Explicit p-adic integration on curves

Jennifer Balakrishnan

Boston University

Branching from number theory: p-adics in the sciences
September 1, 2021

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 Noam Elkies and Michael Stoll in 2008.

Example 2: A question about triangles

We say a *rational* triangle is one with sides of rational lengths.

Question

Does there exist a rational right triangle and a rational isosceles triangle that have the same perimeter and the same area?

Example 2: A question about triangles

We say a *rational* triangle is one with sides of rational lengths.

Question

Does there exist a rational right triangle and a rational isosceles triangle that have the same perimeter and the same area?

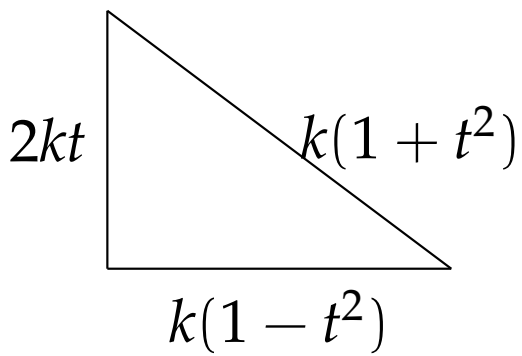
This feels like a very classical question but the answer is surprising – this was the result of work by Y. Hirakawa and H. Matsumura in 2018.

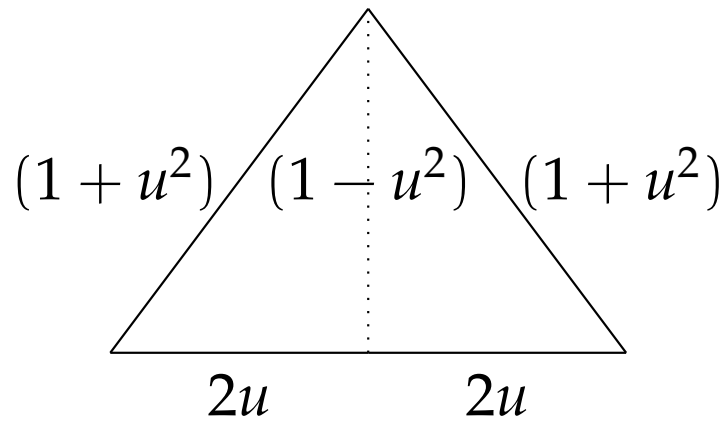
A question about triangles

Assume that there exists such a pair of triangles (rational right triangle, rational isosceles triangle). By rescaling both of the given triangles, we may assume their lengths are

$$(k(1+t^2), k(1-t^2), 2kt) \quad \text{and} \quad ((1+u^2), (1+u^2), 4u),$$

respectively, for some rational numbers $0 < t, u < 1, k > 0$.





A question about triangles

Given side lengths of

$$(k(1+t^2), k(1-t^2), 2kt) \quad \text{and} \quad ((1+u^2), (1+u^2), 4u),$$

by comparing perimeters and areas, we have

$$k + kt = 1 + 2u + u^2 \qquad \text{and} \qquad k^2 t(1-t^2) = 2u(1-u^2).$$

By a change of coordinates, this is equivalent to studying rational points on the genus 2 curve given by

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

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

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

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

We find the points

$$(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3), \infty^{\pm}$$

in $X(\mathbf{Q})$. We've found 10 points!

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

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

We find the points

$$(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3), \infty^{\pm}$$

in $X(\mathbf{Q})$. We've found 10 points!

So we have provably determined $X(\mathbf{Q})$.

A question about triangles

So we consider the rational points on

$$X : y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6.$$

The *Chabauty–Coleman bound* tells us that

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

We find the points

$$(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3), \infty^{\pm}$$

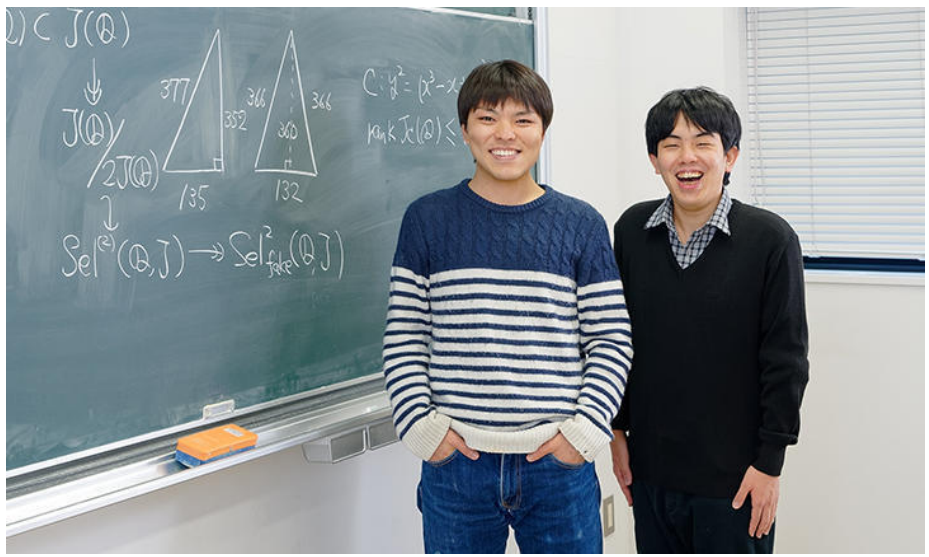
in $X(\mathbf{Q})$. We've found 10 points!
So we have provably determined $X(\mathbf{Q})$.

And $(12/11, 868/11^3)$ gives rise to a pair of triangles.

A question about triangles: answer

Theorem (Hirakawa–Matsumura, 2018)

Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle that have the same perimeter and the same area. The unique pair consists of the right triangle with sides of lengths $(377, 135, 352)$ *and the isosceles triangle with sides of lengths* $(366, 366, 132)$.



Yoshinosuke Hirakawa and Hideki Matsumura

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:
- Crucial hypothesis: satisfying an inequality between the **genus** of the curve X and the **rank** of the Mordell-Weil group of its Jacobian $J(\mathbf{Q})$

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:
- Crucial hypothesis: satisfying an inequality between the **genus** of the curve X and the **rank** of the Mordell-Weil group of its Jacobian $J(\mathbf{Q})$
- Theorem: work of Chabauty and Coleman

Chabauty–Coleman

What allows us to compute $X(\mathbf{Q})$ in the previous example?

- Used the Chabauty–Coleman bound that, for this curve, implied $|X(\mathbf{Q})| \leqslant 10$:
- Crucial hypothesis: satisfying an inequality between the **genus** of the curve X and the **rank** of the Mordell-Weil group of its Jacobian $J(\mathbf{Q})$
- Theorem: work of Chabauty and Coleman
- ...and a bit of luck!

The Chabauty–Coleman method

In 1985, Coleman observed that one could make the following theorem of Chabauty *effective*:

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.

Coleman did this by translating it in terms of p-adic (Coleman) integrals of regular 1-forms.

The Chabauty–Coleman method

In 1985, Coleman observed that one could make the following theorem of Chabauty *effective*:

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.

Coleman did this by translating it in terms of p-adic (Coleman) integrals of regular 1-forms.

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 Coleman integral $\int_b^* \omega$, with $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

The Chabauty–Coleman method

In 1985, Coleman observed that one could make the following theorem of Chabauty *effective*:

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.

Coleman did this by translating it in terms of p-adic (Coleman) integrals of regular 1-forms.

We have

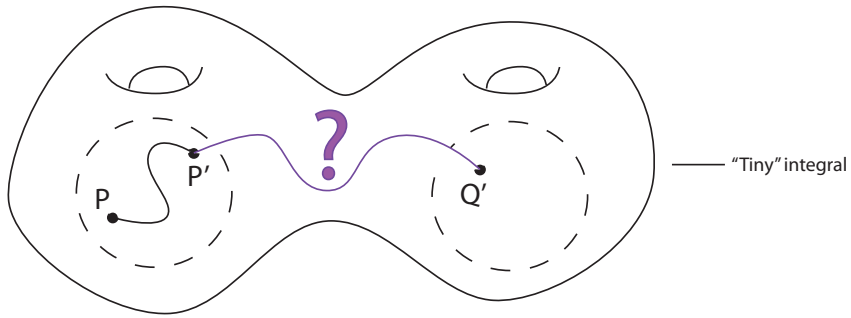
$$X(\mathbf{Q}) \subset X(\mathbf{Q}_p)_1 := \left\{ z \in X(\mathbf{Q}_p) : \int_b^z \omega = 0 \right\}$$

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

To carry out the method, we compute an annihilating differential ω and then calculate the finite set of p-adic points $X(\mathbf{Q}_p)_1$. This works very well in practice, and in general, uses the explicit computation of Coleman integrals.

Coleman integration

Coleman integrals are p-adic *line integrals*.



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

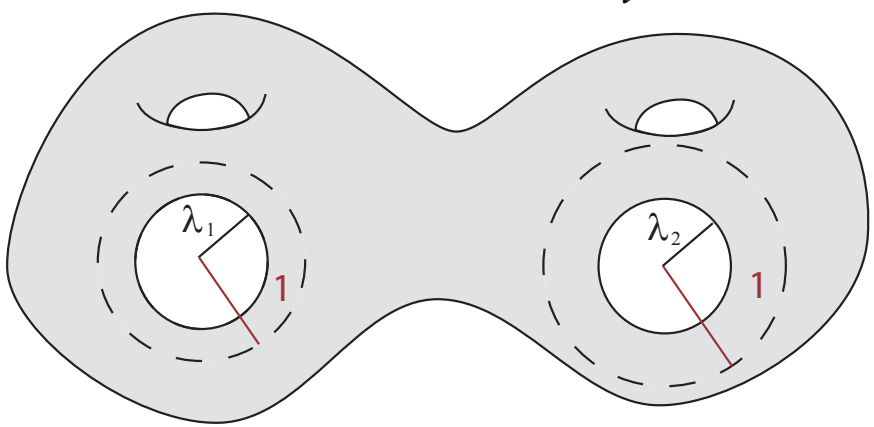
- We can construct local ("tiny") integrals easily, but extending them to the entire space is challenging.
- Coleman's solution: *analytic continuation along Frobenius*, giving rise to a theory of p-adic line integration satisfying the usual nice properties: linearity, additivity, change of variables, fundamental theorem of calculus.
- Idea: compute action of Frobenius on appropriate basis differentials, reduce back to the basis using relations in cohomology, and integrate by solving a linear system.

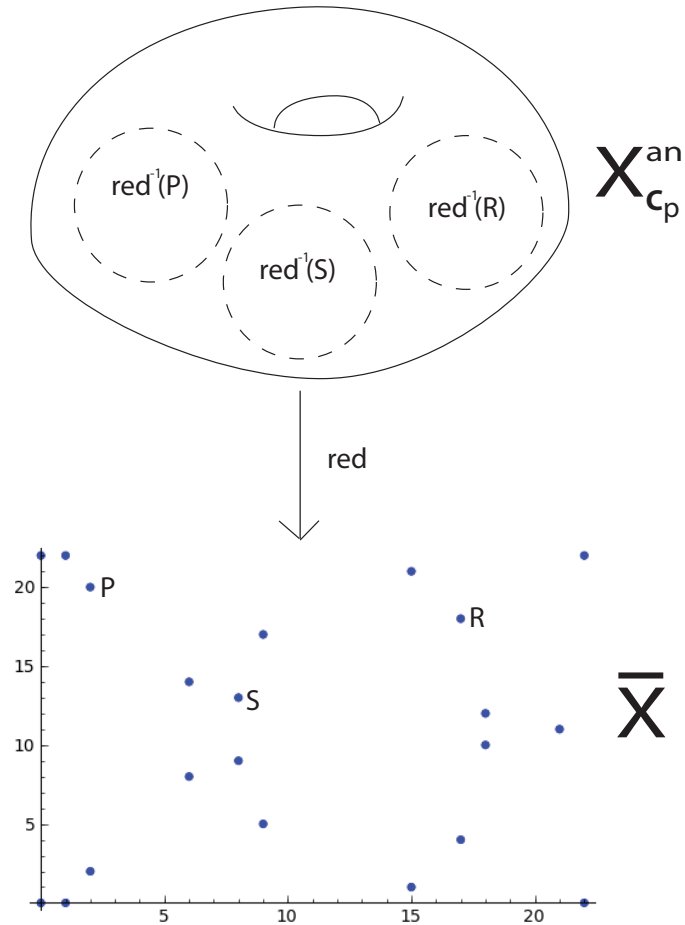
Notation and setup

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





Warm-up: Computing "tiny" integrals

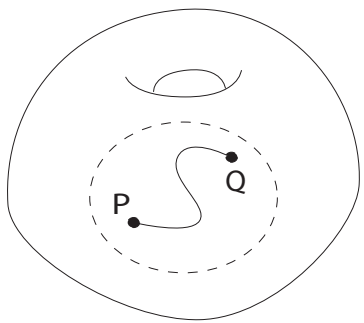
We refer to any Coleman integral of the form $\int_P^Q \omega$ in which P, Q lie in the same residue disk (so $P \equiv Q \pmod{p}$) as a *tiny integral*. To compute such an integral:

- 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.

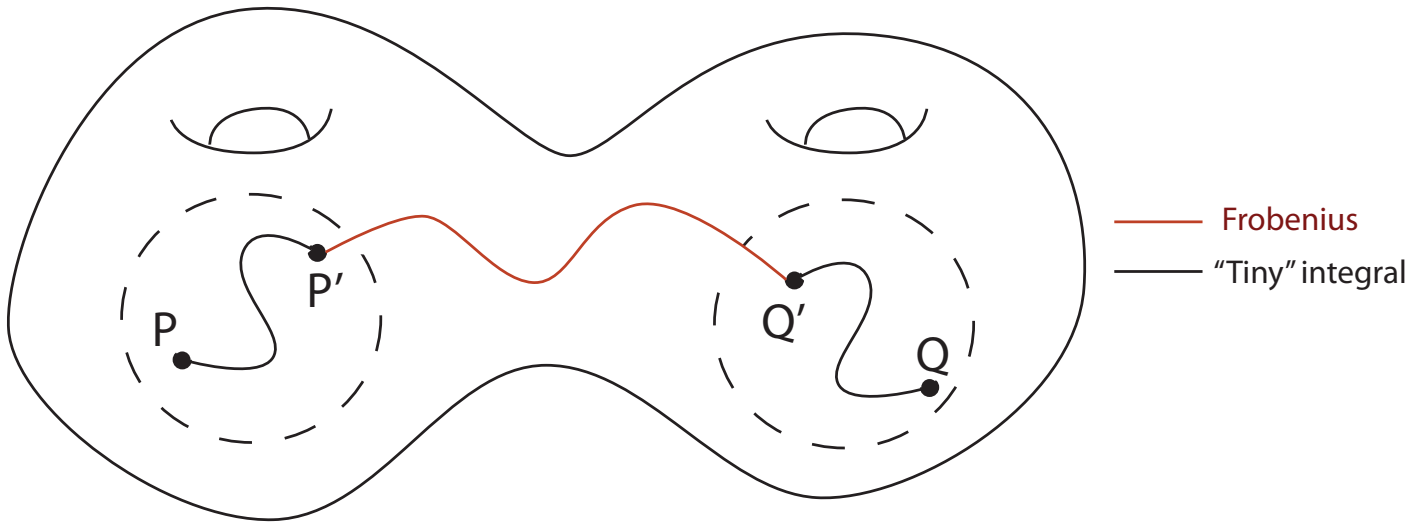
Properties of the Coleman integral include:

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.

From zeta functions to Coleman integrals

p-adic algorithms for computing zeta functions (i.e., computing action of Frobenius on p-adic cohomology) can be used to compute Coleman integrals:

- One fast way of computing zeta functions of hyperelliptic curves over finite fields is Kedlaya's algorithm (2001).
- Kedlaya's algorithm can be recast into an algorithm for computing Coleman integrals (B.–Bradshaw–Kedlaya 2010).
- Long-term goals: adapt generalizations of Kedlaya's algorithm to give Coleman integration algorithms in various new contexts.

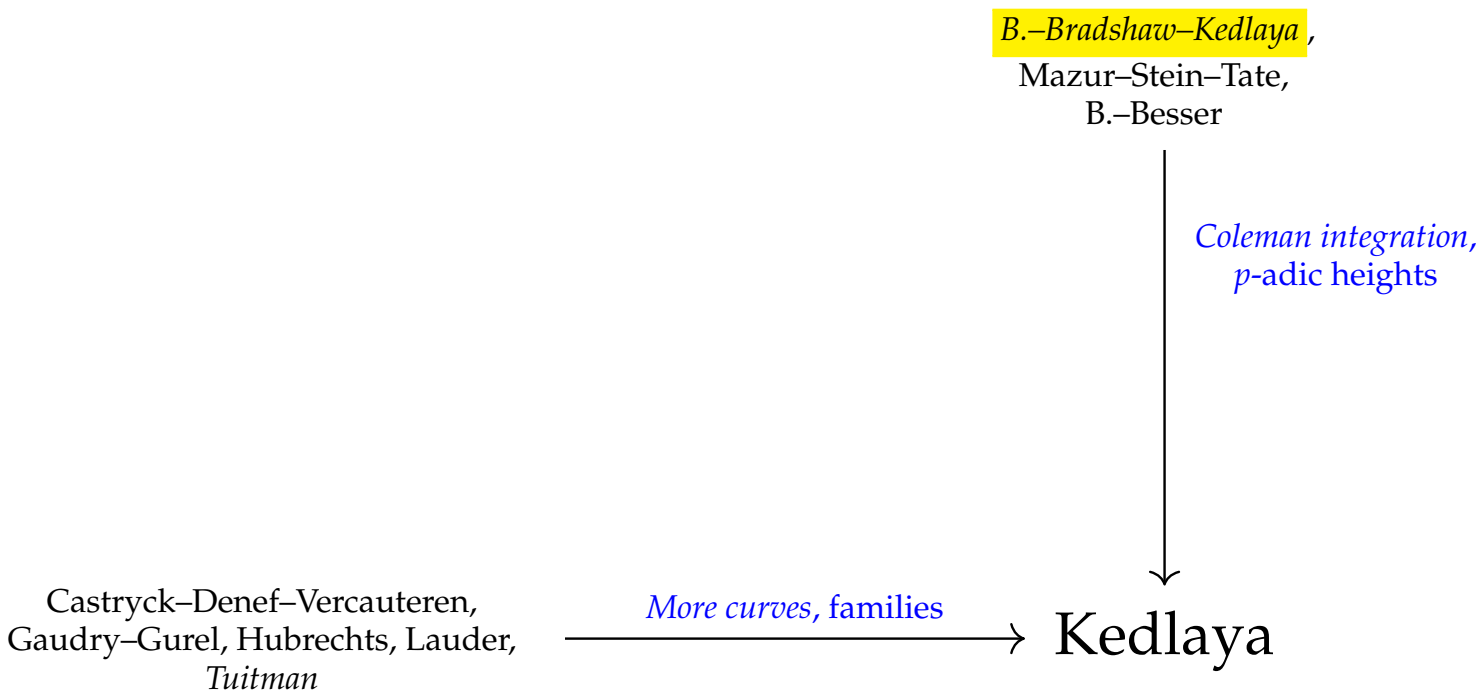
The big picture*

Kedlaya

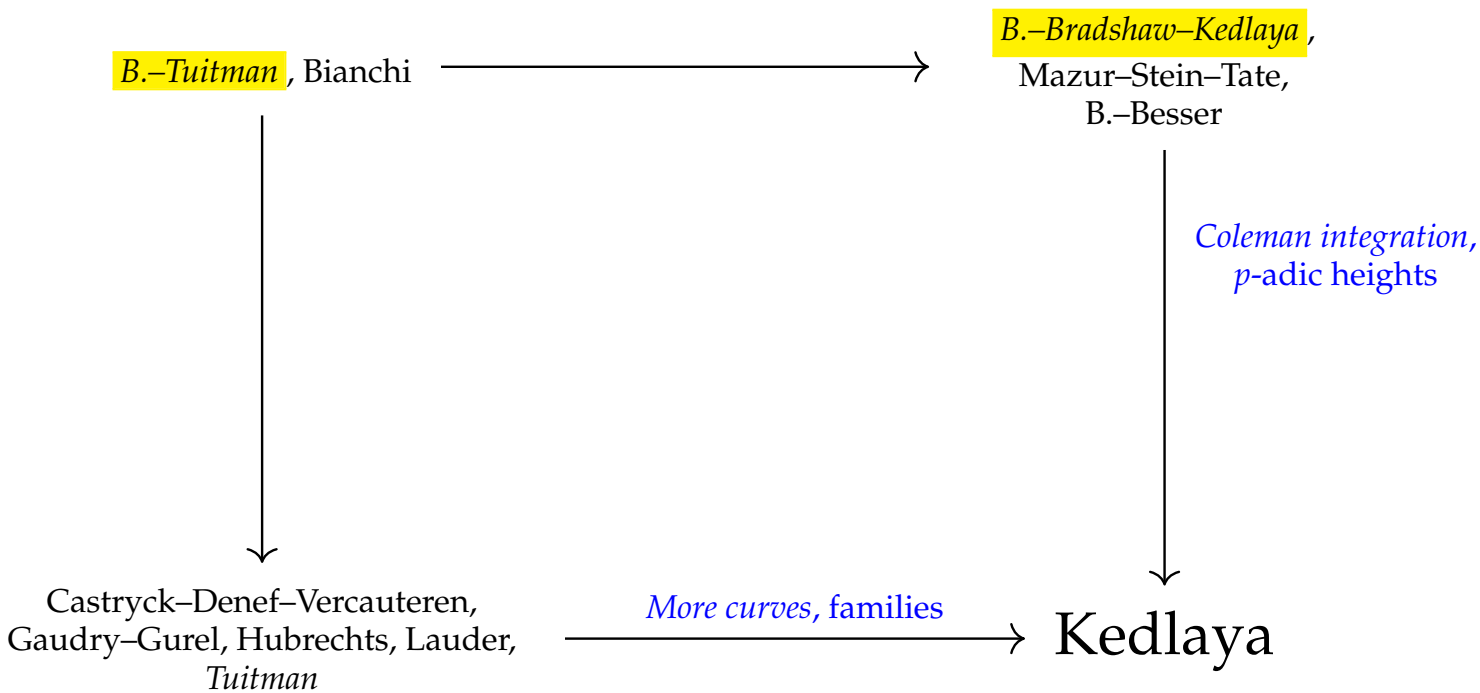
The big picture*

Castryck–Denef–Vercauteren, Gaudry–Gurel, Hubrechts, Lauder, *Tuitman* —*More curves*, families→ Kedlaya

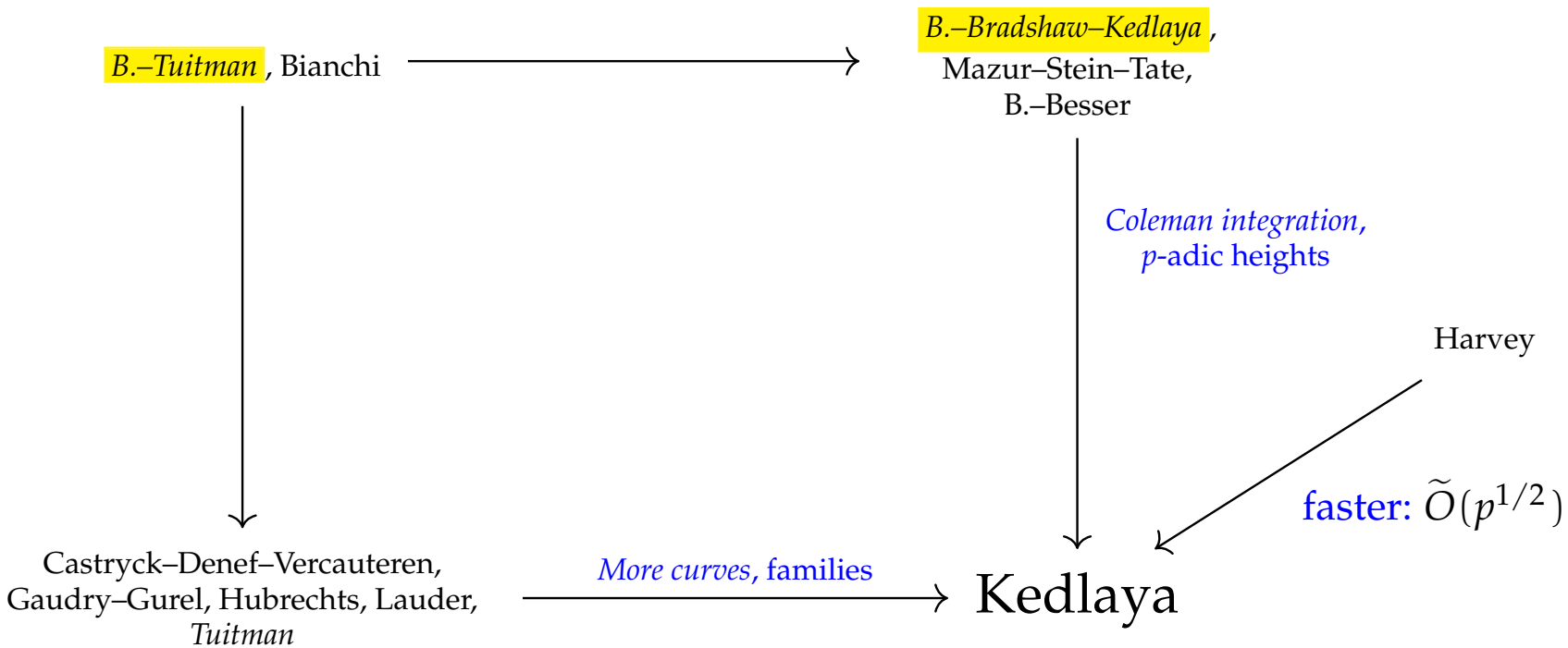
The big picture*



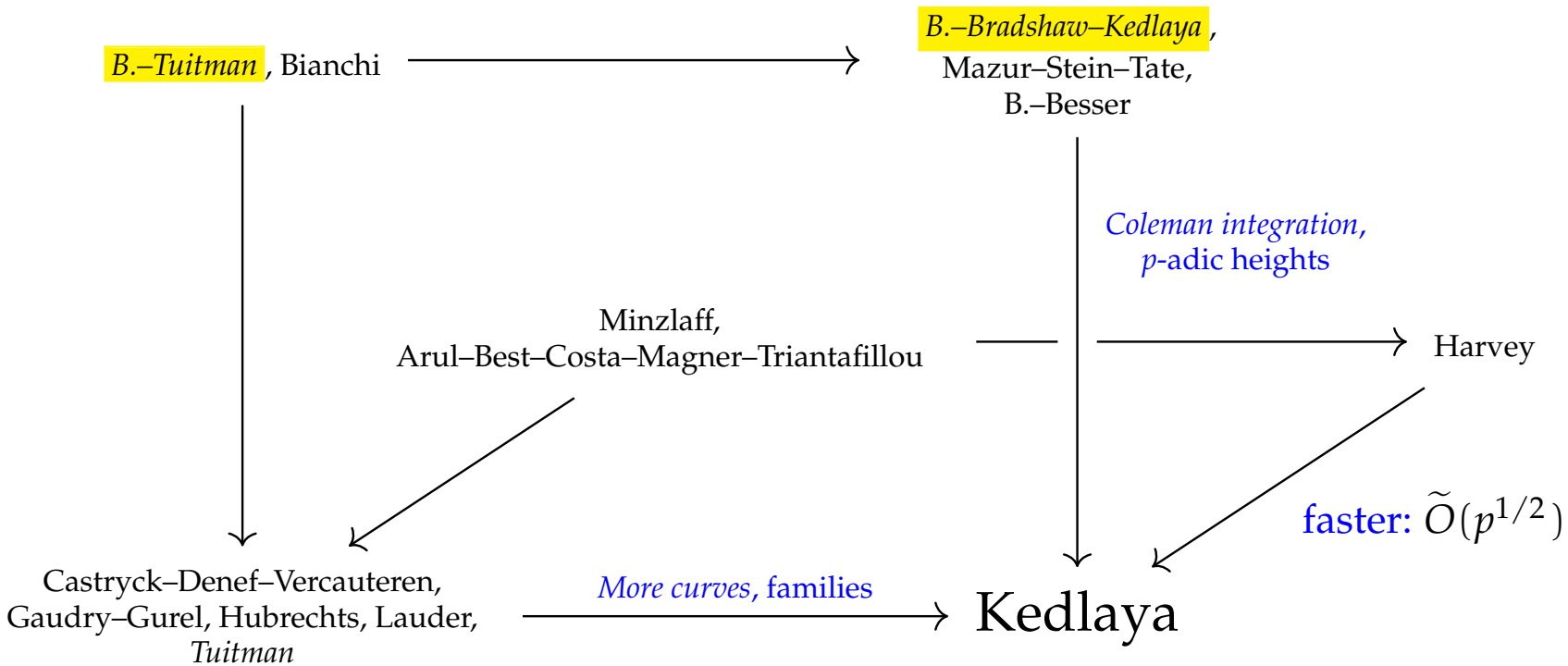
The big picture*



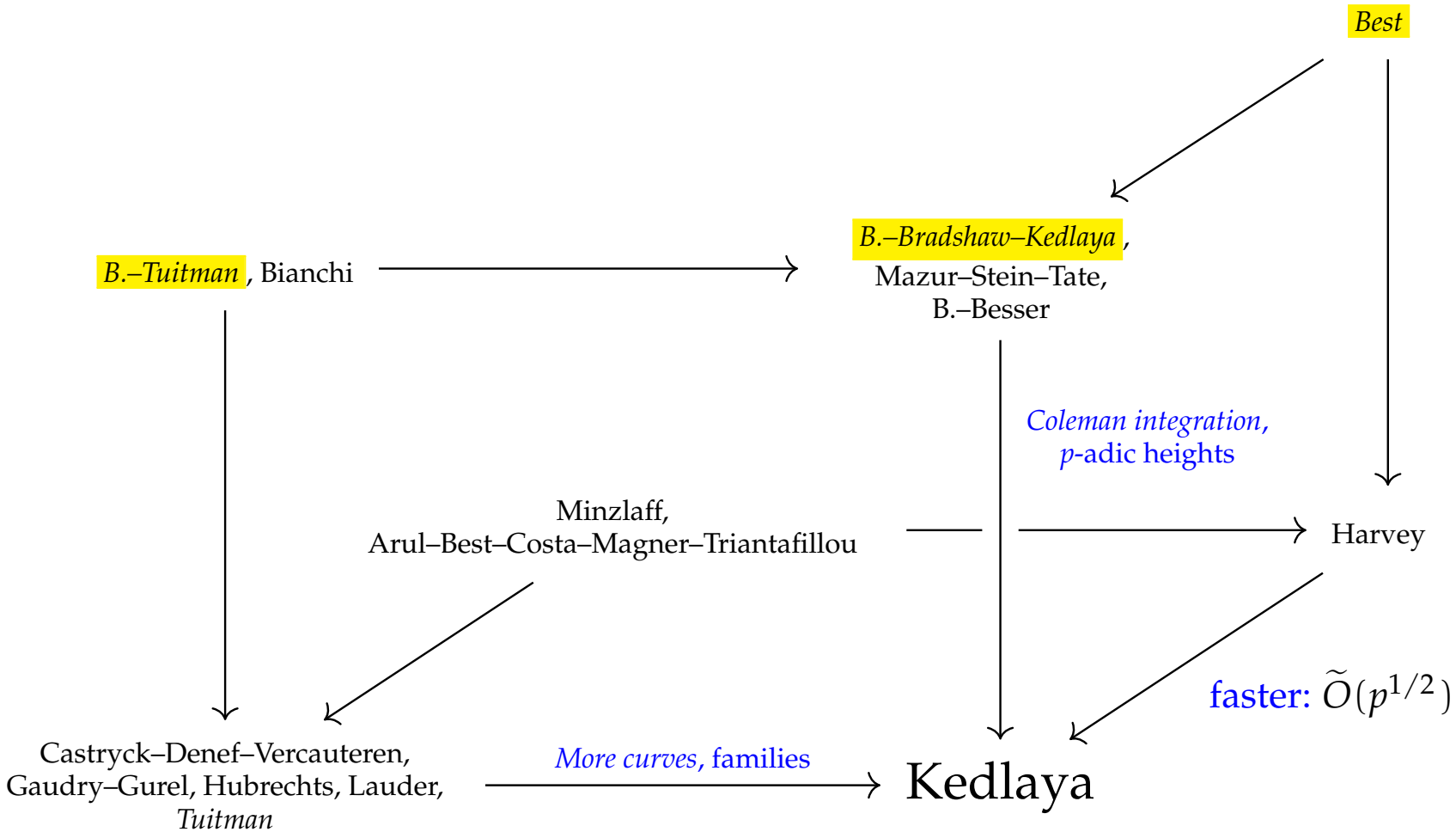
The big picture*



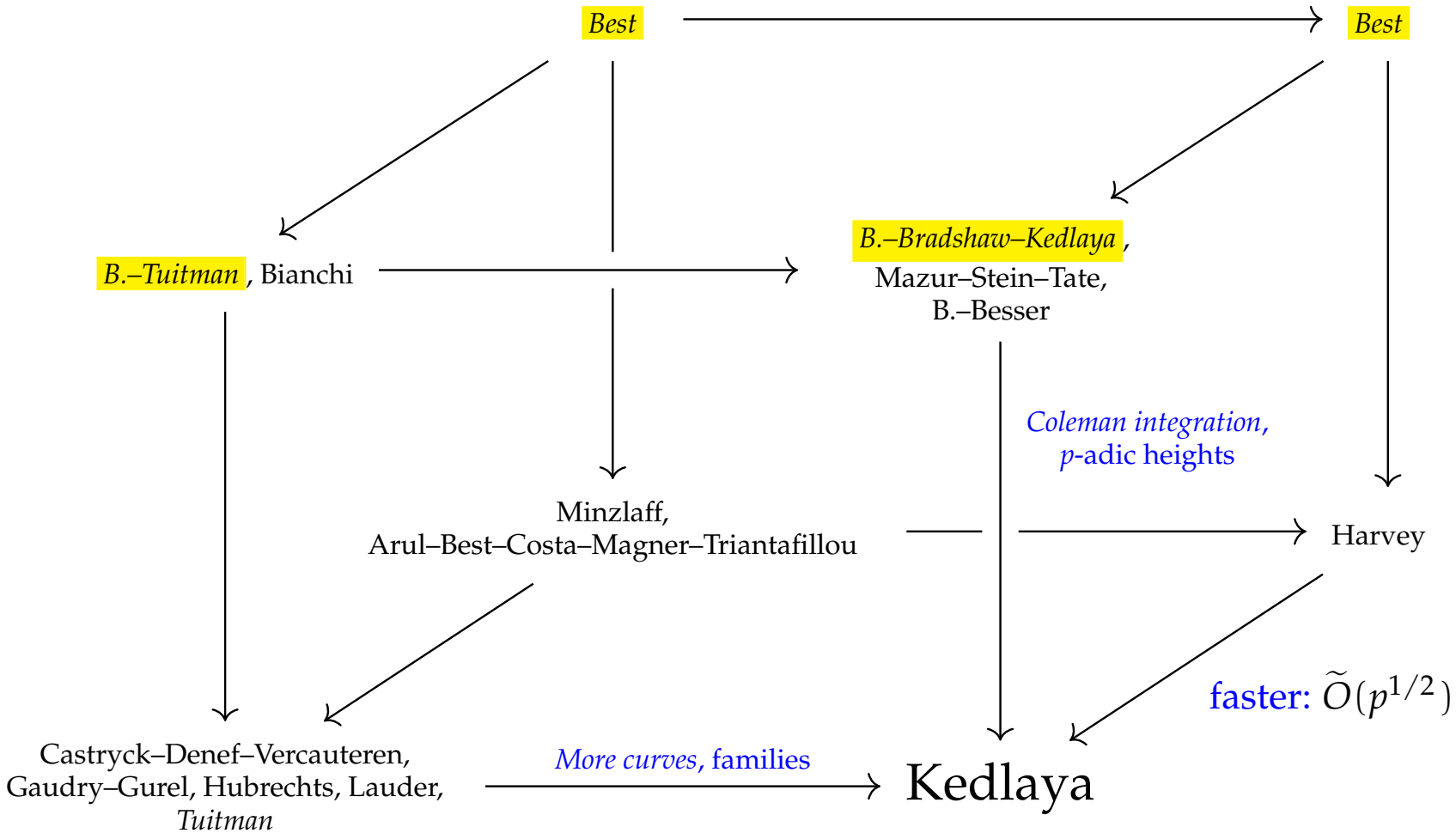
The big picture*



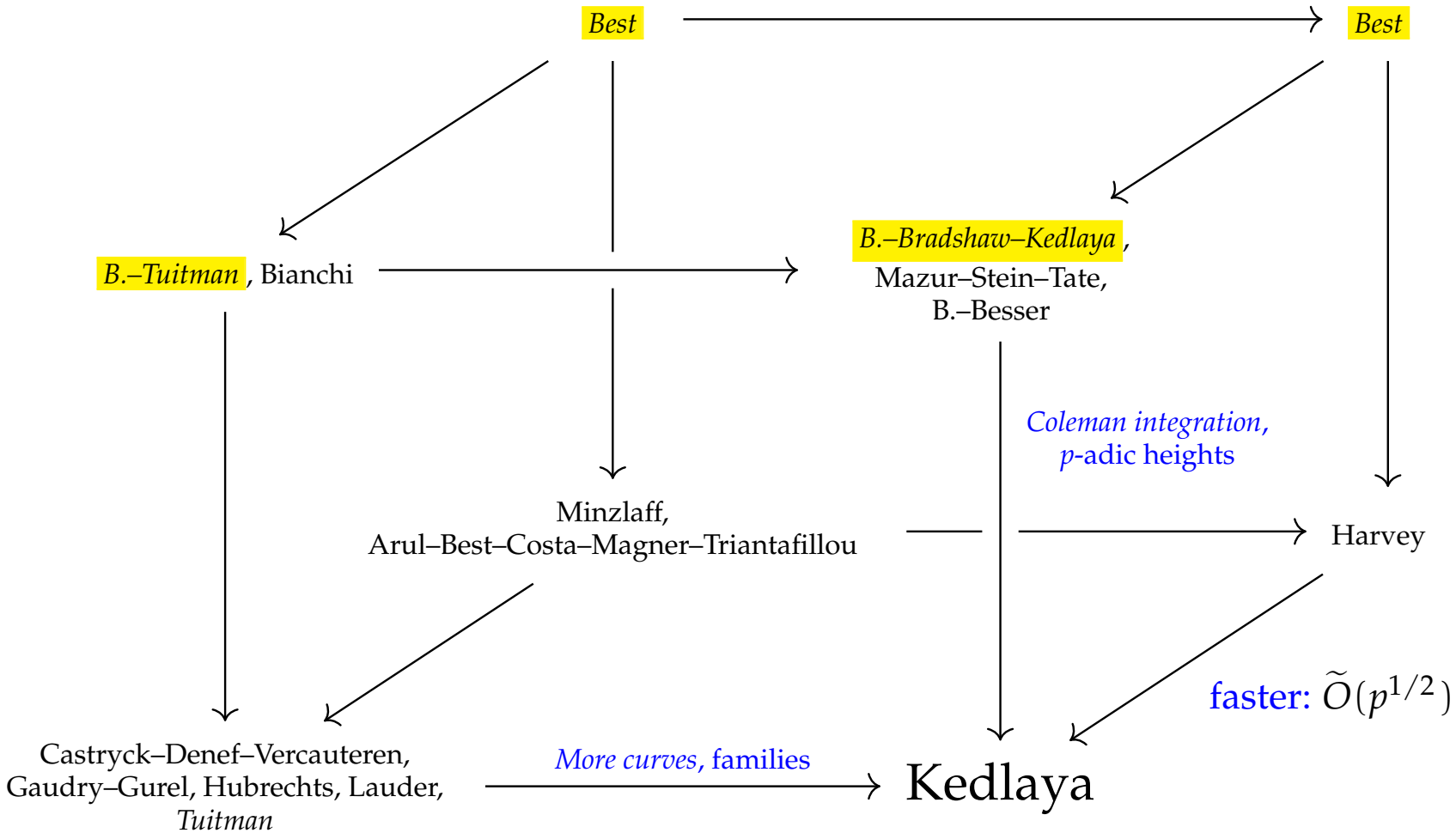
The big picture*



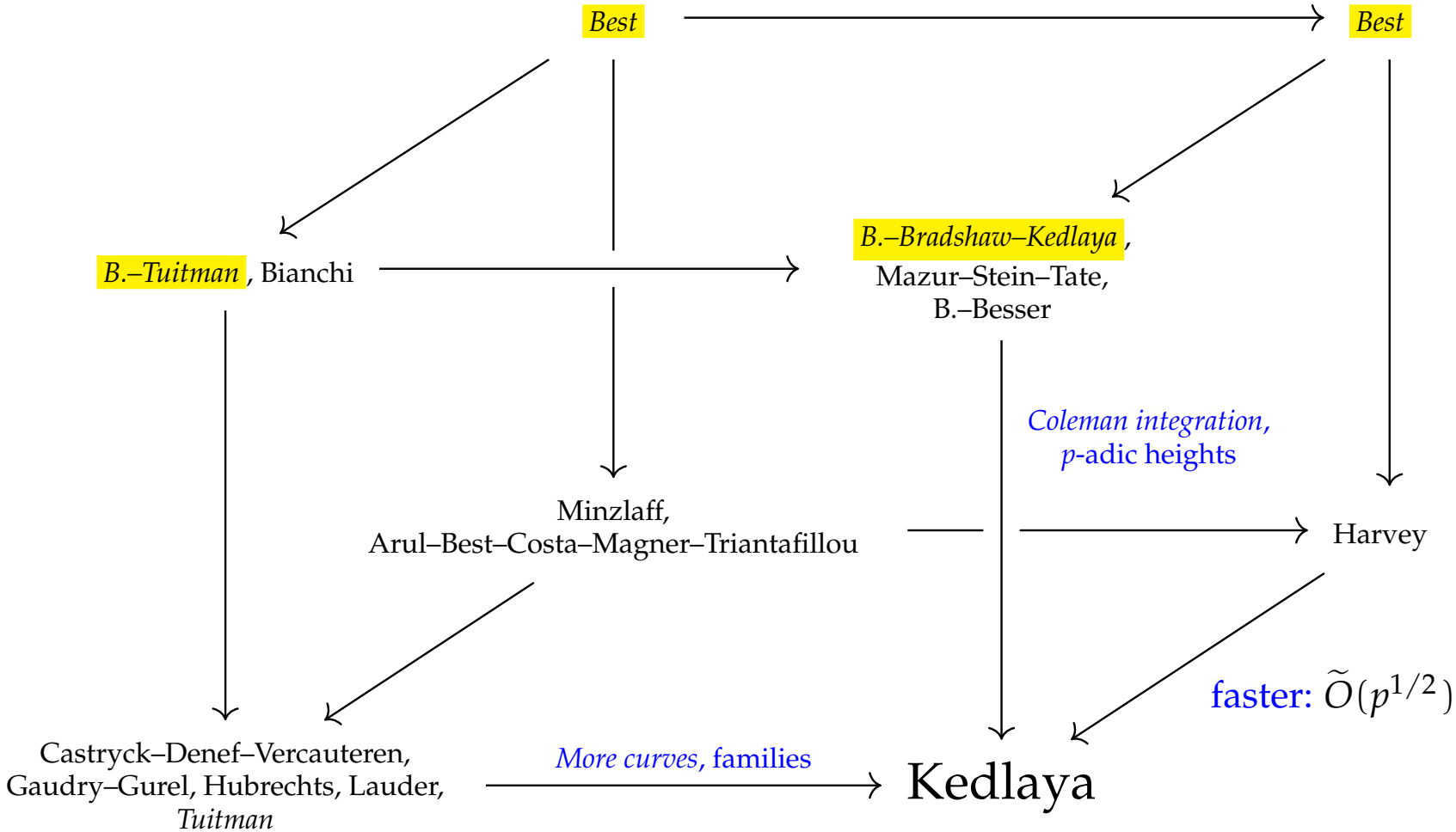
The big picture*



The big picture*



The big picture*



And more: "even faster" via average polynomial time (Harvey), iterated Coleman integration (B.), higher-dimensional varieties (Costa-Harvey-Kedlaya), . . .

*With many thanks to Alex Best for this diagram

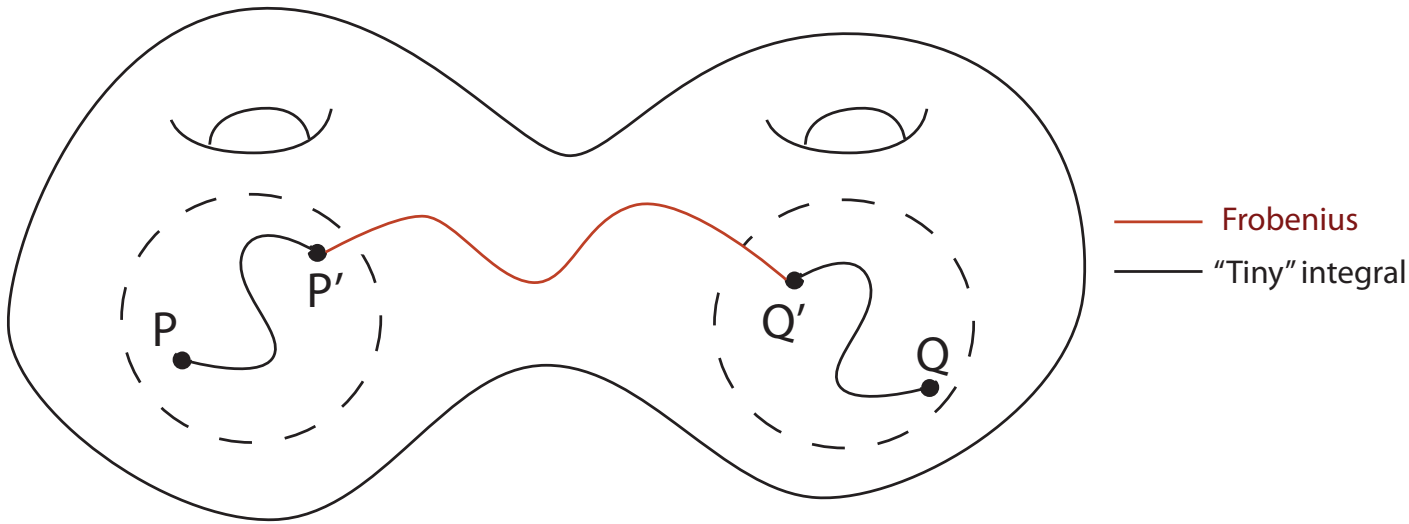
From zeta functions to Coleman integrals

So we will first discuss how to compute Coleman integrals on hyperelliptic curves (B.–Bradshaw–Kedlaya from Kedlaya) and then mention two related results:

- extending this to general curves (B.–Tuitman)
- how Harvey's adaptation of Kedlaya's algorithm can be used to give faster Coleman integration for large p (Best)

Recall: 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 ($X - \{\text{Weierstrass points of } X\}$)
- 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 $A^\dagger$:

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

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

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

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

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 $\omega_i = \frac{x^i dx}{2y}$.

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

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 $\omega_i = \frac{x^i dx}{2y}$.

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

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 $\omega_i = \frac{x^i dx}{2y}$.

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

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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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 $\int_{P'}^{Q'} \omega_i$.

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.

Implementation: Coleman integration for hyperelliptic curves

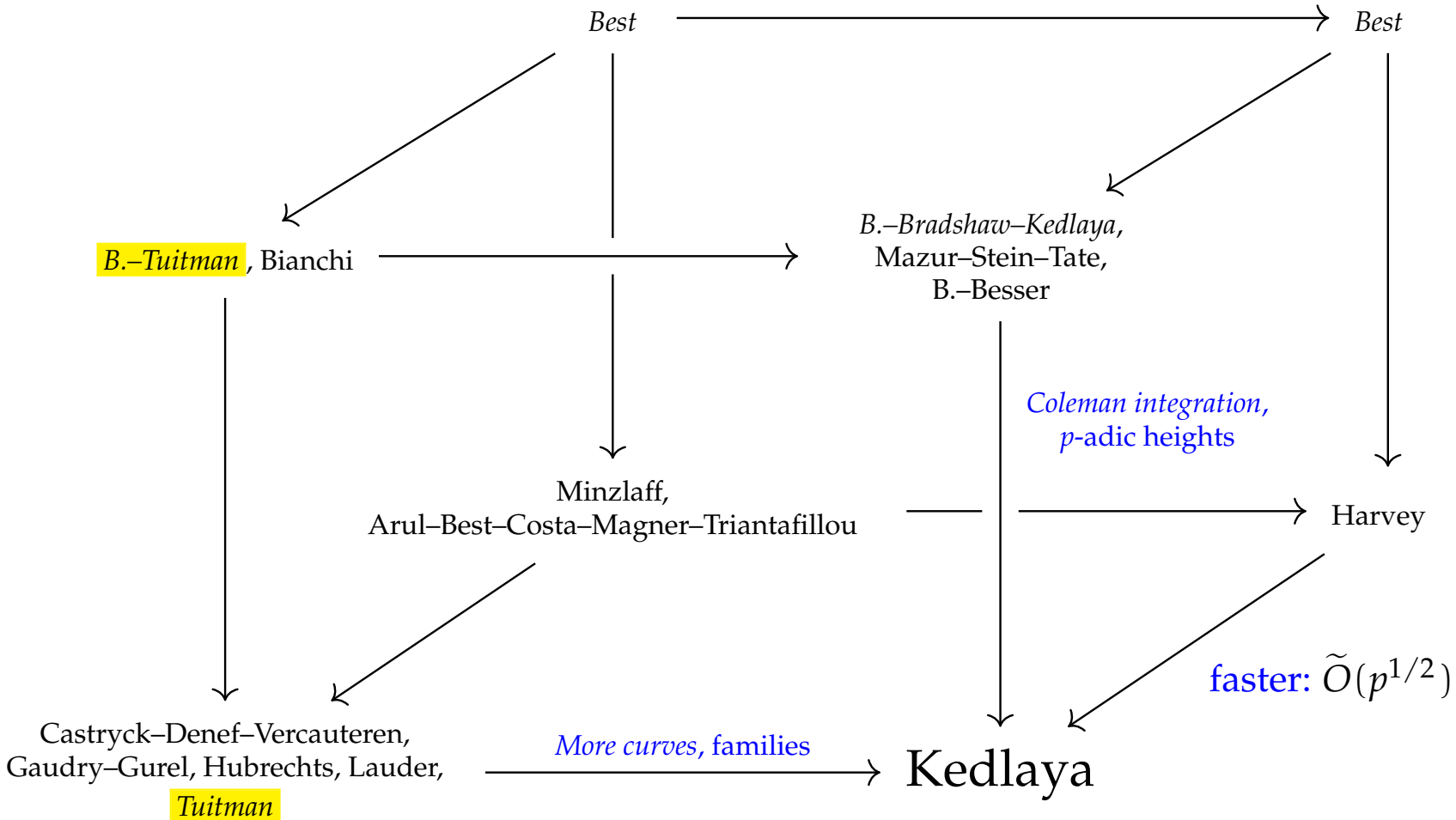
- Coleman integration for hyperelliptic curves over $\mathbf{Q}_p$ is in SageMath (B.–Bradshaw–Kedlaya).
- This uses extensive work of David Roe and others in developing the p-adics in SageMath.

Implementation: Coleman integration for hyperelliptic curves

- Coleman integration for hyperelliptic curves over $\mathbf{Q}_p$ is in SageMath (B.–Bradshaw–Kedlaya).
- This uses extensive work of David Roe and others in developing the p-adics in SageMath.

```
R.<x> = QQ[]
X = HyperellipticCurve(x^5-2*x^3+x+1/4)
p = 3
K = Qp(p,15)
XK = X.change_ring(K)
XK.coleman_integrals_on_basis(XK(0,1/2),XK(-1,-1/2)) #basis is {x^i*dx/(2y)}, i = 0,...,3
(3 + 3^2 + 3^4 + 3^5 + 2*3^6 + 2*3^7 + 2*3^8 + 3^10 + O(3^11),
2 + 2*3 + 2*3^3 + 3^4 + 3^6 + 2*3^8 + 2*3^9 + O(3^10),
2*3^-1 + 2*3 + 2*3^2 + 3^3 + 3^5 + 3^6 + 3^7 + O(3^9),
2*3^-2 + 3^-1 + 2 + 2*3 + 3^2 + 2*3^3 + 3^4 + 2*3^5 + 2*3^6 + 2*3^7 + O(3^8))
```

Coleman integration for smooth curves



Dictionary: from Kedlaya to Tuitman

A comparison of two zeta function algorithms:

algorithm	Kedlaya (2001)	Tuitman (2014, 2015)
curve $X/\mathbf{Q}$	hyperelliptic	smooth
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 $x \to x^p$

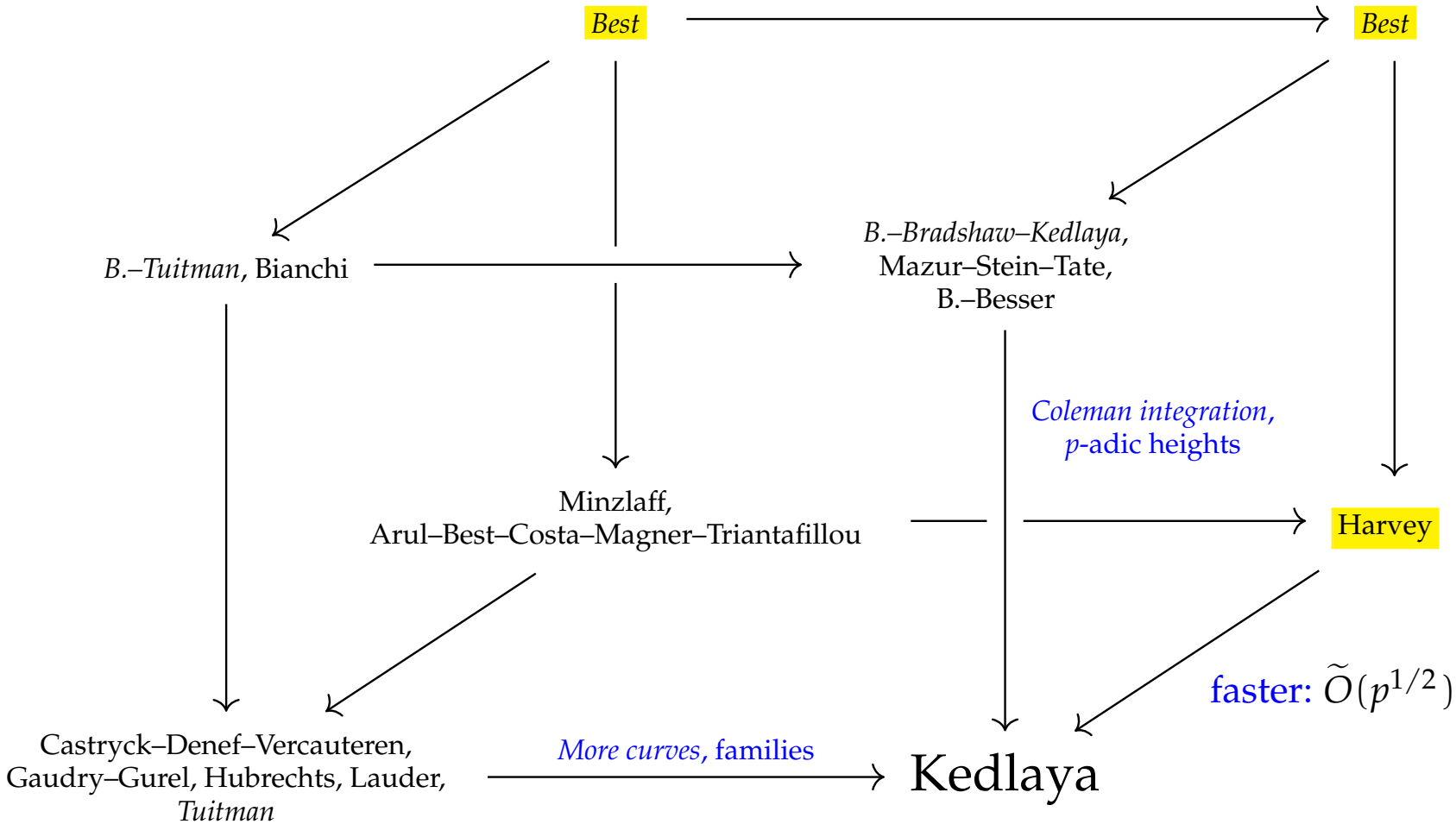
**In Tuitman's algorithm, the goal is the same, but it's worth noting that the linear algebra uses ideas from Lauder's fibration method.

Implementation: Coleman integration for curves

- Coleman integration for smooth curves over $\mathbf{Q}_p$ is available as a Magma package (B.–Tuitman) on GitHub.

```
> load "coleman.m";
> Q:=y^3 - (x^5 - 2*x^4 - 2*x^3 - 2*x^2 - 3*x);
> p:=7;
> N:=20;
> data:=coleman_data(Q,p,N);
> P1:=set_point(1,-2,data);
> P2:=set_point(0,0,data);
IP1P2,N2:=coleman_integrals_on_basis(P1,P2,data:e:=50);
> IP1P2;
(12586493*7 + O(7^10) 19221514*7 + O(7^10) -19207436*7 + O(7^10)
-10636635*7 + O(7^10) 128831118 + O(7^10) 67444962 + O(7^10)
-23020322 + O(7^10) 401602170*7^-1 + O(7^10))
```

Fast Coleman integration for superelliptic curves



From Kedlaya to Harvey

- Kedlaya's algorithm gives that the action of ϕ^* on $H^1_{MW}(X')^-$ can be computed in time $\widetilde{O}(p)$, where ϕ denotes a p-power lift of Frobenius.
- Harvey showed that if $p > (2g+1)(2N-1)$, then the action of ϕ^* on $H^1_{MW}(X')^-$ can be computed in time $\widetilde{O}(p^{1/2})$.

For both zeta function algorithms, what is essential is finding M such that

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

in particular, they do not need df_i. However for Coleman integration, we need the f_i. In Kedlaya's algorithm, the reduction process at each step constructs f_i: if we subtract dg for a monomial g to reduce the pole order of $\phi^*(\omega_i)$, then

$$f_i := f_i + g.$$

Harvey's modifications

- Harvey structures the reductions and keeps track of "horizontal" reductions (lowering degree in x) and "vertical" reductions (lowering degree in y^{-1}).
- He interprets these as linear recurrence relations in cohomology.
- Work of Bostan–Gaudry–Schost gives a fast way to compute a product of these reductions.

From Harvey to Best

- If we subtract dg for a monomial g to reduce, need to keep track of evaluation of g on points.
- But this is no longer linear in the reduction index and BGS no longer applies!
- Trick: use Horner's method to compute the evaluation of g: instead of computing $\sum_{i=0}^{N} a_i x^i$ by computing sequentially $\left(\sum_{i=t}^{N} a_i x^i\right)_{t=N,N-1,\ldots,0}$, compute

$$((\cdots((a_N)x + a_{N-1})x + \cdots)x + a_0)$$

  from the inside to the out.
- This *is* an iterated composition of linear functions, each of which is linear in the reduction index.
- Best uses this to give an $\widetilde{O}(p^{1/2})$ Coleman integration algorithm for hyperelliptic and superelliptic curves.

Implementation: fast Coleman integration

- Fast Coleman integration for superelliptic curves over unramified extensions of $\mathbf{Q}_p$ is available as a Julia/Nemo package (Best) on GitHub.
- Nemo: a new system for computing in commutative algebra, number theory and group theory that is based on several low-level libraries such as MPIR, Flint, Arb, and Antic (maintained by William Hart, Tommy Hofmann, Claus Fieker, and Fredrik Johansson).

Computing iterated integrals

These algorithms have natural generalizations to n-fold iterated integrals:

$$\int_P^Q \omega_n \cdots \omega_1 = \int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1)\, dt_n \cdots dt_1.$$

We focus on the case $n = 2$ and discuss explicit double Coleman integrals. Our convention:

$$\int_P^Q \omega_i \omega_j := \int_P^Q \omega_i(R) \int_P^R \omega_j.$$

Moving between different disks

As before, we can link integrals between non-Weierstrass points via Frobenius.

To compute the integrals $\int_P^Q \omega_i\omega_k$ when P, Q are in different disks:

- Compute Teichmüller points P', Q' in the disks of P, Q.
- Use Frobenius to calculate $\int_{P'}^{Q'} \omega_i\omega_k$.
- Recover the double integral:
$\int_P^Q \omega_i\omega_k = \int_{P'}^{Q'} \omega_i\omega_k - \int_{P'}^{P} \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{P'}^{P} \omega_k\right) - \left(\int_Q^{Q'} \omega_i\right)\left(\int_{P'}^{Q'} \omega_k\right) + \int_{Q'}^{Q} \omega_i\omega_k.$

Expanding Frobenius

Suppose P, Q are Teichmüller. We have

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

Expanding Frobenius

Suppose P, Q are Teichmüller. We have

$$\int_P^Q \omega_i \omega_k = \int_P^Q (\phi^* \omega_i)(\phi^* \omega_k)$$

Expanding Frobenius

Suppose P, Q are Teichmüller. We have

$$\int_P^Q \omega_i \omega_k = \int_P^Q \left(df_i + \sum_{j=0}^{2g-1} M_{ij} \omega_j \right) \left(df_k + \sum_{j=0}^{2g-1} M_{kj} \omega_j \right)$$

The linear system

For all $0 \leqslant i,k \leqslant 2g-1$, define the constants c_{ik}:

$$c_{ik} = \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P))$$
$$+ \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R)(f_k(R) - f_k(P))$$
$$+ f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M_{kj}\omega_j - \int_P^Q f_i(R)(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R)).$$

Then

$$\begin{pmatrix} \int_P^Q \omega_0\omega_0 \\ \int_P^Q \omega_0\omega_1 \\ \vdots \\ \int_P^Q \omega_{2g-1}\omega_{2g-1} \end{pmatrix} = (I_{4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} c_{00} \\ \vdots \\ c_{2g-1,2g-1} \end{pmatrix}.$$

What else can Coleman integrals do?

- Kim's nonabelian Chabauty method: extend Chabauty–Coleman to higher rank curves 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

What else can Coleman integrals do?

- Kim's nonabelian Chabauty method: extend Chabauty–Coleman to higher rank curves 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

I'd love to discuss further applications!