Computing Coleman integrals on modular curves

Kiran S. Kedlaya
joint work (in progress) with Mingjie Chen and Jun Bo Lau

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

AMS Special Session on Rational Points on Algebraic Varieties:
Theory and Computation, II
Joint Mathematics Meetings, Denver
January 16, 2020

Kedlaya was supported by NSF (grant DMS-1802161) and UC San Diego (Warschawski Professorship).

Coleman's theory of p-adic path integrals

Let X be a curve over $\mathbb{Q}_p$ with good reduction (for simplicity).

Coleman (1985) gave a definition of the path integral $\int_P^Q \omega \in \mathbb{C}_p$ where ω is a holomorphic differential on X and $P, Q \in X(\mathbb{C}_p)$. (More generally, ω need only be defined on a generally on a *wide open subspace* U of the associated rigid analytic space, provided that $P, Q \in U(\mathbb{C}_p)$.)

Among its other uses, Coleman integration plays an important role in effective methods in arithmetic geometry.

- Torsion points (effective Manin-Mumford conjecture).
- Rational points on curves via Chabauty-Coleman method.
- Kim's nonabelian Chabauty method (specialized to quadratic Chabauty).

In this talk, we (mostly) ignore applications and focus on the problem of numerically computing Coleman integrals.

Coleman's theory of p-adic path integrals

Let X be a curve over $\mathbb{Q}_p$ with good reduction (for simplicity).

Coleman (1985) gave a definition of the path integral $\int_P^Q \omega \in \mathbb{C}_p$ where ω is a holomorphic differential on X and $P, Q \in X(\mathbb{C}_p)$. (More generally, ω need only be defined on a generally on a *wide open subspace* U of the associated rigid analytic space, provided that $P, Q \in U(\mathbb{C}_p)$.)

Among its other uses, Coleman integration plays an important role in effective methods in arithmetic geometry.

- Torsion points (effective Manin-Mumford conjecture).
- Rational points on curves via Chabauty-Coleman method.
- Kim's nonabelian Chabauty method (specialized to quadratic Chabauty).

In this talk, we (mostly) ignore applications and focus on the problem of numerically computing Coleman integrals.

Coleman's theory of p-adic path integrals

Let X be a curve over $\mathbb{Q}_p$ with good reduction (for simplicity).

Coleman (1985) gave a definition of the path integral $\int_P^Q \omega \in \mathbb{C}_p$ where ω is a holomorphic differential on X and $P, Q \in X(\mathbb{C}_p)$. (More generally, ω need only be defined on a generally on a *wide open subspace* U of the associated rigid analytic space, provided that $P, Q \in U(\mathbb{C}_p)$.)

Among its other uses, Coleman integration plays an important role in effective methods in arithmetic geometry.

- Torsion points (effective Manin-Mumford conjecture).
- Rational points on curves via Chabauty-Coleman method.
- Kim's nonabelian Chabauty method (specialized to quadratic Chabauty).

In this talk, we (mostly) ignore applications and focus on the problem of numerically computing Coleman integrals.

Coleman's theory of p-adic path integrals

Let X be a curve over $\mathbb{Q}_p$ with good reduction (for simplicity).

Coleman (1985) gave a definition of the path integral $\int_P^Q \omega \in \mathbb{C}_p$ where ω is a holomorphic differential on X and $P, Q \in X(\mathbb{C}_p)$. (More generally, ω need only be defined on a generally on a *wide open subspace* U of the associated rigid analytic space, provided that $P, Q \in U(\mathbb{C}_p)$.)

Among its other uses, Coleman integration plays an important role in effective methods in arithmetic geometry.

- Torsion points (effective Manin-Mumford conjecture).
- Rational points on curves via Chabauty-Coleman method.
- Kim's nonabelian Chabauty method (specialized to quadratic Chabauty).

In this talk, we (mostly) ignore applications and focus on the problem of numerically computing Coleman integrals.

Coleman's theory of p-adic path integrals

Let X be a curve over $\mathbb{Q}_p$ with good reduction (for simplicity).

Coleman (1985) gave a definition of the path integral $\int_P^Q \omega \in \mathbb{C}_p$ where ω is a holomorphic differential on X and $P, Q \in X(\mathbb{C}_p)$. (More generally, ω need only be defined on a generally on a *wide open subspace* U of the associated rigid analytic space, provided that $P, Q \in U(\mathbb{C}_p)$.)

Among its other uses, Coleman integration plays an important role in effective methods in arithmetic geometry.

- Torsion points (effective Manin-Mumford conjecture).
- Rational points on curves via Chabauty-Coleman method.
- Kim's nonabelian Chabauty method (specialized to quadratic Chabauty).

In this talk, we (mostly) ignore applications and focus on the problem of numerically computing Coleman integrals.

Coleman's theory of p-adic path integrals

Let X be a curve over $\mathbb{Q}_p$ with good reduction (for simplicity).

Coleman (1985) gave a definition of the path integral $\int_P^Q \omega \in \mathbb{C}_p$ where ω is a holomorphic differential on X and $P, Q \in X(\mathbb{C}_p)$. (More generally, ω need only be defined on a generally on a *wide open subspace* U of the associated rigid analytic space, provided that $P, Q \in U(\mathbb{C}_p)$.)

Among its other uses, Coleman integration plays an important role in effective methods in arithmetic geometry.

- Torsion points (effective Manin-Mumford conjecture).
- Rational points on curves via Chabauty-Coleman method.
- Kim's nonabelian Chabauty method (specialized to quadratic Chabauty).

In this talk, we (mostly) ignore applications and focus on the problem of numerically computing Coleman integrals.

Jacobian arithmetic

The oldest approach to computing Coleman integrals (Wetherell, 1998) used:

- linearity in the endpoints;
- compatibility with the naive definition on a residue disc.

To compute $\int_D \omega$ for $D \in \mathrm{Pic}^0(X)$, find a positive integer n such that nD projects to zero in the Jacobian of X over $\mathbb{F}_p$. One can then write nD in terms of points in a single residue disc, and then compute $\int_D \omega = n^{-1} \int_{nD} \omega$ by direct integration of power series. (We refer to integrals computed by direct integration in a disc as "tiny integrals".)

Applying this method in practice depends on Jacobian arithmetic. This is sometimes impractical.

Jacobian arithmetic

The oldest approach to computing Coleman integrals (Wetherell, 1998) used:

- linearity in the endpoints;
- compatibility with the naive definition on a residue disc.

To compute $\int_D \omega$ for $D \in \mathrm{Pic}^0(X)$, find a positive integer n such that nD projects to zero in the Jacobian of X over $\mathbb{F}_p$. One can then write nD in terms of points in a single residue disc, and then compute $\int_D \omega = n^{-1} \int_{nD} \omega$ by direct integration of power series. (We refer to integrals computed by direct integration in a disc as "tiny integrals".)

Applying this method in practice depends on Jacobian arithmetic. This is sometimes impractical.

Jacobian arithmetic

The oldest approach to computing Coleman integrals (Wetherell, 1998) used:

- linearity in the endpoints;
- compatibility with the naive definition on a residue disc.

To compute $\int_D \omega$ for $D \in \mathrm{Pic}^0(X)$, find a positive integer n such that nD projects to zero in the Jacobian of X over $\mathbb{F}_p$. One can then write nD in terms of points in a single residue disc, and then compute $\int_D \omega = n^{-1} \int_{nD} \omega$ by direct integration of power series. (We refer to integrals computed by direct integration in a disc as "tiny integrals".)

Applying this method in practice depends on Jacobian arithmetic. This is sometimes impractical.

Frobenius lifts on wide open subspaces

A subsequent approach (Balakrishnan-Bradshaw-K, 2008) used:

- direct computation of tiny integrals;
- change of variables for a Frobenius lift φ on a wide open subspace.

Say ω is a differential form whose class in Monsky-Washnitzer cohomology is a Frobenius eigenvector with eigenvalue λ; by change of variables,

$$\lambda \int_P^Q \omega = \int_P^Q \varphi^* \omega + f(Q) - f(P) = \int_{\varphi(P)}^{\varphi(Q)} \omega + f(Q) - f(P)$$

where f is an antiderivative of $(\varphi^* - \lambda)\omega$. Now

$$\int_P^Q \omega = (\lambda - 1)^{-1} \left(f(Q) - f(P) + \int_P^{\varphi(P)} \omega + \int_{\varphi(Q)}^Q \omega \right)$$

where $\lambda - 1 \neq 0$ by weights (i.e., Weil's proof of RH for curves).

This depends on computing in MW cohomology, and thus on explicit equations. This is sometimes impractical.

Frobenius lifts on wide open subspaces

A subsequent approach (Balakrishnan-Bradshaw-K, 2008) used:

- direct computation of tiny integrals;
- change of variables for a Frobenius lift φ on a wide open subspace.

Say ω is a differential form whose class in Monsky-Washnitzer cohomology is a Frobenius eigenvector with eigenvalue λ; by change of variables,

$$\lambda \int_P^Q \omega = \int_P^Q \varphi^* \omega + f(Q) - f(P) = \int_{\varphi(P)}^{\varphi(Q)} \omega + f(Q) - f(P)$$

where f is an antiderivative of $(\varphi^* - \lambda)\omega$. Now

$$\int_P^Q \omega = (\lambda - 1)^{-1} \left(f(Q) - f(P) + \int_P^{\varphi(P)} \omega + \int_{\varphi(Q)}^Q \omega \right)$$

where $\lambda - 1 \neq 0$ by weights (i.e., Weil's proof of RH for curves).

This depends on computing in MW cohomology, and thus on explicit equations. This is sometimes impractical.

Frobenius lifts on wide open subspaces

A subsequent approach (Balakrishnan-Bradshaw-K, 2008) used:

- direct computation of tiny integrals;
- change of variables for a Frobenius lift φ on a wide open subspace.

Say ω is a differential form whose class in Monsky-Washnitzer cohomology is a Frobenius eigenvector with eigenvalue λ; by change of variables,

$$\lambda \int_P^Q \omega = \int_P^Q \varphi^* \omega + f(Q) - f(P) = \int_{\varphi(P)}^{\varphi(Q)} \omega + f(Q) - f(P)$$

where f is an antiderivative of $(\varphi^* - \lambda)\omega$. Now

$$\int_P^Q \omega = (\lambda - 1)^{-1} \left(f(Q) - f(P) + \int_P^{\varphi(P)} \omega + \int_{\varphi(Q)}^Q \omega \right)$$

where $\lambda - 1 \neq 0$ by weights (i.e., Weil's proof of RH for curves).

This depends on computing in MW cohomology, and thus on explicit equations. This is sometimes impractical.

Hecke correspondences on modular curves

We now focus on modular curves. The problem of (provably) finding all rational points on such a curve is of special interest; for example, Mazur's theorem on torsion points on elliptic curves amounts to finding $X_0(N)(\mathbb{Q})$ for all N (namely, only cusps unless the genus is 0).

Unfortunately, explicit equations for modular curves are often very messy, because these curves are "probably (almost) Brill-Noether general". (E.g., they are known to have large gonality.)

Let X be a modular curve (e.g., $X_0(N)$). For each prime ℓ not dividing N, adding ℓ to the level gives rise to a new modular curve X' admitting two projections $\pi_1, \pi_2 : X' \to X$ of degree $\ell + 1$.

We may use X' to define the *Hecke correspondence* T_ℓ. It acts both on divisors and on differential forms via the same formula:

$$D \mapsto \pi_{2*}\pi_1^* D.$$

Hecke correspondences on modular curves

We now focus on modular curves. The problem of (provably) finding all rational points on such a curve is of special interest; for example, Mazur's theorem on torsion points on elliptic curves amounts to finding $X_0(N)(\mathbb{Q})$ for all N (namely, only cusps unless the genus is 0).

Unfortunately, explicit equations for modular curves are often very messy, because these curves are "probably (almost) Brill-Noether general". (E.g., they are known to have large gonality.)

Let X be a modular curve (e.g., $X_0(N)$). For each prime ℓ not dividing N, adding ℓ to the level gives rise to a new modular curve X' admitting two projections $\pi_1, \pi_2 : X' \to X$ of degree $\ell + 1$.

We may use X' to define the *Hecke correspondence* T_ℓ. It acts both on divisors and on differential forms via the same formula:

$$D \mapsto \pi_{2*}\pi_1^* D.$$

Hecke correspondences on modular curves

We now focus on modular curves. The problem of (provably) finding all rational points on such a curve is of special interest; for example, Mazur's theorem on torsion points on elliptic curves amounts to finding $X_0(N)(\mathbb{Q})$ for all N (namely, only cusps unless the genus is 0).

Unfortunately, explicit equations for modular curves are often very messy, because these curves are "probably (almost) Brill-Noether general". (E.g., they are known to have large gonality.)

Let X be a modular curve (e.g., $X_0(N)$). For each prime ℓ not dividing N, adding ℓ to the level gives rise to a new modular curve X' admitting two projections $\pi_1, \pi_2 : X' \to X$ of degree $\ell + 1$.

We may use X' to define the *Hecke correspondence* T_ℓ. It acts both on divisors and on differential forms via the same formula:

$$D \mapsto \pi_{2*}\pi_1^* D.$$

Hecke correspondences on modular curves

We now focus on modular curves. The problem of (provably) finding all rational points on such a curve is of special interest; for example, Mazur's theorem on torsion points on elliptic curves amounts to finding $X_0(N)(\mathbb{Q})$ for all N (namely, only cusps unless the genus is 0).

Unfortunately, explicit equations for modular curves are often very messy, because these curves are "probably (almost) Brill-Noether general". (E.g., they are known to have large gonality.)

Let X be a modular curve (e.g., $X_0(N)$). For each prime ℓ not dividing N, adding ℓ to the level gives rise to a new modular curve X' admitting two projections $\pi_1, \pi_2 : X' \to X$ of degree $\ell + 1$.

We may use X' to define the *Hecke correspondence* T_ℓ. It acts both on divisors and on differential forms via the same formula:

$$D \mapsto \pi_{2*}\pi_1^* D.$$

Coleman integrals of eigenforms

Suppose now that ω is a Hecke eigenform. Then for any divisor D,

$$a_p \int_D \omega = \int_{T_p^*(D)} \omega$$

where a_p denotes the eigenvalue of T_p on ω. We can rewrite as

$$(p + 1 - a_p) \int_D \omega = \int_{(p+1)D - T_p^*(D)} \omega.$$

For each closed point P in D, $(p+1)P$ and $T_p^*(P)$ each consist of $p+1$ points *in the same residue disc*. We can thus compute the right side via tiny integrals; since $p + 1 - a_p \neq 0$ (the Ramanujan bound implies $|a_p| \leq 2\sqrt{p}$), we can solve for $\int_D \omega$.

Coleman integrals of eigenforms

Suppose now that ω is a Hecke eigenform. Then for any divisor D,

$$a_p \int_D \omega = \int_{T_p^*(D)} \omega$$

where a_p denotes the eigenvalue of T_p on ω. We can rewrite as

$$(p + 1 - a_p) \int_D \omega = \int_{(p+1)D - T_p^*(D)} \omega.$$

For each closed point P in D, $(p+1)P$ and $T_p^*(P)$ each consist of $p+1$ points *in the same residue disc*. We can thus compute the right side via tiny integrals; since $p + 1 - a_p \neq 0$ (the Ramanujan bound implies $|a_p| \leq 2\sqrt{p}$), we can solve for $\int_D \omega$.

Avoidance of models

It remains to compute tiny integrals of a Hecke eigenform. If one has access to a model of the curve, one can expand in power series that way.

However, it is not always convenient to compute a model of the curve. Another possible approach is to produce the series expansion over $\mathbb{C}$ using the uniformization by the upper half-plane. The series has coefficients in the eigenvalue field of ω, which is a number field; one can also control the height and denominators of the coefficients. So a sufficiently good complex floating-point approximation (with rigorous error terms) will suffice.

So far we have tested this in some low-genus examples (e.g., $X_0(37)$) by comparing with the model-based method. Asymptotic performance remains to be assessed.

Avoidance of models

It remains to compute tiny integrals of a Hecke eigenform. If one has access to a model of the curve, one can expand in power series that way.

However, it is not always convenient to compute a model of the curve. Another possible approach is to produce the series expansion over $\mathbb{C}$ using the uniformization by the upper half-plane. The series has coefficients in the eigenvalue field of ω, which is a number field; one can also control the height and denominators of the coefficients. So a sufficiently good complex floating-point approximation (with rigorous error terms) will suffice.

So far we have tested this in some low-genus examples (e.g., $X_0(37)$) by comparing with the model-based method. Asymptotic performance remains to be assessed.

Avoidance of models

It remains to compute tiny integrals of a Hecke eigenform. If one has access to a model of the curve, one can expand in power series that way.

However, it is not always convenient to compute a model of the curve. Another possible approach is to produce the series expansion over $\mathbb{C}$ using the uniformization by the upper half-plane. The series has coefficients in the eigenvalue field of ω, which is a number field; one can also control the height and denominators of the coefficients. So a sufficiently good complex floating-point approximation (with rigorous error terms) will suffice.

So far we have tested this in some low-genus examples (e.g., $X_0(37)$) by comparing with the model-based method. Asymptotic performance remains to be assessed.

Coming attractions: iterated integrals

Coleman's theory also produces iterated integrals like $\int_P^Q \omega_1(*) \int_P^* \omega_2$. These appear in Kim's nonabelian Chabauty method.

These can again be computed using pullback by Frobenius (Balakrishnan-Tuitman). However, we no longer have linearity in the endpoints, so it is not immediately clear how to promote this to correspondences. Work on this is ongoing.

Coming attractions: iterated integrals

Coleman's theory also produces iterated integrals like $\int_P^Q \omega_1(*) \int_P^* \omega_2$. These appear in Kim's nonabelian Chabauty method.

These can again be computed using pullback by Frobenius (Balakrishnan-Tuitman). However, we no longer have linearity in the endpoints, so it is not immediately clear how to promote this to correspondences. Work on this is ongoing.