieces V_0, V_1, V_2 look like? Write such a representation as

$$\rho = \begin{pmatrix} \rho_{V_0} & 0 & 0 \\ c_1 & \rho_{V_1} & 0 \\ c_3 & c_2 & \rho_{V_2} \end{pmatrix}.$$

Then c_1 and c_2 define elements of $H^1(G, V_0^* \otimes V_1)$ and $H^1(G, V_1^* \otimes V_2)$. The obstruction to lifting (c_1, c_2) to such a mixed extension is $c_1 \cup c_2 \in H^2(G, V_0^* \otimes V_2)$. Given any two such lifts, $c_3 - c_3'$ gives an element of $H^1(G, V_0^* \otimes V_2)$.

Example: $n = 2$

- In summary: we have an exact sequence of pointed sets

$$H^1(G, V_0^* \otimes V_2) \to M(G; V_0, V_1, V_2)(= H^1(G, U(V_0, V_1, V_2)))$$
$$\to H^1(G, V_0^* \otimes V_1) \times H^1(G, V_1^* \otimes V_2) \xrightarrow{\cup} H^2(G, V_0^* \otimes V_2).$$

- Our case of interest is $V_0 = \mathbb{Q}_p$, $V_1 = V := V_pJ$ and $V_2 = V_pJ^{\otimes 2}$.
- At all primes (away from p) we have $M(G_{\mathbb{Q}_\ell}; \mathbb{Q}_p, V, V^{\otimes 2}) \simeq H^1(G_{\mathbb{Q}_\ell}, V^{\otimes 2})$, so given a global mixed extension, we get an element of $\oplus_{\ell \in S} H^1(\mathbb{Q}_\ell, V^{\otimes 2})$.
- Its image in $\oplus_{\ell \in S} H^1(\mathbb{Q}_\ell, V^{\otimes 2})/H^1(G_{\mathbb{Q},S}, V^{\otimes 2})$ only depends on its image (c_1, c_2) in $H^1(\mathbb{Q}, V) \times \mathrm{Ext}^1_{\mathbb{Q}}(V, V^{\otimes 2})$ is bilinear and is denoted $h(c_1, c_2)$.

Does this define a pairing? How do we compute it?

An equivalent formulation: where are all the mixed motives?

- Where do the mixed representations we seek come from? Geometrically, Galois representations with different weights arise from the étale cohomology of *open* (non-proper) varieties.
- In fact, there's a beautiful formula due to Beilinson that explains how to construct the open varieties whose étale cohomology gives the Galois representations coming from fundamental groups.

To implement full-fat QC, we need to *find* the algebraic cycles whose existence is predicted by hard 'motivic' conjectures.

Theorem (D.)

The Beilinson–Bloch conjectures imply that the generalised height defines a pairing

$$\mathrm{CH}^2(X^3)_0 \times \mathrm{CH}^2(X)_0 \to \mathrm{colim}_S \oplus_{\ell \in S} H^1_g(\mathbb{Q}_\ell, V^{\otimes 2})/H^1(\mathrm{Gal}(\mathbb{Q}_S|\mathbb{Q}), V^{\otimes 2}).$$

The motivic version of diet quadratic Chabauty

- Edixhoven and Lido observed that there is a motivic avatar of $H^1(G, U(V_0, V_1, V_2))$ when $(V_0, V_1, V_2) = (\mathbb{Q}_p, V_pJ, \mathbb{Q}_p(1))$.
- Namely, the Poincare torsor P is a $\mathbb{G}_m$-torsor over $J^\vee \times J$ obtained. Indeed $U(V_0, V_1, V_2)$ is the unipotent fundamental group of P.

- A more naive version of this is used in existing practical implementations: we compute the p-adic height pairing by finding pairs of divisors with disjoint support.
- Remark: the fact that the motivic avatar is a *scheme* is very special (Deligne–Griffiths–Morgan–Sullivan).

'Motivating' case: the unit equation

If $(V_0, V_1, V_2) = (\mathbb{Q}_p, \mathbb{Q}_p(1), \mathbb{Q}_p(2))$. The motivic analogue of the right-hand side of the diagram is the map

$$K^\times \times K^\times \to K_2^M(K) := (K^{\times \otimes 2})/\langle x \otimes (1-x) : x \in K^\times - \{1\}\rangle.$$

Define $\widetilde{B}$ to be the set of triples $(x, y, \sum n_i[z_i])$ in $K^\times \times K^\times \times \mathbb{Z}[K^\times - 1]$ such that

$$x \otimes y = \sum n_i z_i \otimes (1 - z_i)$$

modulo the equivalence relation

$$(x, y, \sum n_i[z_i]) \sim (x', y', \sum n_i'[z_i'])$$

if $\sum n_i[z_i] - \sum n_i' z_i'$ lies in the subspace of $\mathbb{Z}[K]$ generated by

$$[a] + [b] + [\frac{1-a}{1-ab}] + [1-ab] + [\frac{1-b}{1-ab}].$$

‘Motivating’ case: the unit equation

We get a short exact sequence of pointed sets

$$1 \to B_2(K) \to \widetilde{B} \to K^\times \times K^\times \to 1,$$

where $B_2(K)$ is the Bloch group of K, which maps to the short exact sequence for $H^1(G, U_2)$. This can be thought of as an archetypal example of generalising the Poincaré torsor to something non-representable.
This tells use we can compute the equations for $X(\mathbb{Z}_p)_2$ ($X = \mathbb{P}^1 - \{0, 1, \infty\}$) by evaluating dilogarithms of rational points.

Motivic analogue of $H^2(G; V \otimes V)$: the Albanese kernel

This exists in a very general context but we restrict to the case of a self-product of curves $X \times X$.
The Chow group $\mathrm{CH}^2(X^2) := Z^2(X^2)/\sim$ is the group of zero-cycles modulo rational equivalence. We have a homomorphism $Z^2(X \times X) \to Z^1(X) \times Z^1(X)$ given by

$$\sum n_i(P_i, Q_i) \mapsto (\sum n_i P_i, \sum n_i Q_i).$$

This induces homomorphisms

$$\mathrm{CH}^2(X \times X) \to \mathrm{CH}^1(X) \times \mathrm{CH}^1(X)$$
$$\mathrm{CH}^2(X \times X)_0 \to \mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X).$$

The kernel of this homomorphism is called the Albanese kernel $F^2(X^2)$.

Conjecture (Beilinson–Bloch)

If K is a number field, then $F^2(X^2)$ is finite.

Motivic avatar of the cup product: Somekawa K-group product

We have a homomorphism $F^2(X^2) \to H^2(K, H^2_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p(2)))$, and a homomorphism

$$\cup : \mathrm{Jac}(X) \times \mathrm{Jac}(X) \to F^2(X^2)$$

given by $(\sum n_i P_i, \sum m_j Q_j) \mapsto \sum n_i m_j (P_i, Q_j)$.
We have a commutative diagram

$$\begin{array}{ccc} \mathrm{Jac}(X)^2 & \to & F^2(X^2) \\ \downarrow & & \downarrow \\ H^1(K, H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p(1)))^2 & \xrightarrow{\cup} & H^2(K, H^2_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p(2))) \end{array}$$

Motivic avatar of $H^1(K, T_pJ^{\otimes 2})$: $\mathrm{CH}^2(X^2, 1)$

Recall that for a surface S, we may define $\mathrm{CH}^2(S, 1)$ to be the cohomology of the complex

$$K_M^2(K(S)) \to \oplus_{C \in X^{(1)}} K(C)^\times \to Z^2(S)$$

where the maps are the tame symbols

$$\langle f_1, f_2 \rangle \mapsto (\mathrm{div}(f_1), f_2|_{\mathrm{div}(f_1)}) - (\mathrm{div}(f_2), f_1|_{\mathrm{div}(f_2)})$$

and

$$\sum n_i(C_i, f_i) \mapsto \sum n_i \mathrm{div}(f_i) \in Z^2(S).$$

We have an etale regulator map

$$\mathrm{CH}^2(S, 1) \to H^1(K, H^2_{\text{ét}}(S_{\overline{K}}, \mathbb{Z}_p(2)))$$

given by sending $\sum n_i(C_i, f_i)$ to an appropriate subquotient of $H^2_{\text{ét}}(S_{\overline{K}} - \cup C_i, \mathbb{Z}_p(2))$.

Lifting the kernel

If (c_1, c_2) are in the kernel of

$$H^1(K, T_pJ)^2 \to H^2(K, T_pJ^{\otimes 2}),$$

then there is a mixed extension with graded pieces $\mathbb{Z}_p$, T_pJ and $T_pJ^{\otimes 2}$ lifting the extensions c_1 and c_2. What is the motivic analogue? Define $\widetilde{S}$ to be the set of triples $(D_1, D_2, \sum n_i(C_i, f_i))$ up to equivalence, where

- $D_1, D_2 \in \mathrm{Div}^0(X)$ cup to zero in $F^2(X^2)$.
- $\sum \mathrm{div}(f_i) = D_1 \boxtimes D_2$ in $Z^2(X^2)$.
- two triples $(D_1, D_2, \sum n_i(C_i, f_i))$ and $(D_1', D_2', \sum n_i'(C_i', f_i'))$ are equivalent if they have the same image in $\mathrm{CH}^1(X)_0^2$, and $\sum n_i(C_i, f_i) - \sum n_i'(C_i', f_i')$ lies in the image of $K_2^M(K(X^2))$.

Lifting the kernel

Lemma

We have a commutative diagram of pointed sets with exact rows

$$\begin{array}{ccccccc} \mathrm{CH}^2(X^2,1) & \to & \widetilde{S} & \to & \mathrm{Jac}(X)^2 & \to & F^2(X^2) \\ \downarrow & & \downarrow & & & & \\ H^1(K, T_pJ^{\otimes 2}) & \to & H^1(K,U) & \to & H^1(K,T_pJ)^2 & \xrightarrow{\cup} & H^2(K, T_pJ^{\otimes 2}) \end{array}$$

where $U = U(\mathbb{Z}_p, T_pJ, T_pJ^{\otimes 2})$, *the map* $\widetilde{S} \to H^1(K,U)$ *is given by sending* $(D_1, D_2, \sum(C_i, f_i))$ *to an appropriate subquotient of* $H^2_{\text{ét}}(X_{\overline{K}} - \cup C_i \cup D_1 \times X, \mathbb{Z}_p(2))$.

Remark: the idea of combining $F^2(X^2)$, unipotent fundamental groups and rational points is not new! (Esnault–Wittenberg).

Not quite it

Is this a motivic analogue of our Selmer scheme? In general, not quite. The issue is that the extensions of T_pJ by $T_pJ^{\otimes 2}$ coming from rational points on curves are typically *not* in the image of the map

$$\text{“} \otimes T_pJ\text{''} : \mathrm{Ext}^1(\mathbb{Z}_p, T_pJ) \to \mathrm{Ext}^1(T_pJ, T_pJ^{\otimes 2}).$$

The obstruction is old friend of the seminar series the Ceresa cycle! So in general the correct definition is more elaborate, and gives a short exact sequence

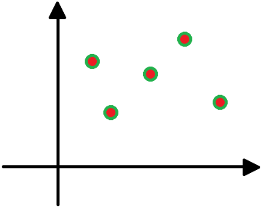
$$\mathrm{CH}^2(X^2, 1) \to \widetilde{S} \to \mathrm{CH}^1(X)_0 \times \mathrm{CH}^2(X^3)_0 \xrightarrow{\cup} F^2(X^2).$$

Here $\widetilde{S}$ consists of triples $(D, Z, \sum(C_i, f_i))$ in $\mathrm{Div}^0(X) \times Z^2(X^3)$ $\times \oplus_{C \in X^{(1)}} K(C)^\times$ satisfying some properties, up to some equivalence relation.

The punchline

In down to earth terms, for a hyperelliptic curve X with a rational Weierstrass point ∞, this means that given $\sum n_i(P_i, Q_i)$ in $Z^2(X^2)$, if we can find curves C_j on X^2 and divisors D_j on C_j such that

- D_j lies in the image of $Z^1(X) \times Z^1(X)$ under the projection maps $\pi_i : C \to X$,
- $\sum n_i(P_i, Q_i) = \sum_j D_j$ in $Z^2(X^2)$,



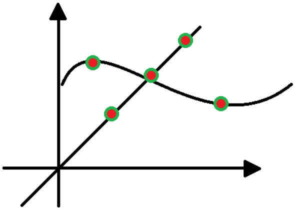
then we can compute $\sum n_i h(P_i - \infty, Q_i - \infty)$.

In particular, Beilinson–Bloch implies the existence of an algorithm, but not the existence of a good one, to compute the generalised height! How do we computationally verify torsion-ness of zero-cycles in X^2 (Murre–Ramakrishnan, Gazaki, Love)

The punchline

In down to earth terms, for a hyperelliptic curve X with a rational Weierstrass point ∞, this means that given $\sum n_i(P_i, Q_i)$ in $Z^2(X^2)$, if we can find curves C_j on X^2 and divisors D_j on C_j such that

- D_j lies in the image of $Z^1(X) \times Z^1(X)$ under the projection maps $\pi_i : C \to X$,
- $\sum n_i(P_i, Q_i) = \sum_j D_j$ in $Z^2(X^2)$,



then we can compute $\sum n_i h(P_i - \infty, Q_i - \infty)$.

In particular, Beilinson–Bloch implies the existence of an algorithm, but not the existence of a good one, to compute the generalised height! How do we computationally verify torsion-ness of zero-cycles in X^2 (Murre–Ramakrishnan, Gazaki, Love)

An example

For hyperelliptic curves, the following trick often seems to work: look for *bihyperelliptic curves* with extra symmetries. For example, consider the curve

$$X : y^2 = f(x) := 4x^5 + 8x^4 + 16x^3 + 12x^2 + 8x + 1.$$

(or 21653.a.21653.1 to its friends). This has Mordell–Weil rank 2, and 5 rational points

$$\{\infty, (0, \pm 1), (1, \pm 7)\}$$

Hence rational points allow us to compute $h((0,1) - \infty, (0,1) - \infty)$ and $h((1,7) - \infty, (1,7) - \infty)$. How can we compute the generalised height

$$h((0,1) - \infty, (1,7) - \infty)?$$

An example

Consider the (normalisation of) the curve

$$C : y^2 = f(x - 1/2), z^2 = f(-1/2 - x)$$

inside $X \times X$. On C we have the principal divisor

$$\begin{aligned}
&5(\frac{\sqrt{-3}}{2}, 1, 1) + 5(\frac{\sqrt{-3}}{2}, -1, -1) + 5(-\frac{\sqrt{-3}}{2}, 1, 1) + 5(-\frac{\sqrt{-3}}{2}, -1, -1) \\
&+ (\frac{\sqrt{-7}}{2}, 1, 1) + (\frac{\sqrt{-7}}{2}, -1, -1) + (-\frac{\sqrt{-7}}{2}, 1, 1) + (-\frac{\sqrt{-3}}{2}, -1, -1) \\
&- (\frac{\sqrt{-31}}{2}, -14 - 3\sqrt{-31}, -14 + 3\sqrt{-31}) \\
&- (\frac{\sqrt{-31}}{2}, -14 - 3\sqrt{-31}, -14 + 3\sqrt{-31}) \\
&- (\frac{\sqrt{-31}}{2}, 14 + 3\sqrt{-31}, 14 - 3\sqrt{-31}) - (\frac{\sqrt{-31}}{2}, 14 + 3\sqrt{-31}, 14 - 3\sqrt{-31}) \\
&- 4\infty^+ - 4\infty^-.
\end{aligned}$$

An example

We have

$$\mathrm{Tr}((\zeta_3, 1) - \infty) \sim -\frac{1}{4}((1,7) - \infty) - \frac{1}{2}((0,1) - \infty)$$

$$\mathrm{Tr}((\frac{-1+\sqrt{-7}}{2}, 1) - \infty) \sim -\frac{1}{4}((1,7) - \infty) + \frac{1}{2}((0,1) - \infty)$$

$$\mathrm{Tr}((\frac{-1+\sqrt{-31}}{2}, 14 + 3\sqrt{-31}) - \infty) \sim 3((0,1) - \infty)$$

Hence using algebraic cycles we have successfully determined the pairing!

Questions

- How to implement this? Should we be using the Jacobian instead of $X \times X$? Or the Kummer variety?
- The 'Tate–Shafarevich' obstruction to computing the dimension of $H^1_f(\mathbb{Q}, \wedge^2 V_p J)$ should come from p-torsion in $F^2(J)$. How can we compute this?
- Beilinson's conjecture implies that we could define a 'circle-valued' generalised height in the style of Mazur–Tate:

$$\mathrm{CH}^1(X)_0 \times \mathrm{CH}^2(X^3)_0 \to \mathrm{Ext}^1_{\mathbb{R}-\mathrm{MHS}}(\mathbb{R}, \wedge^2 H_1(X, \mathbb{R}))/\mathrm{CH}^2(J, 1) \sim (\mathbb{R}/\mathbb{Z})^{\frac{g(g+1)}{2} - \rho(J)}.$$

What is the significance of the numbers you get from this??

Thanks!