

EXPLICIT COMPUTATION WITH COLEMAN INTEGRALS

BU – KEIO WORKSHOP 2019

Alex J. Best

27/6/2019

Boston University

WHY DO WE INTEGRATE THINGS? LOGARITHMS

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

WHY DO WE INTEGRATE THINGS? LOGARITHMS

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

WHY DO WE INTEGRATE THINGS? LOGARITHMS

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

$$\int_1^t \frac{dx}{x} = \log |t|: \mathbf{R}^\times \rightarrow \mathbf{R}$$

has the property that

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

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

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

WHY DO WE INTEGRATE THINGS? INTERESTING FUNCTIONS

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

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

WHY DO WE INTEGRATE THINGS? INTERESTING FUNCTIONS

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

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

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.

For instance near a point α :

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

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.

For instance near a point α :

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

so that

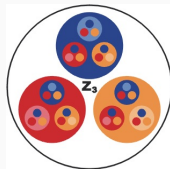
$$\int_{\alpha+x} \omega = - \sum \frac{1}{n+1} \left(\frac{-x}{\alpha} \right)^{n+1} + C$$

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.

For instance near a point α :

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



so that

Bad topology!

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

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

COLEMAN INTEGRATION: MORE PROBLEMS

Now we have functions

$$K\langle t \rangle = \left\{ \sum a_i t^i; a_i \in K, \lim_{i \rightarrow \infty} |a_i| = 0 \right\}$$

and

$$d: T \rightarrow \Omega_T^1$$

and our integral map should send

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

but

COLEMAN INTEGRATION: MORE PROBLEMS

Now we have functions

$$K\langle t \rangle = \left\{ \sum a_i t^i; a_i \in K, \lim_{i \rightarrow \infty} |a_i| = 0 \right\}$$

and

$$d: T \rightarrow \Omega_T^1$$

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.

COLEMAN INTEGRATION: MORE PROBLEMS

Now we have functions

$$K\langle t \rangle = \left\{ \sum a_i t^i; a_i \in K, \lim_{i \rightarrow \infty} |a_i| = 0 \right\}$$

and

$$d: T \rightarrow \Omega_T^1$$

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

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

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. $\phi: X \rightarrow X$ 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 .

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. $\phi: X \rightarrow X$ 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 $\int_b^X: \Omega_{A^\dagger}^1 \otimes \mathbf{Q}_p \rightarrow A_{\text{loc}}(X)$ for which:

$$d \circ \int_b^X = \text{id}: \Omega_{A^\dagger}^1 \otimes \mathbf{Q}_p \rightarrow \Omega_{\text{loc}}^1 \quad \text{"FTC"}$$

$$\int_b^X \circ d = \text{id}: A^\dagger \hookrightarrow A_{\text{loc}}$$

$$\int_b^X \phi^* \omega = \phi^* \int_b^X \omega \quad \text{"Frobenius equivariance"}$$

COMPUTATION: POLYLOGARITHMS ON $\mathbf{P}^1 \setminus \{0, 1, \infty\}$

Let's revisit the **polylogarithms**

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

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.

COMPUTING POLYLOGARITHMS

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

For instance 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)
0(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 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)
0(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 $\omega_1, \dots, \omega_{2g}$ for $H_{\text{dR}}^1(X)$ 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 $\omega_1, \dots, \omega_{2g}$ for $H_{\text{dR}}^1(X)$ 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

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

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 $\omega_1, \dots, \omega_{2g}$ for $H_{\text{dR}}^1(X)$ 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

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

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

COMPUTATION: p -ADIC COHOMOLOGY

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

$$\Rightarrow \begin{pmatrix} \vdots \\ \int_b^P \omega_i \\ \vdots \end{pmatrix} = (M - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) - f_i(b) \\ \vdots \end{pmatrix} \text{ if } b = \phi(b), P = \phi(P)$$

COMPUTATION: p -ADIC COHOMOLOGY

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

$$\Rightarrow \begin{pmatrix} \vdots \\ \int_b^P \omega_i \\ \vdots \end{pmatrix} = (M - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) - f_i(b) \\ \vdots \end{pmatrix} \text{ if } b = \phi(b), P = \phi(P)$$

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

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

$$\Rightarrow \begin{pmatrix} \vdots \\ \int_b^P \omega_i \\ \vdots \end{pmatrix} = (M - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) - f_i(b) \\ \vdots \end{pmatrix} \text{ if } b = \phi(b), P = \phi(P)$$

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

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

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

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

APPLICATIONS: CHABAUTY'S METHOD

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

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

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

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

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

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

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

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

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

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

APPLICATIONS: CHABAUTY-KIM

Minhyong Kim has vastly generalised the above to cases where

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

This can be made effective, and computable

Theorem (Balakrishnan-Dogra-Muller-Tuitman-Vonk)

The (cursed) modular curve $X_{\text{split}}(13)$ (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.

APPLICATIONS: CHABAUTY-KIM

Minhyong Kim has vastly generalised the above to cases where

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

This can be made effective, and computable

Theorem (Balakrishnan-Dogra-Muller-Tuitman-Vonk)

The (cursed) modular curve $X_{\text{split}}(13)$ (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 Minzloff have introduced variants of Kedlaya's algorithm for hyper- and super-elliptic curves that works well when p is large!

MOTIVATING QUESTION

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

For instance Harvey and Minzloff 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

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

but its not clear where the functions f_i went.

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

SUPERELLIPTIC CURVES

We can write down a similar recurrence that evaluates the exact forms also, using

$$\left(\sum_{i=0}^N a_i x^i \right) = ((\cdots ((a_N)x + a_{N-1})x + \cdots)x + a_0)$$

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 $H_{\text{dR}}^1(C)$, basis $\{\omega_{i,j} = x^i dx/y^j\}_{i=0,\dots,b-2, j=1,\dots,a}$, 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

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

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