Coleman integration for general curves

Jan Tuitman

KU Leuven

October 17, 2016

Joint work with Jennifer Balakrishnan (Boston University)

Coleman integration

Suppose given

- $X/\mathbf{Z}_p$ a smooth proper curve,
- $P, Q \in X(\mathbf{Q}_p)$,
- $\omega \in \Omega^1(X)$.

Coleman integration

Suppose given

- $X/\mathbf{Z}_p$ a smooth proper curve,
- $P, Q \in X(\mathbf{Q}_p)$,
- $\omega \in \Omega^1(X)$.

Coleman defined a path independent line integral

$$\int_P^Q \omega.$$

Coleman integration

Suppose given

- $X/\mathbf{Z}_p$ a smooth proper curve,
- $P, Q \in X(\mathbf{Q}_p)$,
- $\omega \in \Omega^1(X)$.

Coleman defined a path independent line integral

$$\int_P^Q \omega.$$

Actually, we can

- replace $\mathbf{Q}_p$ and $\mathbf{Z}_p$ by $\mathbf{C}_p$ and its valuation ring,
- take $\omega \in \Omega^1(U)$ for some (wide) open $U \subset X^{(an)}$,
- extend to integrate over $D \in J(\mathbf{Q}_p)$ where J is the Jacobian of X (above: $D = Q - P$).

Coleman integration

The Coleman integral satisfies (and is characterised by) the following properties;

Theorem

1. *Linearity:* $\int_P^Q \alpha\omega_1 + \beta\omega_2 = \alpha \int_P^Q \omega_1 + \beta \int_P^Q \omega_2$.
2. *Additivity:* $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
3. *Change of variables:* $\int_P^Q f^*\omega = \int_{f(P)}^{f(Q)} \omega$.
4. *Fundamental theorem of calculus:* $\int_P^Q df = f(Q) - f(P)$.

Locally (on disks of radius less than 1) you can define the integral as in complex analysis. However, because the p-adic topology is totally disconnected, there is no notion of analytic continuation to fix the integration constants.

Coleman's key idea is to replace analytic continuation by equivariance with respect to the Frobenius map F_p to move between different disks.

Chabauty method

This notion of integral is particulary interesting since Coleman used it to reformulate the Chabauty method:

Chabauty method

This notion of integral is particulary interesting since Coleman used it to reformulate the Chabauty method:

Theorem

Let $\mathcal{X}$ be a curve of genus $g \geq 2$ over $\mathbf{Q}$, J the Jacobian of $\mathcal{X}$, p a prime of good reduction and $X = \mathcal{X} \otimes \mathbf{Q}_p$. Moreover, let r be the Mordell-Weil rank of $\mathcal{X}$ and suppose that $r < g$. Then there exists $\omega \in \Omega^1(X)$ such that $\int_P^Q \omega = 0$ for all P, Q in $\mathcal{X}(\mathbf{Q})$.

Chabauty method

This notion of integral is particulary interesting since Coleman used it to reformulate the Chabauty method:

Theorem

Let $\mathcal{X}$ be a curve of genus $g \geq 2$ over $\mathbf{Q}$, J the Jacobian of $\mathcal{X}$, p a prime of good reduction and $X = \mathcal{X} \otimes \mathbf{Q}_p$. Moreover, let r be the Mordell-Weil rank of $\mathcal{X}$ and suppose that $r < g$. Then there exists $\omega \in \Omega^1(X)$ such that $\int_P^Q \omega = 0$ for all P, Q in $\mathcal{X}(\mathbf{Q})$.

So by computing Coleman integrals, we might sometimes be able to find rational points, or prove that we have found all of them.

Remark

The nonabelian Chabauty program by Kim tries to get rid of the assumption $r < g$. Note that this still involves (iterated) Coleman integrals!

Hyperelliptic curves

Let X be a hyperelliptic curve of genus g given by

$$y^2 = f(x)$$

with $f(x) \in \mathbf{Z}_p[x]$ monic of degree $2g+1$ separable mod p.

Hyperelliptic curves

Let X be a hyperelliptic curve of genus g given by

$$y^2 = f(x)$$

with $f(x) \in \mathbf{Z}_p[x]$ monic of degree $2g+1$ separable mod p.

Balakrishnan, Bradshaw and Kedlaya gave an algorithm (implemented in SAGE) to compute Coleman integrals in this case.

The method is based on Kedlaya's algorithm for computing zeta functions of hyperelliptic curves over finite fields.

Has been succesfully used for doing new cases of effective Chabauty by Balakrishnan and various co-authors.

General curves

What about more general curves?

Until recently: Main obstruction to compute Coleman integrals for general curves was lack of a Kedlaya type algorithm to compute p-adic cohomology of the curve.

General curves

What about more general curves?

Until recently: Main obstruction to compute Coleman integrals for general curves was lack of a Kedlaya type algorithm to compute p-adic cohomology of the curve.

However, recently I have developed and implemented a practical extension of Kedlaya's algorithm to (almost) all curves.

Magma packages pcc_p and pcc_q can be found at

`https://perswww.kuleuven.be/jan_tuitman/`

It is therefore natural to ask if this algorithm can also be used to compute Coleman integrals on (more) general curves.

General curves

What about more general curves?

Until recently: Main obstruction to compute Coleman integrals for general curves was lack of a Kedlaya type algorithm to compute p-adic cohomology of the curve.

However, recently I have developed and implemented a practical extension of Kedlaya's algorithm to (almost) all curves.

Magma packages pcc_p and pcc_q can be found at

`https://perswww.kuleuven.be/jan_tuitman/`

It is therefore natural to ask if this algorithm can also be used to compute Coleman integrals on (more) general curves.

The answer is yes!

p-adic cohomology

To compute Coleman integrals, we will be using p-adic (also called rigid) cohomology.

For a curve $X/\mathbf{Z}_p$ one can define finite dimensional $\mathbf{Q}_p$ vector spaces $H^i_{\mathrm{rig}}(X)$ (for $i = 0, 1, 2$) that are functorial in (so only depend on) the special fibre $\overline{X} = X \otimes \mathbf{F}_p$. Note that in particular the p-th power Frobenius map on $\overline{X}$ acts on the $H^i_{\mathrm{rig}}(X)$.

These p-adic cohomology spaces have similar properties as:

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

but are much easier to define and compute.

We will now give a rather computational introduction to this theory, keeping everything as explicit as possible, since that is essential for our algorithm.

Setup

Let $\mathcal{X}$ be a nonsingular projective curve of genus g over $\mathbf{Q}$ given by a (possibly singular) plane model $\mathcal{Q}(x, y) = 0$ with $\mathcal{Q}(x, y) \in \mathbf{Z}[x, y]$ irreducible and monic in the variable y.

d_x, d_y the degrees of $\mathcal{Q}$ in x, y.

Setup

Let $\mathcal{X}$ be a nonsingular projective curve of genus g over $\mathbf{Q}$ given by a (possibly singular) plane model $\mathcal{Q}(x, y) = 0$ with $\mathcal{Q}(x, y) \in \mathbf{Z}[x, y]$ irreducible and monic in the variable y.

d_x, d_y the degrees of $\mathcal{Q}$ in x, y.

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

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

Setup

Let $\mathcal{X}$ be a nonsingular projective curve of genus g over $\mathbf{Q}$ given by a (possibly singular) plane model $\mathcal{Q}(x, y) = 0$ with $\mathcal{Q}(x, y) \in \mathbf{Z}[x, y]$ irreducible and monic in the variable y.

d_x, d_y the degrees of $\mathcal{Q}$ in x, y.

$\Delta(x) \in \mathbf{Z}[x]$ the discriminant of $\mathcal{Q}(x, y)$ 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 $\mathcal{Q}(x, y)$ has a singularity lying over x_0,
- the map $x : \mathcal{X} \to \mathbf{P}^1$ has a ramification point lying over x_0.

Integral basis

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

Definition

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

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

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

Integral basis

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

Definition

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

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

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

Example

When the plane model $\mathcal{Q}(x, y) = 0$ *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:

Good reduction at p

We need to impose some conditions on the prime p:

Definition

We say that the triple $(\mathcal{Q}, W^0, W^\infty)$ has good reduction at a prime number p, if the following conditions hold:

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

Good reduction at p

We need to impose some conditions on the prime p:

Definition

We say that the triple $(\mathcal{Q}, W^0, W^\infty)$ has good reduction at a prime number p, if the following conditions hold:

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

Remark

$(\mathcal{Q}, W^0, W^\infty)$ 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 $(\mathcal{Q}, W^0, W^\infty)$ has good reduction at p and denote $X = \mathcal{X} \otimes \mathbf{Z}_p$.

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,
- $\overline{X}, \overline{U}$ and $\overline{V}$ the reductions modulo p of X, U and V,respectively.

Overconvergent rings

From now on we assume that $(\mathcal{Q}, W^0, W^\infty)$ has good reduction at p and denote $X = \mathcal{X} \otimes \mathbf{Z}_p$.

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,
- $\overline{X}, \overline{U}$ and $\overline{V}$ the reductions modulo p of X, U and V,respectively.

We write

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

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

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

Lifting Frobenius

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

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

Remark

In practice it is important that $\mathrm{F}_p(x) = x^p$. However, for a Frobenius lift of this form to exist, we need to remove the zeros of $r(x)$ from the curve.

p-adic cohomology

Definition

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

$$\begin{aligned} H^0_{rig}(\overline{U}) &= \quad \ker(d : R^\dagger \to \Omega^1_{R^\dagger}), \\ H^1_{rig}(\overline{U}) &= \mathrm{coker}(d : R^\dagger \to \Omega^1_{R^\dagger}). \end{aligned}$$

p-adic cohomology

Definition

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

$$\begin{aligned} H^0_{rig}(\overline{U}) &= \quad \ker(d : R^\dagger \to \Omega^1_{R^\dagger}), \\ H^1_{rig}(\overline{U}) &= \mathrm{coker}(d : R^\dagger \to \Omega^1_{R^\dagger}). \end{aligned}$$

Theorem

By the assumption on good reduction, there is a comparison theorem with algebraic De Rham cohomology:

$$H^i_{rig}(\overline{U}) \cong H^i_{dR}(U \otimes \mathbf{Q}_p) \text{ for } i = 0, 1$$

p-adic cohomology

Definition

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

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

Theorem

By the assumption on good reduction, there is a comparison theorem with algebraic De Rham cohomology:

$$H^i_{rig}(\overline{U}) \cong H^i_{dR}(U \otimes \mathbf{Q}_p) \text{ for } i = 0, 1$$

Remark

We can define $H^1_{rig}(\overline{X}) \subset H^1_{rig}(\overline{U})$ 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

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

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 $[b^0_0, \ldots, b^0_{d_y-1}]$ 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 $x(P) \neq \infty$.

Computing the cohomology

In these reductions we have used that $[b^0_0, \ldots, b^0_{d_y-1}]$ 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 $[b^\infty_0, \ldots, b^\infty_{d_y-1}]$ of $\mathbf{Q}(X)$ over $\mathbf{Q}[1/x]$.

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

We find 1-forms $\omega_1, \ldots, \omega_\kappa$ in $\Omega^1(U)$ that are a basis for $H^1_{\mathrm{rig}}(\overline{U})$ such that the first $2g$ are a basis for $H^1_{\mathrm{rig}}(\overline{X})$.

Computing matrix of Frobenius

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

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_j \Phi_{ij}\omega_j$$

for $i = 1, \ldots, \kappa$.

Computing matrix of Frobenius

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

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_j \Phi_{ij} \omega_j$$

for $i = 1, \ldots, \kappa$.

Φ is the matrix of Frobenius on $H^1_{\mathrm{rig}}(\overline{U})$ w.r.t. the basis $[\omega_1, \ldots, \omega_\kappa]$.

Before we did not care about $f_1, \ldots, f_\kappa$ and computed the zeta function of $\overline{X}$ as the reverse characteristic polynomial of the matrix Φ.

Now we are going to compute Coleman integrals on X using Φ and $f_1, \ldots, f_\kappa$.

Residue disks

There is a specialisation map from the analytic space X^{an} over $\mathbf{Q}_p$ to $\overline{X}$ that should be seen as reduction mod p.

The inverse image of a point on $\overline{X}$ under this map is called a residue disk and is isomorphic to the open unit disk $|z| < 1$.

Residue disks

There is a specialisation map from the analytic space X^{an} over $\mathbf{Q}_p$ to $\overline{X}$ that should be seen as reduction mod p.

The inverse image of a point on $\overline{X}$ under this map is called a residue disk and is isomorphic to the open unit disk $|z| < 1$.

We call a residue disk bad if it contains a point of $X \setminus U$ and good if not.

Similarly, we say that a bad residue disk is infinite if it contains a point P with $x(P) = \infty$ and finite if not.

Tiny integrals

Suppose that $P, Q \in X(\mathbf{Q}_p)$ are points in the same residue disk D and $\omega \in \Omega^1(U)$.

For simplicity, assume that ω does not have a pole on D, for example because D is a good disk.

Tiny integrals

Suppose that $P, Q \in X(\mathbf{Q}_p)$ are points in the same residue disk D and $\omega \in \Omega^1(U)$.

For simplicity, assume that ω does not have a pole on D, for example because D is a good disk.

Then $\int_P^Q \omega$ can be computed simply by expanding ω in terms of a local coordinate t on the disk:

$$\omega = \sum_{i \geq 0} c_i t^i dt$$

and integrating as usual

$$\int_{t(P)}^{t(Q)} \sum_{i \geq 0} c_i t^i dt = \sum_{i \geq 0} \frac{c_i}{i+1} (t(Q)^{i+1} - t(P)^{i+1}).$$

This is the easy case, no p-adic cohomology is needed.

Tiny integrals: precision

Proposition

Suppose that P, Q and ω are accurate to p-adic precision N. If we assume that $\omega \in \mathbf{Z}_p[[t]]$ and truncate it modulo t^m, then the tiny integral as computed above is accurate to p-adic precision

$$\min\{N, m+1-\lfloor \log_p(m+1) \rfloor\}.$$

Tiny integrals: precision

Proposition

Suppose that P, Q and ω are accurate to p-adic precision N. If we assume that $\omega \in \mathbf{Z}_p[[t]]$ and truncate it modulo t^m, then the tiny integral as computed above is accurate to p-adic precision

$$\min\{N, m + 1 - \lfloor \log_p(m + 1) \rfloor\}.$$

Proof.

Let us denote the i-th term by $T_i = \frac{c_i}{i+1}(t(Q)^{i+1} - t(P)^{i+1})$. The effect of the truncation is to omit the T_i for $i \geq m$. However, $\mathrm{ord}_p(t(Q)), \mathrm{ord}_p(t(P) \geq 1$, so for $i \geq m$ we have

$$\mathrm{ord}_p(T_i) \geq i + 1 - \lfloor \log_p(i + 1) \rfloor \geq m + 1 - \lfloor \log_p(m + 1) \rfloor.$$

Since $t(P), t(Q)$ are accurate to p-adic precision N, for $i < m$ we have that T_i is accurate to precision

$$N + i - \lfloor \log_p(i + 1) \rfloor \geq N. \qquad \square$$

Good endpoints

Now suppose that $P, Q \in X(\mathbf{Q}_p)$ are points in different good residue disks.

We may assume that P, Q are Teichmueller points (fixed under F_p), because the integral from a point to the corresponding Teichmueller point is tiny!

Good endpoints

Now suppose that $P, Q \in X(\mathbf{Q}_p)$ are points in different good residue disks.

We may assume that P, Q are Teichmueller points (fixed under F_p), because the integral from a point to the corresponding Teichmueller point is tiny!

Recall that for $i = 1, \ldots, \kappa$

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_j \Phi_{ij}\omega_j.$$

Good endpoints

Now suppose that $P, Q \in X(\mathbf{Q}_p)$ are points in different good residue disks.

We may assume that P, Q are Teichmueller points (fixed under F_p), because the integral from a point to the corresponding Teichmueller point is tiny!

Recall that for $i = 1, \ldots, \kappa$

$$\mathrm{F}_p^*(\omega_i) = df_i + \sum_j \Phi_{ij}\omega_j.$$

Integrating, we find

$$\int_P^Q \omega_i = \int_{\mathrm{F}_p(P)}^{\mathrm{F}_p(Q)} \omega_i = \int_P^Q \mathrm{F}_p^*(\omega_i) = f_i(Q) - f_i(P) + \sum_j \Phi_{ij} \int_P^Q \omega_j.$$

So we can find the $\int_P^Q \omega_i$ by solving the linear system

$$(\Phi - I) \int_P^Q \omega_i = f_i(P) - f_i(Q).$$

Good endpoints: precision

Proposition

Suppose that $P, Q \in X(\mathbf{Q}_p)$ *are points lying in good disks, accurate to* N *digits of precision, and suppose that the matrix* Φ *and the functions* f_i *are accurate to* N *digits of precision as well. Then the computed values of* $\int_P^Q \omega_i$ *will be accurate to* $N - \mathrm{ord}_p(\det(\Phi - I))$ *digits of precision.*

Good endpoints: precision

Proposition

Suppose that $P, Q \in X(\mathbf{Q}_p)$ are points lying in good disks, accurate to N digits of precision, and suppose that the matrix Φ and the functions f_i are accurate to N digits of precision as well. Then the computed values of $\int_P^Q \omega_i$ will be accurate to $N - \mathrm{ord}_p(\det(\Phi - I))$ digits of precision.

Proof.

The evaluation of the f_i at P, Q does not suffer from precision loss, since P, Q lie in good disks! The matrix inversion loses at most $\mathrm{ord}_p(\det(\Phi - I))$ digits of precision. □

Good endpoints: precision

Proposition

Suppose that $P, Q \in X(\mathbf{Q}_p)$ are points lying in good disks, accurate to N digits of precision, and suppose that the matrix Φ and the functions f_i are accurate to N digits of precision as well. Then the computed values of $\int_P^Q \omega_i$ will be accurate to $N - \mathrm{ord}_p(\det(\Phi - I))$ digits of precision.

Proof.

The evaluation of the f_i at P, Q does not suffer from precision loss, since P, Q lie in good disks! The matrix inversion loses at most $\mathrm{ord}_p(\det(\Phi - I))$ digits of precision. □

Remark

Note that we can integrate any $\omega \in \Omega^1(U)$ using

$$\int_P^Q \omega = \int_P^Q (df + \sum_i c_i \omega_i) = f(Q) - f(P) + \sum_i c_i \int_P^Q \omega_i .$$

Bad endpoints

Suppose that $P \in X(\mathbf{Q}_p)$ lies in a good disk, but $Q \in X(\mathbf{Q}_p)$ lies in a finite bad disk D (the case of an infinite bad disk is easier).

Bad endpoints

Suppose that $P \in X(\mathbf{Q}_p)$ lies in a good disk, but $Q \in X(\mathbf{Q}_p)$ lies in a finite bad disk D (the case of an infinite bad disk is easier).

Now the problem is that the f_i will in general have a pole in D, so that $f_i(Q)$ does not necessarily converge!

Bad endpoints

Suppose that $P \in X(\mathbf{Q}_p)$ lies in a good disk, but $Q \in X(\mathbf{Q}_p)$ lies in a finite bad disk D (the case of an infinite bad disk is easier).

Now the problem is that the f_i will in general have a pole in D, so that $f_i(Q)$ does not necessarily converge!

However, the f_i will converge close enough to ∂D. Therefore, we compute $\int_P^{Q'} \omega_i$ for some Q' close enough to ∂D. Note that $\int_Q^{Q'} \omega_i$ is a tiny integral!

Bad endpoints

Suppose that $P \in X(\mathbf{Q}_p)$ lies in a good disk, but $Q \in X(\mathbf{Q}_p)$ lies in a finite bad disk D (the case of an infinite bad disk is easier).

Now the problem is that the f_i will in general have a pole in D, so that $f_i(Q)$ does not necessarily converge!

However, the f_i will converge close enough to ∂D. Therefore, we compute $\int_P^{Q'} \omega_i$ for some Q' close enough to ∂D. Note that $\int_Q^{Q'} \omega_i$ is a tiny integral!

How close is close enough?

Bad endpoints: convergence

Proposition

On a finite bad disk, the functions f_i converge outside of the closed disk defined by $\mathrm{ord}_p(r(x)) \geq 1/p$.

Bad endpoints: convergence

Proposition

On a finite bad disk, the functions f_i converge outside of the closed disk defined by $\mathrm{ord}_p(r(x)) \geq 1/p$.

Proof.

The part of f_i coming from finite reductions is of the form

$$\sum_{j=0}^{d_y-1} \sum_{k=1}^{\infty} \frac{c_{ijk}(x)}{r(x)^k} b_0^j,$$

with the c_{ijk} elements of $\mathbf{Q}_p[x]$ of degree smaller than $\deg(r)$, that satisfy

$$\mathrm{ord}_p(c_{ijk}) \geq \lfloor k/p \rfloor + 1 - \lfloor \log_p(ke_0) \rfloor$$

where $e_0 = \max\{e_P \colon P \text{ bad finite point}\}$ and e_P denotes the ramification index of x at P. It is therefore clear that the series converges if $\mathrm{ord}_P(r(x)) < 1/p$. □

Bad endpoints: precision

Proposition

Suppose that $P \in X(\mathbf{Q}_p)$ is a point lying in a good disk, and $Q \in X(\mathbf{Q}_p(p^{1/m}))$ for some a point lying in a finite bad disk, both accurate to N digits of precision. Assume that Φ and the functions f_i are accurate to N digits of precision as well. Denote $\epsilon = \mathrm{ord}_p(r(Q))$ and suppose that $\epsilon < 1/p$. Define a function π on positive integers by

$$\pi(k) = \max\{N, \lfloor k/p \rfloor + 1 - \lfloor \log_p(ke_0) \rfloor\},$$

where $e_0 = \max\{e_P : P \text{ finite bad point }\}$ and e_P denotes the ramification index of x at P. (Note that $\pi(k) - \epsilon k \to \infty$ as $k \to \infty$). Then the computed values of $\int_P^Q \omega_i$ will be accurate to

$$\min_{k \in \mathbf{Z}_{>0}} \{\pi(k) - k\epsilon\} - \mathrm{ord}_p(\det(\Phi - I)).$$

digits of precision.

Implementation

Work on an implementation in Magma is in progress. This also includes double integrals, which we have not talked about today.

Implementation

Work on an implementation in Magma is in progress. This also includes double integrals, which we have not talked about today.

For now we have restricted to curves with a smooth affine model, for which $W^0 = I$. However, soon it should be working in the general case.

Implementation

Work on an implementation in Magma is in progress. This also includes double integrals, which we have not talked about today.

For now we have restricted to curves with a smooth affine model, for which $W^0 = I$. However, soon it should be working in the general case.

Most examples we have tried so far are smooth quartics.

Implementation

Work on an implementation in Magma is in progress. This also includes double integrals, which we have not talked about today.

For now we have restricted to curves with a smooth affine model, for which $W^0 = I$. However, soon it should be working in the general case.

Most examples we have tried so far are smooth quartics.

Soon there should be a preprint online with more general examples.

Implementation

Work on an implementation in Magma is in progress. This also includes double integrals, which we have not talked about today.

For now we have restricted to curves with a smooth affine model, for which $W^0 = I$. However, soon it should be working in the general case.

Most examples we have tried so far are smooth quartics.

Soon there should be a preprint online with more general examples.

We plan on making the code available, once there is a stable version.

Bruin Poonen Stoll

Bruin, Poonen and Stoll (2013) give the example

$$\mathcal{Q} = y^3 + (-x^2 - 1)y^2 - x^3 y + x^3 + 2x^2 + x$$

which has small coefficients and rank 1 (under GRH).

There are 5 finite points

$P_1 = (0,0)$, $P_2 = (0,1)$, $P_3 = (-3,4)$, $P_4 = (-1,0)$, $P_5 = (-1,1)$

and 3 more at infinity.

Some integrals

We computed the integrals at $p = 3$ of $\omega_1, \ldots, \omega_6$ between P_1 and P_2, P_3, P_4:

$$\left(\int_{P_1}^{P_2} \omega_i\right)_{i=1,\ldots,6} = (-808a^{60} + O(a^{280}), 347a^{90} + O(a^{280}), -1646a^{60} + O(a^{280}),$$
$$3667a^{30} + O(a^{280}), 3172a^{30} + O(a^{280}), -5164a^{30} + O(a^{280}))$$

$$\left(\int_{P_1}^{P_3} \omega_i\right)_{i=1,\ldots,6} = (1690a^{60} + O(a^{280}), 319a^{90} + O(a^{280}), -1072a^{60} + O(a^{280}),$$
$$7474a^{30} + O(a^{280}), 3022a^{30} + O(a^{280}), 3509a^{30} + O(a^{280}))$$

$$\left(\int_{P_1}^{P_4} \omega_i\right)_{i=1,\ldots,6} = (-55a^{90} + O(a^{280}), -349a^{120} + O(a^{280}), 229a^{90} + O(a^{280}),$$
$$-4918a^{30} + O(a^{280}), 565a^{90} + O(a^{280}), 8507a^{30} + O(a^{280}))$$

where $a^{30} = 3$ (a is needed for things to converge in the bad disks).

Chabauty

We now compute independent linear combinations ξ_1, ξ_2 of $\omega_1, \omega_2, \omega_3$ such that

$$\int_{P_1}^{P_2} \xi_i = \int_{P_1}^{P_3} \xi_i = \int_{P_1}^{P_4} \xi_i = 0 \qquad \text{for } i = 1, 2$$

and find

$$\xi_1 = (1 + O(3^8))\omega_1 + O(3^{10})\omega_2 + (430 + O(3^8))\omega_3$$
$$\xi_2 = O(3^8)\omega_1 + (1 + O(3^{10}))\omega_2 + (-320 \cdot 3 + O(3^8))\omega_3.$$

No we check that

$$\int_{P_1}^{P_5} \xi_1 = \int_{P_1}^{P_5} \xi_2 = 0.$$

So we must be doing something right!