Explicit computation with Coleman integrals

Journées Arithmétiques XXXI – Istanbul University

Alex J. Best

2/7/2019

Boston University

Question
Is there p-adic analogue of (path) integration?

Question
Is there p-adic analogue of (path) integration?

Given a p-adic space, ($\approx$ the p-adic solutions to some equations). We can locally write down power series defining a 1-form and try to integrate.

Question
Is there p-adic analogue of (path) integration?

Given a p-adic space, ($\approx$ the p-adic solutions to some equations). We can locally write down power series defining a 1-form and try to integrate.

For instance
near a point $\alpha \in \mathbf{G}_m(\mathbf{Q}_p) = \mathbf{Q}_p^\times$:

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

Question
Is there p-adic analogue of (path) integration?

Given a p-adic space, ($\approx$ the p-adic solutions to some equations). We can locally write down power series defining a 1-form and try to integrate.

For instance
near a point $\alpha \in \mathbf{G}_m(\mathbf{Q}_p) = \mathbf{Q}_p^\times$:

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

so that

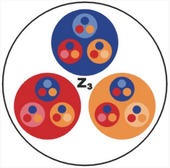
$$\int_{\alpha}^{\alpha+t} \frac{\mathrm{d}x}{x} = -\sum \frac{1}{n+1} \left(\frac{-t}{\alpha}\right)^{n+1} + C$$

Question
Is there p-adic analogue of (path) integration?

Given a p-adic space, ($\approx$ the p-adic solutions to some equations). We can locally write down power series defining a 1-form and try to integrate.

For instance
near a point $\alpha \in \mathbf{G}_m(\mathbf{Q}_p) = \mathbf{Q}_p^\times$:

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



so that

Bad topology!

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

Coleman integration: More problems

Working on one p-adic disk, the space of functions we might want to consider is

$$T = \mathbf{Q}_p \langle t \rangle = \left\{ \sum a_i t^i ; a_i \in \mathbf{Q}_p, \lim_{i \to \infty} |a_i| = 0 \right\}$$

and we have the usual differential

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

so our integral map should send

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

Coleman integration: More problems

Working on one p-adic disk, the space of functions we might want to consider is

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

and we have the usual differential

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

so our integral map should send

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

but $\frac{a_i}{i+1}$ may not converge to 0.

Coleman integration: More problems

Working on one p-adic disk, the space of functions we might want to consider is

$$T = \mathbf{Q}_p \langle t \rangle = \left\{ \sum a_i t^i ; a_i \in \mathbf{Q}_p, \lim_{i \to \infty} |a_i| = 0 \right\}$$

and we have the usual differential

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

so our integral map should send

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

but $\frac{a_i}{i+1}$ may not converge to 0.

$\rightsquigarrow$ Instead work with a subring, of **overconvergent** functions

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

Take $X/\mathbf{Z}_p$ regular and proper, 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 $X \times_{\mathbf{Z}_p} \mathbf{F}_p$, and write $A^\dagger$ (resp. $A_{\mathrm{loc}}(X)$) for overconvergent (resp. locally analytic) functions on X.

Coleman's theorem

Take $X/\mathbf{Z}_p$ regular and proper, 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 $X \times_{\mathbf{Z}_p} \mathbf{F}_p$, and write $A^\dagger$ (resp. $A_{\mathrm{loc}}(X)$) for overconvergent (resp. locally analytic) functions on X.

Theorem (Coleman)

There is a $\mathbf{Q}_p$*-linear map* $\int_b^x\colon (\Omega^1_{A^\dagger} \otimes \mathbf{Q}_p)^{\mathrm{d}=0} \to A_{\mathrm{loc}}(X)$ *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: group structure

If $X/\mathbf{Z}_p$ 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 $X/\mathbf{Z}_p$ 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 (for hyperelliptic curves).

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

Pick a basis $\omega_1, \ldots, \omega_{2g}$ for $H^1_{\mathrm{dR}}(X) = \Omega^1_{A^\dagger} / \mathrm{d}(A^\dagger)$ 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 (for hyperelliptic curves).

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

Pick a basis $\omega_1, \ldots, \omega_{2g}$ for $H^1_{\mathrm{dR}}(X) = \Omega^1_{A^\dagger} / \mathrm{d}(A^\dagger)$ 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 (for hyperelliptic curves).

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

Pick a basis $\omega_1, \ldots, \omega_{2g}$ for $H^1_{\mathrm{dR}}(X) = \Omega^1_{A^\dagger} / \mathrm{d}(A^\dagger)$ 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

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

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

Computation: p-adic cohomology

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

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

Computation: p-adic cohomology

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

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

Every point $P \in U$ is close to one fixed by Frobenius, so we can use this system and formally integrate between nearby points to find integrals with endpoints in U.

Computation: p-adic cohomology

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

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

Every point $P \in U$ is close to one fixed by Frobenius, so we can use this system and formally integrate between nearby points to find integrals with endpoints in 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).

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

They use interpolation to reduce the computation when reducing

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

but its not clear where the functions f_i went in their work, they can simplify by forgetting this data which is irrelevant for computing zeta functions,

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 work well when p is large!

They use interpolation to reduce the computation when reducing

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

but its not clear where the functions f_i went in their work, they can simplify by forgetting this data which is irrelevant for computing zeta functions, but not for Coleman integrals!

We need to know the f_i also, or, crucially, just their evaluations at points P, b.

The reduction procedure for Superelliptic curves

Let $$C/\mathbf{Z}_p \colon y^a = h(x),\ U = C \smallsetminus \{y = 0, \infty\}$$

with $\gcd(a, \deg(h)) = 1$, $p \nmid a$,

The reduction procedure for Superelliptic curves

Let $$C/\mathbf{Z}_p \colon y^a = h(x),\ U = C \setminus \{y = 0, \infty\}$$

with $\gcd(a, \deg(h)) = 1$, $p \nmid a$, Minzlaff uses the lift of Frobenius ϕ where

$$\phi(x) = x^p,\ \phi(y) = y^p \sum_{k=0}^{\infty} \binom{\frac{1}{a}}{k} \frac{(\phi(h) - h^p)^k}{y^{apk}}$$

The reduction procedure for Superelliptic curves

Let $$C/\mathbf{Z}_p\colon y^a = h(x),\ U = C \smallsetminus \{y = 0, \infty\}$$

with $\gcd(a, \deg(h)) = 1$, $p \nmid a$, Minzlaff uses the lift of Frobenius ϕ where

$$\phi(x) = x^p,\ \phi(y) = y^p \sum_{k=0}^{\infty} \binom{\frac{1}{a}}{k} \frac{(\phi(h) - h^p)^k}{y^{apk}}$$

$$\rightsquigarrow \phi^*(x^i \, \mathrm{d}x/y^j) \equiv \sum_{k=0}^{N-1} \sum_{r=0}^{bk} \mu_{k,r,j} x^{p(i+r+1)-1} y^{-p(ak+j)} \, \mathrm{d}x \pmod{p^N}.$$

The reduction procedure for Superelliptic curves

Let
$$C/\mathbf{Z}_p \colon y^a = h(x),\ U = C \setminus \{y = 0, \infty\}$$
with $\gcd(a, \deg(h)) = 1$, $p \nmid a$, Minzlaff uses the lift of Frobenius ϕ where

$$\phi(x) = x^p,\ \phi(y) = y^p \sum_{k=0}^{\infty} \binom{\frac{1}{a}}{k} \frac{(\phi(h) - h^p)^k}{y^{apk}}$$

$$\rightsquigarrow \phi^*(x^i\,\mathrm{d}x/y^j) \equiv \sum_{k=0}^{N-1} \sum_{r=0}^{bk} \mu_{k,r,j} x^{p(i+r+1)-1} y^{-p(ak+j)}\,\mathrm{d}x \pmod{p^N}.$$

To find a cohomologous sum of basis differentials we use relations like

$$\begin{aligned} x^i y^{-at-\beta}\,\mathrm{d}x &- \frac{-a}{at+\beta-a}\,\mathrm{d}(S_i(x) y^{-at-\beta+a}) \\ &= \frac{(at+\beta-a)R_i(x) + aS_i'(x)}{at+\beta-a} y^{-a(t-1)-\beta}\,\mathrm{d}x \end{aligned}$$

repeatedly to reduce the y-degree until we reach the basis.

Note that the term

$$\frac{(at+\beta-a)R_i(x)+aS_i'(x)}{at+\beta-a}$$

is linear in the exponent t of y, this is key to applying the algorithm of Bostan-Gaudry-Schost to speed up evaluation.

Note that the term

$$\frac{(at+\beta-a)R_i(x)+aS_i'(x)}{at+\beta-a}$$

is linear in the exponent t of y, this is key to applying the algorithm of Bostan-Gaudry-Schost to speed up evaluation. But the term that we must add to evaluate the f_i

$$\frac{-a}{at+\beta-a}S_i(x)y^{-at-\beta+a}$$

is not linear in t!

Note that the term

$$\frac{(at+\beta-a)R_i(x)+aS_i'(x)}{at+\beta-a}$$

is linear in the exponent t of y, this is key to applying the algorithm of Bostan-Gaudry-Schost to speed up evaluation. But the term that we must add to evaluate the f_i

$$\frac{-a}{at+\beta-a}S_i(x)y^{-at-\beta+a}$$

is not linear in t! However if we think of evaluating f as follows

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

we obtain a linear recurrence whose coefficients are fractions of linear functions of t.

Theorem (B.)
For X superelliptic as above. 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

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

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

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 $\omega_{\text{ann}} \in H^0(X, \Omega^1)$ 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

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

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.

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.

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 set of 7-adic points of cardinality 16.