Computing Coleman integrals II.

Jan Tuitman

KU Leuven

June 29, 2017

Coleman integrals

Let:

- X a smooth projective curve over $\mathbf{Q}$ with good reduction at p
- points $P_1, P_2 \in X(\mathbf{Q}_p)$
- ω meromorphic 1-form on $X \otimes \mathbf{Q}_p$

Coleman defined a path independent line integral

$$\int_{P_1}^{P_2} \omega$$

which extends to integrals over $D \in J(\mathbf{Q}_p)$, where J denotes the Jacobian of X (above $D = P_2 - P_1$).

He used this integration theory to reformulate the *Chabauty method* for finding rational points on (some) algebraic curves over $\mathbf{Q}$.

Coleman defined his integrals using *p-adic cohomology*.

p-adic cohomology

For a curve X over $\mathbf{Z}_p$ one can define *rigid cohomology spaces* $H^i_{\text{rig}}(X)$ with $i = 0, 1, 2$ which are vector spaces over $\mathbb{Q}_p$ that are functorial in (so only depend on) $\overline{X} = X \otimes \mathbf{F}_p$. Note that in particular the p-th power Frobenius map Φ of $\overline{X}$ acts on the $H^i_{\text{rig}}(X)$.

These p-adic cohomology spaces have similar properties as

- ℓ-adic (étale) cohomology (for $\ell \neq p$)
- crystalline cohomology

but are easier to define and compute.

By the *Lefschetz formula* for rigid cohomology we have that

$$Z(\overline{X}, T) := \exp\left(\sum_{i=1}^{\infty} |\overline{X}(\mathbf{F}_{p^i})| \frac{T^i}{i}\right) = \frac{\det(1 - \Phi\, T | H^1_{\text{rig}}(X))}{(1-T)(1-pT)}$$

So the *zeta-function* $Z(\overline{X}, T)$ can be computed from $H^1_{\text{rig}}(X)$ as well.

Computing p-adic cohomology

For hyperelliptic curves, $H^1_{\mathrm{rig}}(X)$ with the action of Frobenius can be computed using Kedlaya's algorithm (2001).

Extensions of Kedlaya's algorithm were developed, but

- they either still only applied to very special curves (Gaudry-Gurel for superelliptic curves, for example),
- or they were not practical and therefore not implemented (notably: Castryck-Denef-Vercauteren for nondegenerate curves).

In 2014, I proposed an algorithm to compute $H^1_{\mathrm{rig}}(X)$ with the action of Frobenius that is as practical as Kedlaya's algorithm but applies to much more general curves (essentially all curves, it turns out).

The main idea is to 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.

Setup

We will now describe what we need to know about p-adic cohomology keeping everything as explicit as possible.

Let X be a nonsingular projective curve over $\mathbf{Q}$ given by a (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 the degrees of Q in x, y.

$\Delta(x) \in \mathbf{Z}[x]$ the discriminant of $Q(x, y)$ w.r.t. y.

$r(x) \in \mathbf{Z}[x]$ squarefree with the same roots as $\Delta(x)$.

Note that if $r(x_0) = 0$ then one of the following two holds:

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

Integral bases

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

Definition

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

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

then $[b_0^0, \ldots, b_{d_y-1}^0]$ *is an integral basis for* $\mathbf{Q}(X)$ *over* $\mathbf{Q}[x]$.

Similary, we let $W^\infty \in Gl_{d_y}(\mathbf{Q}[x, 1/x, 1/r])$ *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 in that case.*

Good reduction at p

We need to impose some conditions on the prime p:

Definition

We say that the triple (Q, W^0, W^∞) has good reduction at a prime number p, if the following conditions hold:

- *the curve X has good reduction at p,*
- *the divisors defined by $r(x)$ on X and on $\mathbf{P}^1$ have good reduction at p, i.e. the points in their support all have different reductions modulo p.*
- $W^0 \in Gl_{d_y}(\mathbf{Z}_p[x, 1/r])$,
- $W^\infty \in Gl_{d_y}(\mathbf{Z}_p[x, 1/x, 1/r])$,

Remark

(Q, W^0, W^∞) has good reduction at all but a finite number of primes p and for Chabauty one can vary p. However, for computing zeta functions p is fixed and it can in general be hard to find a lift that has good reduction in the above sense.

Overconvergent rings

From now on we assume that (Q, W^0, W^∞) has good reduction at p.

Let:

- V 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 write

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

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

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

Lifting Frobenius

The p-the power Frobenius map Φ in characteristic p can be lifted to the rings $S^\dagger = \mathbf{Q}_p\langle x, 1/r\rangle^\dagger$ and $R^\dagger = \mathbf{Q}_p\langle x, 1/r, y\rangle^\dagger/(Q)$ in the following way:

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

Remark

In practice it is important that $\Phi(x) = x^p$. For a Frobenius lift of this form to exist, need that $\frac{dQ}{dy} \neq 0 \bmod p$. Therefore, we have removed the zeros of $r(x)$ from the curve.

p-adic cohomology

Definition

The p-adic cohomology of U is the cohomology of the overconvergent de Rham complex $\Omega^\bullet_{R^\dagger}$. More precisely, we have $\Omega^1_{R^\dagger} = \frac{R^\dagger dx \oplus R^\dagger dy}{dQ}$ and

$$H^0_{rig}(U) = \ker(d : R^\dagger \to \Omega^1_{R^\dagger}),$$
$$H^1_{rig}(U) = \operatorname{coker}(d : R^\dagger \to \Omega^1_{R^\dagger}).$$

Remark

We can define and compute $H^1_{rig}(X) \subset H^1_{rig}(U)$ as the kernel of a residue map.

Reducing in cohomology

Proposition

For all $\ell \in \mathbf{N}$ *and every vector* $w \in \mathbf{Q}_p[x]^{\oplus d_y}$, *there exist vectors* $u, v \in \mathbf{Q}_p[x]^{\oplus d_y}$ *with* $\deg(v) < \deg(r)$, *such that*

$$\frac{\sum_{i=0}^{d_y-1} w_i b_i^0}{r^\ell} \frac{dx}{r} = d\left(\frac{\sum_{i=0}^{d_y-1} v_i b_i^0}{r^\ell}\right) + \frac{\sum_{i=0}^{d_y-1} u_i b_i^0}{r^{\ell-1}} \frac{dx}{r}.$$

Idea of proof.

To lowest order in r, the vector v has to satisfy the $d_y \times d_y$ linear system

$$\left(\frac{rG^0}{r'} - \ell I\right) v \equiv \frac{w}{r'} \pmod{r}$$

over $\mathbf{Q}_p[x]/(r)$ for some matrix $G^0 \in M_{d_y \times d_y}(\mathbf{Q}_p[x])$ such that the eigenvalues of $\frac{rG^0}{r'}$ are contained in $\mathbf{Q} \cap [0,1) \cap \mathbf{Z}_p$ at every zero of $r(x)$. Therefore, as long as $\ell \geq 1$ we can solve the system and reduce the pole order at the zeros of $r(x)$. □

Computing the cohomology

In these reductions we have used that $[b_0^0, \ldots, b_{d_y-1}^0]$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[x]$, otherwise G^0 would not consist of polynomials.

By applying repeatedly, we can can represent the cohomology class of any 1-form on U by one that is logarithmic at all $P \in X \setminus U$ for which $x(P) \neq \infty$.

We can do something similar at the points P with $x(P) = \infty$ by working with the integral basis $[b_0^\infty, \ldots, b_{d_y-1}^\infty]$ of $\mathbf{Q}(X)$ over $\mathbf{Q}[1/x]$.

Finding a basis for $H^1_{\mathrm{rig}}(X)$ is now reduced to finite dimensional linear algebra.

We find 1-forms $\omega_1, \ldots, \omega_{2g}$ on U that are a basis for $H^1_{\mathrm{rig}}(X)$.

Computing matrix of Frobenius

By applying Φ and using the cohomological reductions, we find a matrix $M \in M_{2g \times 2g}(\mathbf{Q}_p)$ and functions $f_1, \ldots, f_{2g} \in R^\dagger$ such that:

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

for $i = 1, \ldots, 2g$.

M is the *matrix of Frobenius* on $H^1_{\text{rig}}(X)$ w.r.t. the basis $[\omega_1, \ldots, \omega_{2g}]$.

Applications

- To determine the zeta function $Z(\overline{X}, T)$ of $\overline{X}$ we forget about $f_1, \ldots, f_{2g}$ and compute the reverse characteristic polynomial of the matrix M. Also works over $\mathbf{F}_q$ with $q = p^n$.

  In joint work with W. Castryck, we construct X from $\overline{X}$ for (almost) all curves of genus at most 5. Lifting $\overline{X}$ is easy in many other cases.

  This is all **completely implemented**, can be found on my website and will come with the next release of Magma.

- To compute the Coleman integrals $\int_P^Q \omega_j$, we solve the linear system

$$\int_P^Q \omega_i = f_i(Q) - f_i(P) + \sum_{j=1}^{2g} M_{ij} \int_P^Q \omega_j \qquad \text{for } 1 \leq i \leq 2g$$

  by inverting $M - I$. Together with J. Balakrishnan we are working on a paper and Magma package that implement this idea for all points on all curves, both single and double integrals (**soon to be released**).

Example: $X = X_{ns}^{+}(13)$

'The cursed modular curve'.

Smooth plane quartic:

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

By computing a lot of Coleman integrals (both single and double) on X, we have managed to work out non-Abelian Chabauty on this curve and have shown that it has no rational points apart from the known ones.

Theorem (J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, J. Vonk)

We have $|X_{ns}^{+}(13)| = 7$.

We are currently writing this up.

While this curve is very interesting, from the point of view of this talk it is just a smooth plane quartic. What about Coleman integrals on more general curves?

$X = X_0(44)$

This curve has genus 4. The plane model given by

$$Q(x,y) = y^5 + 12x^2y^3 - 14x^2y^2 + (13x^4 + 6x^2)y - (11x^6 + 6x^4 + x^2)$$

has a singularity at $(0,0)$. We have:

$$r = x(x^4 + 6x^2 + 1)(45753125x^8 + 8440476x^6 + 1340814x^4 + 69756x^2 + 3125)$$

$$b^0 = \left[1, y, y^2, \frac{y^3}{x}, \frac{-10x^4 - (6x^4 - 13x^2)y + (x^4 + 12x^2)y^2 - x^2y^3 + 1}{x^5 + 6x^3 + x}\right]$$

(Q, W^0, W^∞) has good reduction at $p = 7$. Let:

- P_1 be the point $(x,y) = (1,1)$
- P_2 be the point where $x = 0$ and $b^0 = [1,0,0,0,0]$.

Our algorithm finds that $\int_{P_1}^{P_2} \omega = 0$ for all holomorphic differentials ω on X. This suggests that $P_1 - P_2$ is torsion on the Jacobian of X. Indeed, it turns out that $15(P_1 - P_2) = O$.