Numerical computation of Coleman integrals

Kiran S. Kedlaya

Department of Mathematics, Massachusetts Institute of Technology

p-adic Methods and Rational Points
Rényi Institute (Budapest), May 20, 2007

Contents

Contents

Overview of Coleman integration

Let C be a smooth proper curve over $\mathbb{Z}_q = W(\mathbb{F}_q)$. Coleman described a canonical integral $\int_P^Q \omega$ whenever ω is a meromorphic 1-form on $C_{\mathbb{Q}_q}$, and $P, Q \in C(\mathbb{Q}_q)$ are points where ω is holomorphic. Properties include:

- 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 C' 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: $\int_P^Q df = f(Q) - f(P)$.

Application: Chabauty-Coleman method

Let C be a smooth curve over $\mathbb{Z}[1/N]$ admitting a compactification $\overline{C}$ which is smooth proper over $\mathbb{Z}[1/N]$, with $\overline{C} - C$ a relative normal crossings divisor. (E.g., a smooth proper curve, or $\mathbb{P}^1 - \{0, 1, \infty\}$.) Assume $p \nmid N$.

The *Chabauty condition* is

$$\operatorname{rank} J(C)(\mathbb{Z}[1/N]) < \dim J(C).$$

When this is satisfied, $J(C)(\mathbb{Z}[1/N])$ lies in a closed analytic subspace of $J(C)^{\mathrm{an}}$, which meets C^{an} in finitely many points. Equivalently, there exists a 1-form ω on $J(C)^{\mathrm{an}}$ with $\int_O^P \omega = 0$ for $P \in J(C)(\mathbb{Z}[1/N])$.

If we can find all points $P \in C^{\mathrm{an}}$ where $\int_O^P \omega = 0$, we *may* be able to determine $C(\mathbb{Z}[1/N])$.

Application: Kim's nonabelian Chabauty method

What if the Chabauty condition fails? Instead of $J(C)$, one can work with a *Selmer variety* corresponding to a unipotent quotient of $\pi_1^{\mathrm{geom}}(C)$. Kim conjectures that a suitable analogue of the Chabauty condition holds for a sufficiently large quotient (true for $\mathbb{P}^1 - \{0, 1, \infty\}$).

If one can describe the Selmer variety, one can proceed as the original Chabauty method, but replacing the Coleman integral by an iterated version. (Cf. talk of Wewers.)

Application: p-adic heights

One can use Coleman integrals to compute p-adic heights on Jacobians of curves over number fields (Coleman-Gross, Besser). These heights appear in analogues of the Birch-Swinnerton-Dyer conjecture for p-adic L-functions (Mazur-Tate-Teitelbaum). (Cf. talk of Besser.)

Contents

The fundamental linear system

Fix an open dense subscheme $\overline{U}$ of $C_{\mathbb{F}_q}$, and let $\phi : V_1 \to V_2$ be a q-power Frobenius lift between two strict neighborhoods of the tube $]\overline{U}[$ of $\overline{U}$ in $C_{\mathbb{Q}_q}$. Let $\omega_1, \dots, \omega_n$ be 1-forms forming a basis for $H^1_{\mathrm{dR}}(V)$ for V a wide open strict neighborhood of $]\overline{U}[$. We can then write

$$\phi^* \omega_i = df_i + \sum_{j=1}^{n} A_{ij} \omega_j$$

for some functions f_i and some $n \times n$ matrix A over $\mathbb{Q}_q$.

Using the fundamental linear system

Say we want to compute $\int_P^Q \omega$, for ω a meromorphic 1-form on $C_{\mathbb{Q}_q}$ and $P, Q \in]\overline{U}[$. We can write

$$\omega = df + c_1\omega_1 + \cdots + c_n\omega_n$$

for some function f and some $c_i \in \mathbb{Q}_q$, so it suffices to compute the $\int_P^Q \omega_i$.

Using the fundamental linear system, we write

$$\int_{\phi(P)}^{\phi(Q)} \omega_i = \int_P^Q \phi^* \omega_i = f_i(Q) - f_i(P) + \sum_{j=1}^n A_{ij} \int_P^Q \omega_j.$$

In other words,

$$\int_P^Q \omega_i = \int_P^{\phi(P)} \omega_i + \int_{\phi(Q)}^Q \omega_i + f_i(Q) - f_i(P) + \sum_{j=1}^n A_{ij} \int_P^Q \omega_j.$$

Using the fundamental linear system (contd.)

The last equation from the previous slide is equivalent to

$$\sum_{j=1}^{n} (A - I)_{ij} \int_P^Q \omega_j = f_i(P) - f_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^{Q} \omega_i.$$

The integrals on the right side are within a single residue disc, where the formal antiderivative of ω_i converges. So we can numerically approximate the right side of the equation.

The matrix $A - I$ is invertible because the eigenvalues of A have $\mathbb{C}$-norm $q^{1/2}$ or q, so we can solve the linear system. (This is almost Coleman's original construction.)

If $q \neq p$, it is easier to write down an analogous semilinear system for a p-power Frobenius lift ϕ_p, then derive the linear system for the appropriate power of ϕ_p.

Teichmüller points

In each residue disc, there is a unique point P with $\phi(P) = P$; this is a *Teichmüller point* for the map ϕ.

When computing Coleman integrals, it may be convenient to first compute the integral between Teichmüller points in the right discs (for which $\int_P^{\phi(P)} \omega_i = 0$) and then correct the endpoints afterward.

Contents

Hyperelliptic curves

Assume $p \neq 2$. Let $C/\mathbb{Z}_q$ be a hyperelliptic curve of genus g with a rational Weierstrass point; we can then write C as

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

for $P(x)$ monic of degree $2g+1$.

We will take our subscheme $\overline{U}$ of $C_{\mathbb{F}_q}$ to be the complement of the Weierstrass points; i.e.,

$$\overline{U} = \operatorname{Spec} \mathbb{F}_q[x,y,z]/(y^2 - \overline{P}(x), yz-1).$$

Cohomology of hyperelliptic curves

The first de Rham cohomology of C minus its Weierstrass point is generated by

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

Moreover, there is a simple procedure to express any 1-form as an exact 1-form plus a linear combination of these, using relations such as:

$$\frac{A(s-2)P'\,dy}{y^s} \equiv \frac{2A'\,dx}{y^{s-2}} \qquad (s \neq 2).$$

This extends to a wide open V in which one removes a closed disc of radius < 1 around each Weierstrass point.

Computing the Frobenius action

We use the Frobenius lift

$$\begin{aligned} x &\mapsto x^q \\ y &\mapsto y^q \left(\frac{P(x^q) - P(x)^q}{P(x)^q} \right)^{1/2} \end{aligned}$$

truncated to some appropriate p-adic precision. Again, if $q \neq p$, it is easier to work with a p-power Frobenius instead.

Contents

An implementation in Magma

The computation of Coleman integrals on hyperelliptic curves, using the above paradigm, was described in the M.Sc. thesis of Igor Gutnik (Ben Gurion, 2005).

Gutnik produced an implementation in `Magma`. To our knowledge, this was an orphan; it has not been tested, optimized, distributed, or used for any application.

In particular, this work was unbeknownst to me when...

An implementation in SAGE

I proposed the numerical calculation of Coleman integrals on hyperelliptic curves first at Banff (2/2007), then at the Arizona Winter School (3/2007).

An implementation for $g = 1, q = p$ was developed in SAGE mostly by Robert Bradshaw, using an implementation of the Frobenius calculation for $g = 1, q = p$ developed at MSRI (6/2006) by Bradshaw, Jennifer Balakrishnan, David Harvey, and Liang Xiao.

With Bradshaw, we extended this to g arbitrary, $q = p$. (Note: ω is only allowed to have poles at Weierstrass points.) This became available in SAGE version 2.5.

A word from our sponsor: About SAGE

SAGE is an *open-source* project organized by William Stein, to develop a high-level system for computational algebra, in the style of Magma but built on the common scripting language Python. Although SAGE is very much a work in progress, it has already acquired some rather sophisticated functionalities. (This is partly achieved by incorporating other open-source packages: GAP, PARI, Singular, etc.)

See

`http://www.sagemath.org/`

for more information.

Demonstration

Let's see a demonstration of the `SAGE` implementation, using the `SAGE` notebook interface.

(Switch now to

`http://localhost:8000`

for the demonstration.)

Contents

Iterated integrals

There is also a good theory of iterated Coleman integrals, e.g.,

$$\int_P^Q \omega_1 \omega_2 = \int_P^Q \omega_1(R) \int_R^Q \omega_2.$$

One can use a similar construction to compute these. But can one avoid having to compute all of the $\leq k$-fold integrals in the process of computing a single one?

More generally, one could start with a crystal on C; the usual Coleman integrals come from the trivial crystal, and iterated Coleman integrals come from unipotent crystals (Besser).

Beyond the hyperelliptic case

It should be possible to use this setup to compute Coleman integrals for any family where one can compute the Frobenius action on rigid cohomology.

For instance, one can do this for *nondegenerate curves* (Castryck-Denef-Vercauteren).

Also, one should allow working over a general finite extension of $\mathbb{Z}_p$.

Beyond good reduction

One can also compute Coleman integrals on curves with semistable reduction (depending on a choice of branch for the p-adic logarithm). This has been done for polylogarithms (Besser-de Jeu).

In the general case, one may need to use an explicit description of the Hyodo-Kato Frobenius and monodromy actions (Coleman-Iovita).

Experiments with Chabauty's method

Let C be a smooth proper curve over $\mathbb{Q}$ with good reduction at p, satisfying the Chabauty condition

$$\operatorname{rank} J(C)(\mathbb{Q}) < g(C)$$

and containing a rational point O.

To high numerical accuracy, we can find a basis $\omega_1, \dots, \omega_r$ of the space of holomorphic 1-forms on $J(C)^{\mathrm{an}}$ vanishing on $J(C)(\mathbb{Q})$, then find the points $P \in C^{\mathrm{an}}(\mathbb{Q}_p)$ where $\int_O^P \omega_i = 0$ for all i. This includes all of $C(\mathbb{Q})$ but might include extra points.

Question: are the extra points algebraic? For instance, do they all lie in the intersection of C with the divisible closure of $J(C)(\mathbb{Q})$?