Explicit Coleman integration for curves

Jennifer Balakrishnan

Boston University

Arithmetic of Hyperelliptic Curves
ICTP
September 4, 2017

Motivation

Question

How do we compute rational points on (hyperelliptic) curves?

Motivation

Question

How do we compute rational points on (hyperelliptic) curves?

That is, given a (hyperelliptic) curve X defined over $\mathbf{Q}$, how do we compute $X(\mathbf{Q})$?

Motivation

Question

How do we compute rational points on (hyperelliptic) curves?

That is, given a (hyperelliptic) curve X defined over $\mathbf{Q}$, how do we compute $X(\mathbf{Q})$?

Can we make this algorithmic?

Example 1: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600.$$

Example 1: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600.$$

It has at least **642** rational points*, with x-coordinates:

0, -1, 1/3, 4, -4, -3/5, -5/3, 5, 6, 2/7, 7/4, 1/8, -9/5, 7/10, 5/11, 11/5, -5/12, 11/12, 5/12, 13/10, 14/9, -15/2, -3/16, 16/15, 11/18, -19/12, 19/5, -19/11, -18/19, 20/3, -20/21, 24/7, -7/24, -17/28, 15/32, 5/32, 33/8, -23/33, -35/12, -35/18, 12/35, -37/14, 38/11, 40/17, -17/40, 34/41, 5/41, 41/16, 43/9, -47/4, -47/54, -9/55, -55/4, 21/55, -11/57, -59/15, 59/9, 61/27, -61/37, 62/21, 63/2, 65/18, -1/67, -60/67, 71/44, 71/3, -73/41, 3/74, -58/81, -41/81, 29/83, 19/83, 36/83, 11/84, 65/84, -86/45, -84/89, 5/89, -91/27, 92/21, 99/37, 100/19, -40/101, -32/101, -104/45, -13/105, 50/111, -113/57, 115/98, -115/44, 116/15, 123/34, 124/63, 125/36, 131/5, -64/133, 135/133, 35/136, -139/88, -145/7, 101/147, 149/12, -149/80, 75/157, -161/102, 97/171, 173/132, -65/173, -189/83, 190/63, 196/103, -195/196, -193/198, 201/28, 210/101, 227/81, 131/240, -259/3, 265/24, 193/267, 19/270, -279/281, 283/33, -229/298, -310/309, 174/335, 31/337, 400/129, -198/401, 384/401, 409/20, -422/199, -424/33, 434/43, -415/446, 106/453, 465/316, -25/489, 490/157, 500/317, -501/317, -404/513, -491/516, 137/581, 597/139, -612/359, 617/335, -620/383, -232/623, 653/129, 663/4, 583/695, 707/353, -772/447, 835/597, -680/843, 853/48, 860/697, 515/869, -733/921, -1049/33, -263/1059, -1060/439, 1075/21, -1111/30, 329/1123, -193/1231, 1336/1033, 321/1340, 1077/1348, -1355/389, 1400/11, -1432/359, -1505/909, 1541/180, -1340/1639, -1651/731, -1705/1761, -1757/1788, -1456/1893, -235/1983, -1990/2103, -2125/84, -2343/635, -2355/779, 2631/1393, -2639/2631, 396/2657, 2691/1301, 2707/948, -164/2777, -2831/508, 2988/43, 3124/395, -3137/3145, -3374/303, 3505/1148, 3589/907, 3131/3655, 3679/384, 535/3698, 3725/1583, 3940/939, 1442/3981, 865/4023, 2601/4124, -2778/4135, 1096/4153, 4365/557, -4552/2061, -197/4620, 4857/1871, 1337/5116, 5245/2133, 1007/5534, 1616/5553, 5965/2646, 6085/1563, 6101/1858, -5266/6303, -4565/6429, 6535/1377, -6613/6636, 6354/6697, -6908/2715, -3335/7211, 7363/3644, -4271/7399, -2872/8193, 2483/8301, -8671/3096, -6975/8941, 9107/6924, -9343/1951, -9589/3212, 10400/373, -8829/10420, 10511/2205, 1129/10836, 675/11932, 8045/12057, 12945/4627, -13680/8543, 14336/243, -100/14949, -15175/8919, 1745/15367, 16610/16683, 17287/16983, 2129/18279, -19138/1865, 19710/4649, -18799/20047, -20148/1141, -20873/9580, 21949/6896, 21985/6999, 235/25197, 16070/26739, 22991/28031, -33555/19603, -37091/14317, -2470/39207, 40645/6896, 46055/19518, -46925/11181, -9455/47584, 55904/8007, 39946/56827, -44323/57516, 15920/59083, 62569/39635, 73132/13509, 82315/67051, -82975/34943, 95393/22735, 14355/98437, 15121/102391, 130190/93793, -141665/55186, 39628/153245, 30145/169333, -140047/169734, 61203/171017, 148451/182305, 86648/195399, -199301/54169, 11795/225434, -84639/266663, 283567/143436, -291415/171792, -314333/195860, 289902/322289, 405523/327188, -342731/523857, 24960/630287, -665281/83977, -688283/82436, 199504/771597, 233305/795263, -799843/183558, -867313/1008993, 1142044/157607, 1399240/322953, -1418023/463891, 1584712/90191, 726821/2137953, 2224780/807321, -2849969/629081, -3198658/3291555, 675911/3302518, -5666740/2779443, 1526015/5872096, 13402625/4101272, 12027943/13799424, -71658936/86391295, 148596731/35675865, 58018579/158830656, 208346440/37486601, -1455780835/761431834, -3898675687/2462651894

Is this list complete?

*Computed by Michael Stoll in 2008.

Example 2: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

The *Chabauty-Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

Example 2: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

The *Chabauty-Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0),(1,0),(2,0),(5,0),(6,0),\infty$$

Example 2: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

The *Chabauty-Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0), (1,0), (2,0), (5,0), (6,0), \infty$$

and

$$(3, \pm 6), (10, \pm 120)$$

in $X(\mathbf{Q})$.

Example 2: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

The *Chabauty-Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0), (1,0), (2,0), (5,0), (6,0), \infty$$

and

$$(3, \pm 6), (10, \pm 120)$$

in $X(\mathbf{Q})$.

We've found 10 points!

Example 2: Can we compute $X(\mathbf{Q})$?

Consider X with affine equation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

The *Chabauty-Coleman bound* tells us that

$$|X(\mathbf{Q})| \leqslant 10.$$

We find the points

$$(0,0), (1,0), (2,0), (5,0), (6,0), \infty$$

and

$$(3, \pm 6), (10, \pm 120)$$

in $X(\mathbf{Q})$.

We've found 10 points!

Hence we have provably determined

$$X(\mathbf{Q}) = \{(0,0), (1,0), (2,0), (5,0), (6,0), (3, \pm 6), (10, \pm 120), \infty\}.$$

Chabauty-Coleman

What is different in this second example? What allows us to compute $X(\mathbf{Q})$?

Chabauty-Coleman

What is different in this second example? What allows us to compute $X(\mathbf{Q})$?

(A bit of luck +) satisfying an inequality between the **genus** of the curve X and the **rank** of the Mordell-Weil group of its Jacobian $J(\mathbf{Q})$ (+ work of Chabauty and Coleman).

Chabauty's theorem

Theorem (Chabauty, '41)

Let X be a curve of genus $g \geqslant 2$ over $\mathbf{Q}$. Suppose the Mordell-Weil rank r of $J(\mathbf{Q})$ is less than g. Then $X(\mathbf{Q})$ is finite.

To make Chabauty's theorem effective:

- Need to find a way to bound $X(\mathbf{Q}_p) \cap \overline{J(\mathbf{Q})}$
- Do this by constructing functions (p-adic integrals of 1-forms) on $J(\mathbf{Q}_p)$ that vanish on $J(\mathbf{Q})$ and restrict them to $X(\mathbf{Q}_p)$

Chabauty's theorem

Theorem (Chabauty, '41)

Let X be a curve of genus $g \geqslant 2$ over $\mathbf{Q}$. Suppose the Mordell-Weil rank r of $J(\mathbf{Q})$ is less than g. Then $X(\mathbf{Q})$ is finite.

To make Chabauty's theorem effective:

- Need to find a way to bound $X(\mathbf{Q}_p) \cap \overline{J(\mathbf{Q})}$
- Do this by constructing functions (p-adic integrals of 1-forms) on $J(\mathbf{Q}_p)$ that vanish on $J(\mathbf{Q})$ and restrict them to $X(\mathbf{Q}_p)$

This was done by Coleman (1985).

The method of Chabauty-Coleman

Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $b \in X(\mathbf{Q})$.

- $\iota : X \hookrightarrow J$, sending $P \mapsto [(P) - (b)]$
- $p > 2$: prime of good reduction for X

The method of Chabauty-Coleman

Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $b \in X(\mathbf{Q})$.

- $\iota : X \hookrightarrow J$, sending $P \mapsto [(P) - (b)]$
- $p > 2$: prime of good reduction for X

Recall that the map $H^0(J_{\mathbf{Q}_p}, \Omega^1) \longrightarrow H^0(X_{\mathbf{Q}_p}, \Omega^1)$ induced by ι is an isomorphism of $\mathbf{Q}_p$-vector spaces. Suppose ω_J restricts to ω.

The method of Chabauty-Coleman

Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $b \in X(\mathbf{Q})$.

- $\iota : X \hookrightarrow J$, sending $P \mapsto [(P) - (b)]$
- $p > 2$: prime of good reduction for X

Recall that the map $H^0(J_{\mathbf{Q}_p}, \Omega^1) \longrightarrow H^0(X_{\mathbf{Q}_p}, \Omega^1)$ induced by ι is an isomorphism of $\mathbf{Q}_p$-vector spaces. Suppose ω_J restricts to ω. Then for $Q, Q' \in X(\mathbf{Q}_p)$, define

$$\int_Q^{Q'} \omega := \int_0^{[Q'-Q]} \omega_J.$$

The method of Chabauty-Coleman

Assume $X(\mathbf{Q}) \neq \emptyset$ and fix a basepoint $b \in X(\mathbf{Q})$.

- $\iota : X \hookrightarrow J$, sending $P \mapsto [(P) - (b)]$
- $p > 2$: prime of good reduction for X

Recall that the map $H^0(J_{\mathbf{Q}_p}, \Omega^1) \longrightarrow H^0(X_{\mathbf{Q}_p}, \Omega^1)$ induced by ι is an isomorphism of $\mathbf{Q}_p$-vector spaces. Suppose ω_J restricts to ω. Then for $Q, Q' \in X(\mathbf{Q}_p)$, define

$$\int_Q^{Q'} \omega := \int_0^{[Q'-Q]} \omega_J.$$

If $r < g$, there exists $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$ such that

$$\int_b^P \omega = 0$$

for all $P \in X(\mathbf{Q})$. Thus by studying the zeros of $\int \omega$, we can find a finite set of p-adic points containing the rational points of X.

Computing rational points via Chabauty Coleman

We have

$$X(\mathbf{Q}) \subset X(\mathbf{Q}_p)_1 := \left\{ z \in X(\mathbf{Q}_p) : \int_b^z \omega = 0, \right\}$$

for a p-adic line integral $\int_b^* \omega$, with $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

We would like to compute an annihilating differential ω and then calculate the finite set of p-adic points $X(\mathbf{Q}_p)_1$.

Example: Chabauty-Coleman with $g = 2, r = 1$

Suppose we have a genus 2 curve $X/\mathbf{Q}$ with $\operatorname{rk} J(\mathbf{Q}) = 1$ and $X(\mathbf{Q}) \neq \emptyset$. Fix a basepoint $b \in X(\mathbf{Q})$.

- We know $H^0(X_{\mathbf{Q}_p}, \Omega^1) = \langle \omega_0, \omega_1 \rangle$.
- Since $r = 1 < 2 = g$, we can compute $X(\mathbf{Q}_p)_1$ as the zero set of a p-adic integral.
- If we know one more point $P \in X(\mathbf{Q})$, we can compute the constants $A, B \in \mathbf{Q}_p$:

  $$\int_b^P \omega_0 = A, \quad \int_b^P \omega_1 = B,$$

  then solve the equation

  $$f(z) := \int_b^z (B\omega_0 - A\omega_1) = 0$$

  for $z \in X(\mathbf{Q}_p)$.
- The set of such z is finite, and $X(\mathbf{Q})$ is contained in this set.

From zeta functions to Coleman integrals

During the summer school last week, we learned various things about zeta functions and L-functions

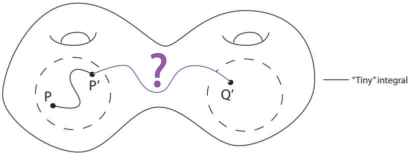
- One fast way of computing zeta functions of hyperelliptic curves over finite fields is Kedlaya's algorithm.
- Kedlaya's algorithm can be recast into an algorithm for computing Coleman integrals.
- Having an algorithm for Coleman integrals can help us compute rational points on hyperelliptic curves.

So I will first discuss how to compute Coleman integrals on hyperelliptic curves* and then discuss how to extend this to general curves.

*For the experts: there are other interesting zeta function algorithms using p-adic techniques. It'd be interesting to turn some of these zeta function algorithms into Coleman integration algorithms!

p-adic line integrals

Coleman integrals are p-adic *line integrals*.



p-adic line integration is difficult – how do we construct the correct path?

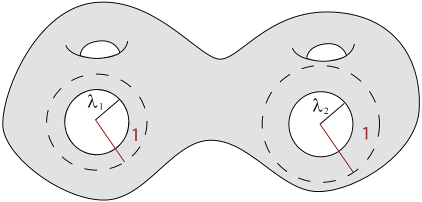
- We can construct local ("tiny") integrals easily, but extending them to the entire space is challenging.
- Coleman's solution: *analytic continuation along Frobenius*, giving rise to a theory of p-adic line integration satisfying the usual nice properties

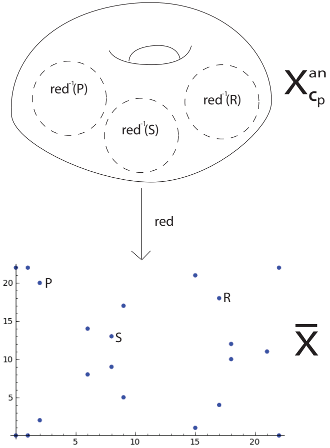
Notation and setup

- X: genus g hyperelliptic curve (of the form $y^2 = f(x)$, f monic of degree $2g+1$) over $K = \mathbf{Q}_p$
- p: prime of good reduction
- $\overline{X}$: special fibre of X
- $X^{\mathrm{an}}_{\mathbf{C}_p}$: generic fibre of X (as a rigid analytic space)

Notation and setup, in pictures

- There is a natural reduction map from $X_{\mathbf{C}_p}^{\mathrm{an}}$ to $\overline{X}$; the inverse image of any point of $\overline{X}$ is a subspace of $X_{\mathbf{C}_p}^{\mathrm{an}}$ isomorphic to an open unit disk. We call such a disk a *residue disk* of X.
- A *wide open subspace* of $X_{\mathbf{C}_p}^{\mathrm{an}}$ is the complement in $X_{\mathbf{C}_p}^{\mathrm{an}}$ of the union of a finite collection of disjoint closed disks of radius $\lambda_i < 1$:





Warm-up: Computing "tiny" integrals

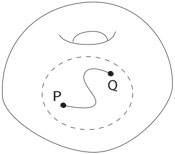
We refer to any Coleman integral of the form $\int_P^Q \omega$ in which P, Q lie in the same residue disk (so $P \equiv Q \pmod{p}$) as a *tiny integral*. To compute such an integral:

- Construct a linear interpolation from P to Q. For instance, in a non-Weierstrass residue disk, we may take

$$x(t) = (1-t)x(P) + tx(Q)$$
$$y(t) = \sqrt{f(x(t))},$$

  where $y(t)$ is expanded as a formal power series in t.
- Formally integrate the power series in t:

$$\int_P^Q \omega = \int_0^1 \omega(x(t), y(t))\, dt.$$



Properties of the Coleman integral

Coleman formulated an integration theory on wide open subspaces of curves over $\mathcal{O}$.

This allows us to define $\int_P^Q \omega$ whenever ω is a meromorphic 1-form on X, and $P, Q \in X(\mathbf{Q}_p)$ are points where ω is holomorphic.

Properties of the Coleman integral include:

Theorem (Coleman)

- *Linearity:* $\int_P^Q (\alpha\omega_1 + \beta\omega_2) = \alpha \int_P^Q \omega_1 + \beta \int_P^Q \omega_2$.

Properties of the Coleman integral

Coleman formulated an integration theory on wide open subspaces of curves over $\mathcal{O}$.

This allows us to define $\int_P^Q \omega$ whenever ω is a meromorphic 1-form on X, and $P, Q \in X(\mathbf{Q}_p)$ are points where ω is holomorphic.

Properties of the Coleman integral include:

Theorem (Coleman)

- *Linearity:* $\int_P^Q (\alpha\omega_1 + \beta\omega_2) = \alpha \int_P^Q \omega_1 + \beta \int_P^Q \omega_2$.
- *Additivity:* $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.

Properties of the Coleman integral

Coleman formulated an integration theory on wide open subspaces of curves over $\mathcal{O}$.

This allows us to define $\int_P^Q \omega$ whenever ω is a meromorphic 1-form on X, and $P, Q \in X(\mathbf{Q}_p)$ are points where ω is holomorphic.

Properties of the Coleman integral include:

Theorem (Coleman)

- *Linearity:* $\int_P^Q (\alpha\omega_1 + \beta\omega_2) = \alpha \int_P^Q \omega_1 + \beta \int_P^Q \omega_2$.
- *Additivity:* $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
- *Change of variables: if X' is another such curve, and $f : U \to U'$ is a rigid analytic map between wide opens, then* $\int_P^Q f^*\omega = \int_{f(P)}^{f(Q)} \omega$.

Properties of the Coleman integral

Coleman formulated an integration theory on wide open subspaces of curves over $\mathcal{O}$.

This allows us to define $\int_P^Q \omega$ whenever ω is a meromorphic 1-form on X, and $P, Q \in X(\mathbf{Q}_p)$ are points where ω is holomorphic.

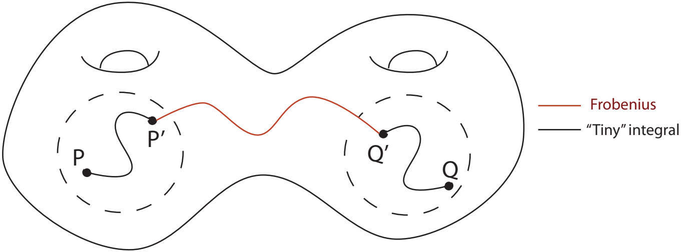
Properties of the Coleman integral include:

Theorem (Coleman)

- *Linearity:* $\int_P^Q (\alpha\omega_1 + \beta\omega_2) = \alpha \int_P^Q \omega_1 + \beta \int_P^Q \omega_2$.
- *Additivity:* $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
- *Change of variables: if X' is another such curve, and $f : U \to U'$ is a rigid analytic map between wide opens, then* $\int_P^Q f^*\omega = \int_{f(P)}^{f(Q)} \omega$.
- *Fundamental theorem of calculus:* $\int_P^Q df = f(Q) - f(P)$.

Coleman's construction

How do we integrate if P, Q aren't in the same residue disk? Coleman's key idea: use Frobenius to move between different residue disks (Dwork's "analytic continuation along Frobenius")



So we need to calculate the action of Frobenius on differentials.

Frobenius, MW-cohomology

- X': affine curve ($X - \{$Weierstrass points of $X\}$)
- A: coordinate ring of X'

Frobenius, MW-cohomology

- X': affine curve ($X - \{$Weierstrass points of $X\}$)
- A: coordinate ring of X'

To discuss the differentials we will be integrating, we recall:
The *Monsky-Washnitzer (MW) weak completion of* A is the ring $A^\dagger$ consisting of infinite sums of the form

$$\left\{ \sum_{i=-\infty}^{\infty} \frac{B_i(x)}{y^i},\ B_i(x) \in K[x], \deg B_i \leqslant 2g \right\},$$

further subject to the condition that $v_p(B_i(x))$ grows faster than a linear function of i as $i \to \pm\infty$. We make a ring out of these using the relation $y^2 = f(x)$.
These functions are holomorphic on wide opens, so we will integrate 1-forms

$$\omega = g(x,y)\frac{dx}{2y}, \quad g(x,y) \in A^\dagger.$$

Using the basis differentials

Any odd differential $\omega = h(x,y)\frac{dx}{2y}, h(x,y) \in A^\dagger$ can be written as

$$\omega = df_\omega + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1},$$

where $f_\omega \in A^\dagger$, $c_i \in \mathbf{Q}_p$ and

$$\omega_i = \frac{x^i\,dx}{2y} \qquad (i = 0, \ldots, 2g-1).$$

The set $\{\omega_i\}_{i=0}^{2g-1}$ forms a basis of the odd part of the de Rham cohomology of $A^\dagger$.

By linearity and the fundamental theorem of calculus, we reduce the integration of ω to the integration of the ω_i.

Some notation and setup

Let ϕ denote a lift of p-power Frobenius:

- On a hyperelliptic curve $y^2 = f(x)$,

$$\phi : (x, y) \mapsto (x^p, \sqrt{f(x^p)}).$$

- A *Teichmüller point* of X is a point P fixed by Frobenius: $\phi(P) = P$.

Integrals between points in different residue disks

One way to compute Coleman integrals $\int_P^Q \omega_i$:

- Find the Teichmüller points P', Q' in the residue disks of P, Q.

Integrals between points in different residue disks

One way to compute Coleman integrals $\int_P^Q \omega_i$:

- Find the Teichmüller points P', Q' in the residue disks of P, Q.
- Use Frobenius to compute $\int_{P'}^{Q'} \omega_i$.

Integrals between points in different residue disks

One way to compute Coleman integrals $\int_P^Q \omega_i$:

- Find the Teichmüller points P', Q' in the residue disks of P, Q.
- Use Frobenius to compute $\int_{P'}^{Q'} \omega_i$.
- Use additivity in endpoints to recover the integral: $\int_P^Q \omega_i = \int_P^{P'} \omega_i + \int_{P'}^{Q'} \omega_i + \int_{Q'}^{Q} \omega_i$.

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\begin{aligned}\phi(x) &= x^p,\\ \phi(y) = \sqrt{f(x^p)} &= y^p\left(1+\frac{f(x^p)-f(x)^p}{f(x)^p}\right)^{1/2}\\ &= y^p\sum_{i=0}^{\infty}\binom{1/2}{i}\frac{(f(x^p)-f(x)^p)^i}{y^{2pi}}.\end{aligned}$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

$$\phi^*(\omega_i) = \frac{x^{pi} d(x^p)}{2\phi(y)}$$

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

$$\phi^*(\omega_i) = \frac{x^{pi} p x^{p-1} dx}{2\phi(y)}$$

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

$$\phi^*(\omega_i) = px^{pi+p-1} \frac{y}{\phi(y)} \frac{dx}{2y}$$

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

$$\phi^*(\omega_i) = px^{pi+p-1}y\left(y^{-p}\sum_{i=0}^{\infty}\binom{-1/2}{i}\frac{(f(x^p)-f(x)^p)^i}{y^{2pi}}\right)\frac{dx}{2y}$$

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

$$\phi^*(\omega_i) = px^{pi+p-1}y^{1-p}\left(\sum_{i=0}^{\infty} \binom{-1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}\right)\frac{dx}{2y}$$

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

$$\phi^*(\omega_i) = [\text{....some } p\text{-adic magic...!}]$$

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.

$$\phi^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j$$

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.
Then

$$\phi^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j$$

for some $f_i \in A^\dagger$ and some $2g \times 2g$ matrix M.

The Frobenius step (Kedlaya's algorithm)

We have a p-power lift of Frobenius ϕ on $A^\dagger$:

$$\phi(x) = x^p,$$

$$\phi(y) = \sqrt{f(x^p)} = y^p \left(1 + \frac{f(x^p) - f(x)^p}{f(x)^p}\right)^{1/2}$$

$$= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Now we use it on $H^1_{MW}(X')^-$; let $\omega_i = \frac{x^i dx}{2y}$.
Then

$$\phi^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j$$

for some $f_i \in A^\dagger$ and some $2g \times 2g$ matrix M.

*p-adic magic: the df_i come from appropriate linear combinations of $d(x^k y^j)$ and $d(y^2 = f(x))$.

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

- Compute $\int_{P'}^{Q'} \omega_j$ by solving a linear system

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^* \omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j.$$

- Compute $\int_{P'}^{Q'} \omega_j$ by solving a linear system

$$\int_{P'}^{Q'} \omega_i = \int_{\phi(P')}^{\phi(Q')} \omega_i$$

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

- Compute $\int_{P'}^{Q'} \omega_j$ by solving a linear system

$$\int_{P'}^{Q'} \omega_i = \int_{P'}^{Q'} \phi^*\omega_i$$

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^* \omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j.$$

- Compute $\int_{P'}^{Q'} \omega_j$ by solving a linear system

$$\int_{P'}^{Q'} \omega_i = \int_{P'}^{Q'} \left(df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j \right)$$

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

- Compute $\int_{P'}^{Q'} \omega_j$ by solving a linear system

$$\int_{P'}^{Q'} \omega_i = \int_{P'}^{Q'} df_i + \sum_{j=0}^{2g-1} M_{ij} \int_{P'}^{Q'} \omega_j$$

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

- Compute $\int_{P'}^{Q'} \omega_j$ by solving a linear system

$$\int_{P'}^{Q'} \omega_i = f_i(Q') - f_i(P') + \sum_{j=0}^{2g-1} M_{ij} \int_{P'}^{Q'} \omega_j.$$

Frobenius and Coleman integrals (B.-Bradshaw-Kedlaya ('10))

- Use Kedlaya's algorithm to calculate the action of Frobenius ϕ on each basis differential, letting

$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

- Compute $\int_{P'}^{Q'} \omega_j$ by solving a linear system

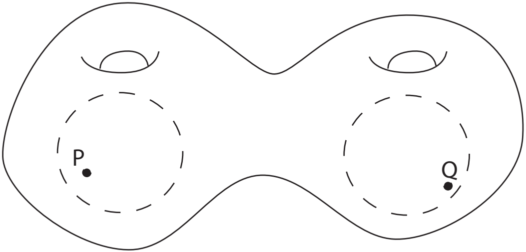
$$\int_{P'}^{Q'} \omega_i = f_i(Q') - f_i(P') + \sum_{j=0}^{2g-1} M_{ij} \int_{P'}^{Q'} \omega_j.$$

- As the eigenvalues of the matrix M are algebraic integers of $\mathbf{C}$-norm $p^{1/2} \neq 1$, the matrix $M - I$ is invertible, and we may solve the system to obtain the integrals $\int_{P'}^{Q'} \omega_i$.

Integrals via Teichmüller, continued

- The linear system gives us the integral between different residue disks.

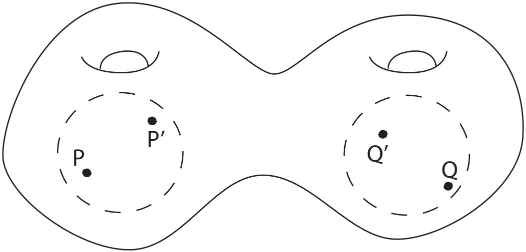
$$\int_P^Q \omega_i =$$



Integrals via Teichmüller, continued

- The linear system gives us the integral between different residue disks.
- Then putting it all together, we have

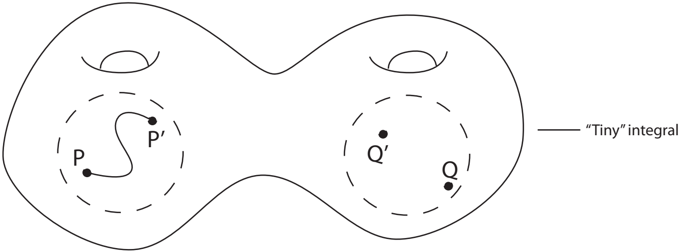
$$\int_P^Q \omega_i =$$



Integrals via Teichmüller, continued

- The linear system gives us the integral between different residue disks.
- Then putting it all together, we have

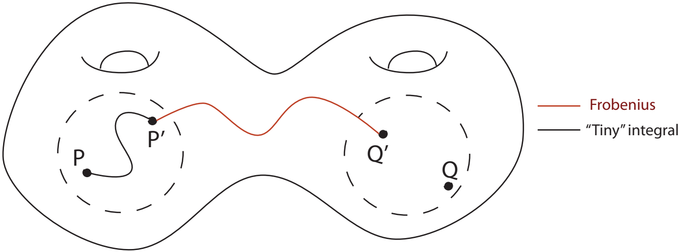
$$\int_P^Q \omega_i = \int_P^{P'} \omega_i$$



Integrals via Teichmüller, continued

- The linear system gives us the integral between different residue disks.
- Then putting it all together, we have

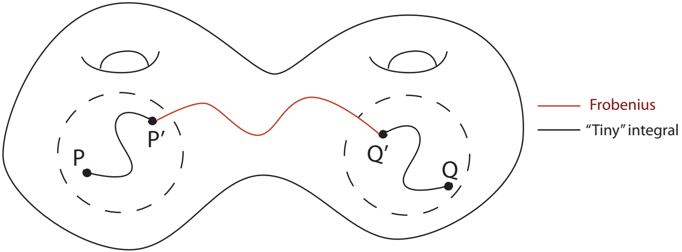
$$\int_P^Q \omega_i = \int_P^{P'} \omega_i + \int_{P'}^{Q'} \omega_i$$



Integrals via Teichmüller, continued

- The linear system gives us the integral between different residue disks.
- Then putting it all together, we have

$$\int_P^Q \omega_i = \int_P^{P'} \omega_i + \int_{P'}^{Q'} \omega_i + \int_{Q'}^{Q} \omega_i$$



Integrating from a Weierstrass residue disk

Suppose we want to integrate from $P = (a, 0)$, a Weierstrass point on X.

- In the previous algorithm, one step is evaluation of f_i on the endpoints of integration.
- But f_i, as an element of $A^\dagger = \left\{ \sum_{i=-\infty}^{\infty} \frac{B_i(x)}{y^i},\ B_i(x) \in K[x], \deg B_i \leqslant 2g \right\}$ need not converge at P.
- However, f_i does converge at any point R near the boundary of the disk, i.e., in the complement of a certain smaller disk which can be bounded explicitly.
- We break up the path as $\int_P^Q \omega_i = \int_P^R \omega_i + \int_R^Q \omega_i$ for a suitable "near-boundary point" R in the disk of P: that is, we evaluate $\int_R^Q \omega$ using Frobenius, then compute $\int_P^R \omega$ as a tiny integral.

Beyond hyperelliptic curves

Jan Tuitman gave practical algorithms (2014, 2015) to compute zeta functions for general curves...

Beyond hyperelliptic curves

Jan Tuitman gave practical algorithms (2014, 2015) to compute zeta functions for general curves...

[joint work with Jan Tuitman]

Dictionary: from Kedlaya to Tuitman

A comparison of the two zeta function algorithms:

algorithm	Kedlaya	Tuitman
curve $X/\mathbf{Q}$	hyperelliptic	general
cohomology	Monsky-Washnitzer	rigid
basis of $H^1(X)$	$\omega_i = \frac{x^i dx}{2y}$	$\omega_i =$ it's complicated*
Frobenius lift ϕ	$\phi : x \to x^p$	
reduction in $H^1(X)$	linear algebra reducing pole order**	
output	$\phi^* \omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j$	

*Main idea: use a map $x : X \to \mathbf{P}^1$ to represent functions and 1-forms on X and then choose a particularly simple Frobenius lift that sends $x \to x^p$

**In Tuitman's algorithm, the goal is the same, but it's worth noting that the linear algebra uses ideas from Lauder's fibration method.

Tuitman's algorithm: setup

- $X/\mathbf{Q}$: nonsingular projective curve given by a (possibly singular) plane model $Q(x,y) = 0$ with $Q(x,y) \in \mathbf{Z}[x,y]$ irreducible and monic in y
- d_x, d_y: degrees of Q in y, x
- p prime of good* reduction for X
- $\Delta(x) \in \mathbf{Z}[x]$ the discriminant of $Q(x,y)$ with respect to y
- $r(x) \in \mathbf{Z}[x]$ squarefree with the same roots as $\Delta(x)$

Note that $r(x) = 0$ gives us a collection of "bad" points: if $r(x_0) = 0$, then one of the following holds:

- the plane model $Q(x,y) = 0$ has a singularity lying over x_0
- the map $x : X \to \mathbf{P}^1$ has a ramification point lying over x_0

*...and further technical reduction conditions on points in the support of $r(x)$ and matrices W^0, W^∞ (next slide) giving integral bases for $\mathbf{Q}(X)$ over $\mathbf{Q}[x]$ and over $\mathbf{Q}[1/x]$

Tuitman's algorithm: integral bases

Let $\mathbf{Q}(X)$ denote the function field of X.

Definition

We let $W^0 \in \mathrm{GL}_{d_y}(\mathbf{Q}[x, 1/r])$ denote a matrix such that if

$$b_j^0 = \sum_{i=0}^{d_y-1} W^0_{i+1,j+1} y^i,$$

then $\{b_0^0, \ldots, b_{d_y-1}^0\}$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[x]$.
Similarly we let $W^\infty \in \mathrm{GL}_{d_y}(\mathbf{Q}[x, 1/x, 1/r])$ denote a matrix such that $\{b_0^\infty, \ldots, b_{d_y-1}^\infty\}$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[1/x]$.

Tuitman's algorithm: integral bases

Let $\mathbf{Q}(X)$ denote the function field of X.

Definition

We let $W^0 \in \mathrm{GL}_{d_y}(\mathbf{Q}[x, 1/r])$ denote a matrix such that if

$$b_j^0 = \sum_{i=0}^{d_y-1} W^0_{i+1,j+1} y^i,$$

then $\{b_0^0, \ldots, b_{d_y-1}^0\}$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[x]$.
Similarly we let $W^\infty \in \mathrm{GL}_{d_y}(\mathbf{Q}[x, 1/x, 1/r])$ denote a matrix such that $\{b_0^\infty, \ldots, b_{d_y-1}^\infty\}$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[1/x]$.

Example

When the plane model $Q(x, y) = 0$ is smooth, we can take $W^0 = I$ since $\{y^0, \ldots, y^{d_y-1}\}$ is already an integral basis.

Tuitman's algorithm: overconvergent rings

Let:

- V be the Zariski open of $\mathbf{P}^1_{\mathbf{Z}_p}$ defined by the two conditions $x \neq \infty$ and $r(x) \neq 0$
- $U = x^{-1}(V)$ the Zariski open of X lying over V.

We take

$$S^\dagger = \mathbf{Q}_p\langle x, 1/r\rangle^\dagger, \quad R^\dagger = \mathbf{Q}_p\langle x, 1/r, y\rangle^\dagger/(Q),$$

where $\langle\rangle^\dagger$ denotes weak completion, i.e.,

$$\mathbf{Q}_p\langle x_1, \ldots, x_m\rangle^\dagger = \{\sum_I c_I x_1^{i_1} \cdots x_m^{i_m} : \text{radius of convergence} > 1\}$$

Tuitman's algorithm: Frobenius

We lift p-power Frobenius ϕ to $S^\dagger = \mathbf{Q}_p\langle x, 1/r\rangle^\dagger$ and $R^\dagger = \mathbf{Q}_p\langle x, 1/r, y\rangle^\dagger/(Q)$ in the following way:

- Let $\phi(x) = x^p$
- Compute $\phi(1/r) \in S^\dagger$ Hensel lifting $\phi(1/r) = 1/r(x^p)$, starting from $1/r^p$
- Compute $\phi(y) \in R^\dagger$ Hensel lifting $Q(x^p, \phi(y)) = 0$, starting from y^p

We compute the action of Frobenius on a basis of differentials and reduce in cohomology using linear algebra, writing everything with respect to integral bases $\{b_i^0\}$ and $\{b_i^\infty\}$.

We computes $H^1(X) \subset H^1(U)$ as the kernel of a residue map.

Matrix of Frobenius and Coleman integration

As before, by applying ϕ and reducing within cohomology, we can find a matrix M and functions $f_0, \ldots, f_{2g-1} \in R^\dagger$ such that

$$\phi^*(\omega_i) = df_i + \sum_j M_{ij}\omega_j$$

for $i = 0, \ldots, 2g-1$, where M is the matrix of Frobenius on $H^1(X)$ wrt the basis $\{\omega_0, \ldots, \omega_{2g-1}\}$

To compute Coleman integrals $\int_P^Q \omega_j$ we solve the linear system via Teichmüller points P', Q'

$$\int_{P'}^{Q'} \omega_i = f_i(Q') - f_i(P') + \sum_{j=0}^{2g-1} M_{ij} \int_{P'}^{Q'} \omega_j$$

and correct endpoints.

In joint work with Jan Tuitman, we have an algorithm that does this, along with precision bounds, and a Magma implementation.

Example: computing rational points $X_{split}(13)$

The "cursed" modular curve $X = X_{split}(13)$ is a smooth plane quartic with genus 3 and rank 3, given by

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

By computing various types of Coleman integrals on X and carrying out explicit nonabelian Chabauty on this curve, we can prove that it has no rational points apart from previously known ones.

Theorem (B., Dogra, Müller, Tuitman, Vonk)

We have $|X_{split}(13)(\mathbf{Q})| = 7$.

Future work: what else can Coleman integrals do?

- Chabauty-Coleman method for finding rational points on curves (with small rank)
- Kim's nonabelian Chabauty method: extend this to higher rank by considering *iterated* Coleman integrals
- Local p-adic heights on curves: $h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$, part of a global p-adic height
- p-adic regulators