Explicit computation with Coleman integrals

BU – Keio Workshop 2019

Alex J. Best

27/6/2019

Boston University

Why do we integrate things? Logarithms

Take $\frac{\mathrm{d}x}{x}$, as a differential on the group $\mathrm{R}^{\times}$,

Why do we integrate things? Logarithms

Take $\frac{\mathrm{d}x}{x}$, as a differential on the group $\mathsf{R}^\times$, this is translation invariant, i.e. $(a \cdot -)^*(\mathrm{d}x/x) = \mathrm{d}(ax)/ax = \mathrm{d}x/x$

Why do we integrate things? Logarithms

Take $\frac{\mathrm{d}x}{x}$, as a differential on the group $\mathsf{R}^\times$, this is translation invariant, i.e. $(a\cdot -)^*(\mathrm{d}x/x) = \mathrm{d}(ax)/ax = \mathrm{d}x/x$, hence

$$\int_1^t \frac{\mathrm{d}x}{x} = \log|t| \colon \mathsf{R}^\times \to \mathsf{R}$$

has the property that

$$\int_1^{ab} \frac{\mathrm{d}x}{x} = \int_a^{ab} \frac{\mathrm{d}x}{x} + \int_1^{a} \frac{\mathrm{d}x}{x} = \int_1^{b} \frac{\mathrm{d}x}{x} + \int_1^{a} \frac{\mathrm{d}x}{x}$$

Integration can define logarithm maps between groups and their tangent spaces.

How do we calculate $\log|t|$? Power series on $\mathsf{R}_{>0}$ and use the relation $\log|t| = \frac{1}{2}\log t^2$

We have already seen **polylogarithms**, defined recursively by

$$L_1(z) = -\log(1-z),\ L_k(z) = \int_0^z L_{k-1}(s)\frac{\mathrm{d}s}{s} : \mathbb{C} \setminus [1,\infty) \to \mathbb{C}$$

Why do we integrate things? Interesting functions

We have already seen **polylogarithms**, defined recursively by

$$L_1(z) = -\log(1-z),\ L_k(z) = \int_0^z L_{k-1}(s)\frac{\mathrm{d}s}{s} : \mathbb{C} \setminus [1,\infty) \to \mathbb{C}$$

These functions can alternatively be described via the power series

$$L_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}$$

Coleman integration

Is there p-adic analogue of this?

Coleman integration

Is there p-adic analogue of this? Given a p-adic space, (as p-adic solutions to some equations) we can locally write down convergent power series for a 1-form and integrate.

Coleman integration

Is there p-adic analogue of this? Given a p-adic space, (as p-adic solutions to some equations) we can locally write down convergent power series for a 1-form and integrate.

E.g. near a point α:

$$\omega = \frac{\mathrm{d}(\alpha + x)}{\alpha + x} = \frac{\mathrm{d}x}{\alpha + x} = \frac{1}{\alpha} \sum \left(\frac{-x}{\alpha} \right)^n \mathrm{d}x$$

Is there p-adic analogue of this? Given a p-adic space, (as p-adic solutions to some equations) we can locally write down convergent power series for a 1-form and integrate.

E.g. near a point α:

$$\omega = \frac{\mathrm{d}(\alpha + x)}{\alpha + x} = \frac{\mathrm{d}x}{\alpha + x} = \frac{1}{\alpha} \sum \left(\frac{-x}{\alpha} \right)^n \mathrm{d}x$$

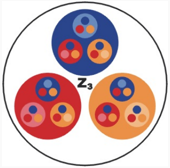
so that

$$\int_{\alpha + x} \omega = -\sum \frac{1}{n+1} \left(\frac{-x}{\alpha} \right)^{n+1} + C$$

Is there p-adic analogue of this? Given a p-adic space, (as p-adic solutions to some equations) we can locally write down convergent power series for a 1-form and integrate.

E.g. near a point α:

$$\omega = \frac{\mathrm{d}(\alpha + x)}{\alpha + x} = \frac{\mathrm{d}x}{\alpha + x} = \frac{1}{\alpha} \sum \left(\frac{-x}{\alpha} \right)^n \mathrm{d}x$$



Bad topology!

so that

$$\int_{\alpha + x} \omega = -\sum \frac{1}{n+1} \left(\frac{-x}{\alpha} \right)^{n+1} + C$$

But we cannot find C! There is a different choice in each disk.

Coleman integration: More problems

Now we have functions

$$\mathrm{T} = \mathrm{K}\langle t\rangle = \left\{\sum a_{\mathrm{i}}t^{\mathrm{i}}; a_{\mathrm{i}} \in \mathrm{K}, \lim_{\mathrm{i}\to\infty} |a_{\mathrm{i}}| = 0\right\}$$

and

$$\mathrm{d}\colon T \to \Omega^1_T$$

and our integral map should send

$$\sum a_i t^{i+1} \mapsto \sum \frac{a_i}{i+1} t^{i+1}$$

but

$$\frac{a_i}{i+1}$$

may not converge to 0.

So instead we work with a subring of **overconvergent** functions

$$\mathcal{T}^\dagger = \left\{\sum a_{\mathrm{i}}t^{\mathrm{i}}; a_{\mathrm{i}} \in K, \exists r > 1 \text{ such that } \lim_{\mathrm{i}\to\infty} |a_{\mathrm{i}}|\, r^{\mathrm{i}} = 0\right\}.$$

Coleman's theorem

Take $X/\mathbf{Z}_p$ a genus g curve, and p an odd prime.

We pick a lift of the Frobenius map, i.e. $\phi\colon X \to X$ which reduces to the Frobenius on $X \times \mathbf{F}_p$, and write $A^\dagger$ (resp. $A_{\mathrm{loc}}(X)$) for overconvergent (resp. locally analytic) functions on X.

Coleman's theorem

Take $X/\mathbf{Z}_p$ a genus g curve, and p an odd prime.

We pick a lift of the Frobenius map, i.e. $\phi\colon X \to X$ which reduces to the Frobenius on $X \times \mathbf{F}_p$, and write $A^\dagger$ (resp. $A_{\text{loc}}(X)$) for overconvergent (resp. locally analytic) functions on X.

Theorem (Coleman)

There is a $\mathbf{Q}_p$-linear map $\int_b^x\colon \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p \to A_{\mathrm{loc}}(X)$ for which:

$$\mathrm{d} \circ \int_b^x = \mathrm{id}\colon \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p \to \Omega^1_{loc} \quad \text{“FTC”}$$

$$\int_b^x \circ\, \mathrm{d} = \mathrm{id}\colon A^\dagger \hookrightarrow A_{\mathrm{loc}}$$

$$\int_b^x \phi^*\omega = \phi^* \int_b^x \omega \quad \text{“Frobenius equivariance”}$$

Computation: Polylogarithms on $\mathbf{P}^1 \setminus \{0, 1, \infty\}$

Let's revisit the **polylogarithms**

$$L_1(z) = -\log(1 - z),\ L_k(z) = \int_0^z L_{k-1}(s)\frac{\mathrm{d}s}{s} : \mathbf{C} \setminus [1, \infty) \to \mathbf{C}$$

Coleman integration then defines a p-adic analogue of these functions, with exactly the same definition via iterated integration on $\mathbf{P}^1 \setminus \{0, 1, \infty\}$.

(We must choose a branch of the p-adic logarithm, for simplicity we take the **Iwasawa logarithm** where $\log_p(p) = 0$.)

The power series definition still holds near $z = 0$, but otherwise we must use frobenius equivariance to define it.

Computing polylogarithms

Besser and de Jeu have given a complete algorithm to compute these functions, and this is now implemented in SageMath.

For instance in Sage we can check relations among polylogarithms

```
sage: K = Qp(7, prec=30)
sage: x = K(1/3)
sage: (x^2).polylog(4) - 8*x.polylog(4) -
    8*(-x).polylog(4)
O(7^23)
```

Computing polylogarithms

Besser and de Jeu have given a complete algorithm to compute these functions, and this is now implemented in SageMath.

For instance in Sage we can check relations among polylogarithms

```
sage: K = Qp(7, prec=30)
sage: x = K(1/3)
sage: (x^2).polylog(4) - 8*x.polylog(4) -
    8*(-x).polylog(4)
O(7^23)
```

In exactly the same way as:

```
sage: x = RBF(1/3) # Real ball, or do pari(1/3)
sage: (x^2).polylog(4) - 8*x.polylog(4) -
    8*(-x).polylog(4)
[+/- 2.51e-14]
```

Computation: group structure

If $X/\mathbf{Q}_p$ is an algebraic group, ω is a translation invariant 1-form we have

$$\int_0^{P+Q} \omega = \int_0^P \omega + \int_0^Q \omega \implies \int_0^P \omega = \frac{1}{n} \int_0^{nP} \omega$$

but if $n = \#\tilde{X}(\mathbf{F}_p)$ then $nP \in B(0,1)$ so the integral on the right can be performed locally with only power series.

Computation: group structure

If $X/\mathbf{Q}_p$ is an algebraic group, ω is a translation invariant 1-form we have

$$\int_0^{P+Q}\omega = \int_0^P \omega + \int_0^Q \omega \implies \int_0^P \omega = \frac{1}{n}\int_0^{nP}\omega$$

but if $n = \#\tilde{X}(\mathbf{F}_p)$ then $nP \in B(0,1)$ so the integral on the right can be performed locally with only power series.

This requires arithmetic in the group, which may be hard. And can only integrate invariant differentials.

Computation: p-adic cohomology

There is an alternate approach via p-adic cohomology, due to Balakrishnan-Bradshaw-Kedlaya.

Let $X/\mathbf{Z}_p$ be a smooth curve of good reduction.

Pick a basis $\omega_1, \ldots, \omega_{2g}$ for $H^1_{\mathrm{dR}}(X)$ and let $U \subseteq X$ be an affine subspace containing no poles of any ω_i and on which we have a lift of frobenius ϕ.

Computation: p-adic cohomology

There is an alternate approach via p-adic cohomology, due to Balakrishnan-Bradshaw-Kedlaya.

Let $X/\mathbf{Z}_p$ be a smooth curve of good reduction.

Pick a basis $\omega_1, \ldots, \omega_{2g}$ for $H^1_{\mathrm{dR}}(X)$ and let $U \subseteq X$ be an affine subspace containing no poles of any ω_i and on which we have a lift of frobenius ϕ.

If we apply ϕ^* to ω_i we may write

$$\phi^*\omega_i = \sum_{j=1}^{2g} M_{ij}\omega_j - \mathrm{d}f_i \quad \text{using Kedlaya's algorithm, or a variant}$$

Computation: p-adic cohomology

There is an alternate approach via p-adic cohomology, due to Balakrishnan-Bradshaw-Kedlaya.

Let $X/\mathbf{Z}_p$ be a smooth curve of good reduction.

Pick a basis $\omega_1, \ldots, \omega_{2g}$ for $H^1_{\mathrm{dR}}(X)$ and let $U \subseteq X$ be an affine subspace containing no poles of any ω_i and on which we have a lift of frobenius ϕ.

If we apply ϕ^* to ω_i we may write

$$\phi^*\omega_i = \sum_{j=1}^{2g} M_{ij}\omega_j - \mathrm{d}f_i \quad \text{using Kedlaya's algorithm, or a variant}$$

$$\int_{\phi(b)}^{\phi(P)} \omega_i = \int_b^P \phi^*\omega_i = \int_b^P \left(\sum_{j=1}^{2g} M_{ij}\omega_j\right) - \int_b^P \mathrm{d}f_i$$

Computation: p-adic cohomology

$$\int_{\phi(b)}^{\phi(P)} \omega_i = \int_b^P \left(\sum_{j=1}^{2g} M_{ij}\omega_j \right) - (f_i(P) - f_i(b))$$

$$\implies \qquad \begin{pmatrix} \vdots \\ \int_{\phi(b)}^{\phi(P)} \omega_i \\ \vdots \end{pmatrix} = (M - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) - f_i(b) \\ \vdots \end{pmatrix}$$

Computation: p-adic cohomology

$$\int_{\phi(b)}^{\phi(P)} \omega_i = \int_b^P \left(\sum_{j=1}^{2g} M_{ij}\omega_j \right) - (f_i(P) - f_i(b))$$

$$\implies \qquad \begin{pmatrix} \vdots \\ \int_{\phi(b)}^{\phi(P)} \omega_i \\ \vdots \end{pmatrix} = (M - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) - f_i(b) \\ \vdots \end{pmatrix}$$

Every point $P \in U$ is close to one fixed by Frobenius, so we can use the above and local integration to find integrals between points of U.

Computation: p-adic cohomology

$$\int_{\phi(b)}^{\phi(P)} \omega_i = \int_b^P \left(\sum_{j=1}^{2g} M_{ij}\omega_j \right) - (f_i(P) - f_i(b))$$

$$\implies \qquad \begin{pmatrix} \vdots \\ \int_{\phi(b)}^{\phi(P)} \omega_i \\ \vdots \end{pmatrix} = (M - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) - f_i(b) \\ \vdots \end{pmatrix}$$

Every point $P \in U$ is close to one fixed by Frobenius, so we can use the above and local integration to find integrals between points of U.

To move outside of U we have to either work close to the boundary of the removed disks (i.e. in a highly ramified extension). Or use tricks due to the special geometry of the curve (extra automorphisms).

Applications: Chabauty's method

Given $X/\mathbf{Q}$ a smooth curve and $p > 2 \cdot \mathsf{genus}(X)$ a prime of good reduction for X and base point $b \in X(\mathbf{Q})$. If

$$\mathsf{rank}(\mathsf{Jac}(X))(\mathbf{Q}) < \mathsf{genus}(X)$$

we can find a differential $\omega_{\mathrm{ann}} \in H^0(X, \Omega^1)$ such that

$$X(\mathbf{Q}) \subseteq F^{-1}(0) \text{ for } F(z) = \int_b^z \omega_{\mathrm{ann}}$$

Applications: Chabauty's method

Given $X/\mathbf{Q}$ a smooth curve and $p > 2 \cdot \mathsf{genus}(X)$ a prime of good reduction for X and base point $b \in X(\mathbf{Q})$. If

$$\mathsf{rank}(\mathsf{Jac}(X))(\mathbf{Q}) < \mathsf{genus}(X)$$

we can find a differential $\omega_{\mathrm{ann}} \in H^0(X, \Omega^1)$ such that

$$X(\mathbf{Q}) \subseteq F^{-1}(0) \text{ for } F(z) = \int_b^z \omega_{\mathrm{ann}}$$

this F and its zero set can be computed explicitly in practice, giving an explicit finite set containing $X(\mathbf{Q})$ in many examples.

Applications: Chabauty's method

Given $X/\mathbf{Q}$ a smooth curve and $p > 2 \cdot \mathsf{genus}(X)$ a prime of good reduction for X and base point $b \in X(\mathbf{Q})$. If

$$\mathsf{rank}(\mathsf{Jac}(X))(\mathbf{Q}) < \mathsf{genus}(X)$$

we can find a differential $\omega_{\mathrm{ann}} \in H^0(X, \Omega^1)$ such that

$$X(\mathbf{Q}) \subseteq F^{-1}(0) \text{ for } F(z) = \int_b^z \omega_{\mathrm{ann}}$$

this F and its zero set can be computed explicitly in practice, giving an explicit finite set containing $X(\mathbf{Q})$ in many examples.

Note: We can use either the group theory or p-adic cohomology method here.

Applications: Chabauty-Kim

Minhyong Kim has vastly generalised the above to cases where

$$\mathrm{rank}(\mathrm{Jac}(X))(\mathbb{Q}) \geq \mathrm{genus}(X)$$

Applications: Chabauty-Kim

Minhyong Kim has vastly generalised the above to cases where

$$\mathrm{rank}(\mathrm{Jac}(X))(\mathbb{Q}) \geq \mathrm{genus}(X)$$

This can be made effective, and computable

Theorem (Balakrishnan-Dogra-Muller-Tuitman-Vonk)
The (cursed) modular curve $X_{split}(13)$ (of genus 3 and jacobian rank 3), has 7 rational points: one cusp and 6 points that correspond to CM elliptic curves whose mod-13 Galois representations land in normalizers of split Cartan subgroups.

Minhyong Kim has vastly generalised the above to cases where

$$\mathrm{rank}(\mathrm{Jac}(X))(\mathbf{Q}) \geq \mathrm{genus}(X)$$

This can be made effective, and computable

Theorem (Balakrishnan-Dogra-Muller-Tuitman-Vonk)
The (cursed) modular curve $X_{split}(13)$ (of genus 3 and jacobian rank 3), has 7 rational points: one cusp and 6 points that correspond to CM elliptic curves whose mod-13 Galois representations land in normalizers of split Cartan subgroups.

Their method can also be applied to other interesting curves:

Theorem (WIP B.-Bianchi-Triantafillou-Vonk)
The modular curve $X_0(67)^+$ (of genus 2 and jacobian rank 2), has rational points contained in an explicitly computable finite set of 7-adic points.

Motivating question

Can p-adic algorithms for computing zeta functions be turned into algorithms for computing Coleman integrals?

Motivating question

Can p-adic algorithms for computing zeta functions be turned into algorithms for computing Coleman integrals?

For instance Harvey and Minzlaff have introduced variants of Kedlaya's algorithm for hyper- and super-elliptic curves that works well when p is large!

They use interpolation to reduce the work when reducing

$$\phi^* \omega_j \rightsquigarrow \sum M_{ij} \omega_j$$

not clear where the functions f_i went.

Key to the interpolation is the fact that reductions in cohomology are linear in the exponents of x, y.

Surprising consequence: Evaluation is faster than writing the function down!

Balakrishnan-Tuitman have an alternative approach for

Theorem (B.)
Let

$$C/\mathbf{Z}_{p^n} : y^a = h(x)$$

with $\gcd(a, \deg(h)) = 1$, $p \nmid a$, *Let* M *be the matrix of Frobenius, acting on* $H^1_{\mathrm{dR}}(C)$, *basis* $\{\omega_{i,j} = x^i \,\mathrm{d}x/y^j\}_{i=0,\ldots,b-2, j=1,\ldots,a}$, *and points* $P, Q \in C(\mathbf{Q}_{p^n})$ *known to precision* p^N, *if* $p > (aN-1)b$, *the vector of Coleman integrals* $\left(\int_P^Q \omega_{i,j}\right)_{i,j}$ *can be computed in time*

$$\widetilde{O}\left(g^3\sqrt{p}nN^{5/2} + N^4 g^4 n^2 \log p\right)$$

to absolute precision $N - v_p(\det(M - I))$.

Theorem (B.)
Let

$$C/\mathbf{Z}_{p^n} : y^a = h(x)$$

with $\gcd(a, \deg(h)) = 1$, $p \nmid a$, *Let* M *be the matrix of Frobenius, acting on* $H^1_{\mathrm{dR}}(C)$, *basis* $\{\omega_{i,j} = x^i \,\mathrm{d}x/y^j\}_{i=0,\dots,b-2, j=1,\dots,a}$, *and points* $P, Q \in C(\mathbf{Q}_{p^n})$ *known to precision* p^N, *if* $p > (aN-1)b$, *the vector of Coleman integrals* $\left(\int_P^Q \omega_{i,j}\right)_{i,j}$ *can be computed in time*

$$\widetilde{O}\left(g^3\sqrt{p}nN^{5/2} + N^4g^4n^2\log p\right)$$

to absolute precision $N - v_p(\det(M - I))$.

By integrating invariant differentials we can check/guess linear relations between points on the Jacobian of this superelliptic curve.

Theorem (B.)
Let

$$C/\mathbf{Z}_{p^n} : y^a = h(x)$$

with $\gcd(a, \deg(h)) = 1$, $p \nmid a$, *Let* M *be the matrix of Frobenius, acting on* $H^1_{\mathrm{dR}}(C)$, *basis* $\{\omega_{i,j} = x^i \,\mathrm{d}x/y^j\}_{i=0,\ldots,b-2,j=1,\ldots,a}$, *and points* $P, Q \in C(\mathbf{Q}_{p^n})$ *known to precision* p^N, *if* $p > (aN-1)b$, *the vector of Coleman integrals* $\left(\int_P^Q \omega_{i,j}\right)_{i,j}$ *can be computed in time*

$$\widetilde{O}\left(g^3\sqrt{p}nN^{5/2} + N^4 g^4 n^2 \log p\right)$$

to absolute precision $N - v_p(\det(M - I))$.

By integrating invariant differentials we can check/guess linear relations between points on the Jacobian of this superelliptic curve.

Speed of this algorithm may lend itself to answering distributional questions?