p-adic integration on bad reduction on hyperelliptic curves

Eric Katz (The Ohio State University)
joint with Enis Kaya

September 24, 2020

Good reduction vs. bad reduction

Let R be a complete DVR (think $\mathbb{Z}_p$) with residue field $\mathbf{k}$ and field of fractions K.

Definition

A curve X over K is of good reduction if there is a regular model $\mathfrak{X}/R$ with

1. $\mathfrak{X}_K \cong X$ and
2. the special fiber $\mathfrak{X}_0 = \mathfrak{X} \times_R \mathbf{k}$ is smooth

"the curve remains smooth after reduction mod p."
Otherwise, the curve is of bad reduction.

After possibly extending K we can produce $\mathfrak{X}$ such that $\mathfrak{X}_0$ has at worst nodal singularities (isomorphic to $xy = 0$).

Berkovich–Coleman integration

These are line integrals on curves X/K where K is a finite extension of $\mathbb{Q}_p$.

They need: 1-form $\omega \in \Omega^1(X)$; and a path γ on X^{an} (the Berkovich space).

A path here is a path in the dual graph together with K-points on the components corresponding to its endpoints.

$$\int_\gamma \omega \in K$$

If X is of good reduction, the integral only depends on the endpoints of γ. This is Coleman integration and it's important in number theory.

Integration on bad reduction curves

If X is bad reduction, there are some complications. We have to integrate 1-forms like dx/x on annuli like

$$A = \{x \in \mathbb{A}^1 \mid r \leq \|x\|_p \leq R\}$$

Which branch of $\mathrm{Log}(x)$ do we choose?
Two possibilities for how to manage this:

1. pick one branch of Log once and for all; this leads to Berkovich–Coleman integration. It is path dependent, but it can be computed locally on the curve.
2. keep path independence; this leads to abelian integration. It is no longer local, but it is this integration that is important for number theory.

Abelian integration

Given a base point $x_0 \in X(K)$, take the Abel–Jacobi map $\iota\colon X \to J(X)$. Then $\int_{x_0}^{x}$ is given by

$$X \xrightarrow{\iota} J(X) \xrightarrow{\log} \operatorname{Lie} J(X) \xrightarrow{\omega} K$$

where we interpret $\omega \in \Omega^1(X) \cong TX_0^\vee \cong \operatorname{Lie} J(X)^\vee$.

We can convert between Berkovich–Coleman and abelian integration due to work of Besser–Zerbes, Stoll, K–Rabinoff–Zureick-Brown. We need as input the Berkovich–Coleman periods, the integrals along closed loops γ_i.

Theorem

$$\,^{\mathrm{BC}}\!\!\int_\gamma \omega - \,^{\mathrm{Ab}}\!\!\int_{x_0}^{x} \omega = \sum_i \left(\,^{\mathrm{BC}}\!\!\int_{\gamma_i} \omega\right)\left(\,^{t}\!\!\int_{\tau(\gamma)} \eta_i\right)$$

Here $\,^{t}\!\!\int$ denotes tropical integration of certain tropical 1-forms η_i on the dual graph.

Hyperelliptic curves

These are compactifications of

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

where $f(x)$ is a polynomial of degree d.
We interpret the curve as having a degree 2 map

$$\pi\colon X \to \mathbb{P}^1$$

This is

1. smooth if $f(x)$ has distinct roots;
2. good reduction if the roots remain distinct after specializing $R \to \mathbf{k}$.

Intergration on good reduction hyperelliptic curves

There are algorithms for computing Coleman integrals on good reduction hyperelliptic curves. The original one is due to Balakrishnan–Bradshaw–Kedlaya.

The ingredients are the following:

1. Consider the affine bit of the curve $X^\circ = X \cap (K^*)^2$.
2. Look at $H^1_{\mathrm{dR}}(X^\circ)^-$, the (-1)-eigenspace of the cohomology under $y \mapsto -y$
3. A basis for the odd cohomology is given by $\omega_i = x^i \frac{dx}{y}$ for $i = 0, 1, \ldots, d-2$.
4. Lift Frobenius to $\phi\colon X^\circ \to X^\circ$. We get an action on cohomology.
5. Write $\omega = [\ \omega_1 \quad \omega_2 \quad \ldots \quad \omega_{d-2}\ ]$, and solve for $\phi^*\omega = M\omega + dF$ for a matrix M and a vector of functions F.
6. Use $\int_P^Q \phi^*\omega = \int_{\phi(P)}^{\phi(Q)} \omega$.

Aside: If we remove discs D_j around points $\beta_j \in \mathbb{P}^1$ and take $X^{\mathrm{an}} \setminus \cup \pi^{-1}(D_i)$, we have to add $\nu_j = \frac{dx}{(x-\beta_j)2y}$.

Bad reduction case

On bad reduction curves, this does not work.

This is not a reasonable definition of the lift of Frobenius . There is an action of Frobenius on cohomology but it has eigenvectors of the wrong weight which prevent one from solving for the integral.

Instead, you can reduce to the good reduction case to get Berkovich–Coleman integrals.

The algorithm for bad reduction curves

1. Cover X^{an} by open subsets U_j that can be embedded in good reduction hyperelliptic curves X_j.
2. Pullback ω_i's to U_j and write them in terms of our basis of cohomology (plus an exact form); here ω_i's may acquire poles when extended to X_j's.
3. Break up the path into paths in U_j's and compute Berkovich–Coleman integrals on good reduction curves.
4. Find Berkovich–Coleman periods and convert to Abelian integrals.

Our algorithm has been carried out in Sage modulo limitations. We sometimes have to use more general extensions of $\mathbb{Q}_p$ than what Sage can handle.

Finding the covering

Consider $X \to \mathbb{P}^1$ given by $y^2 = f(x)$. Let $S \subset \mathbb{P}^1$ be the zeroes of f (where we consider ∞ if f is of odd degree). Look at open subsets of $\mathbb{P}^1$ given by an open disc minus some closed discs

$$V = B(a, r) \setminus \bigsqcup \overline{B}(a_i, r_i).$$

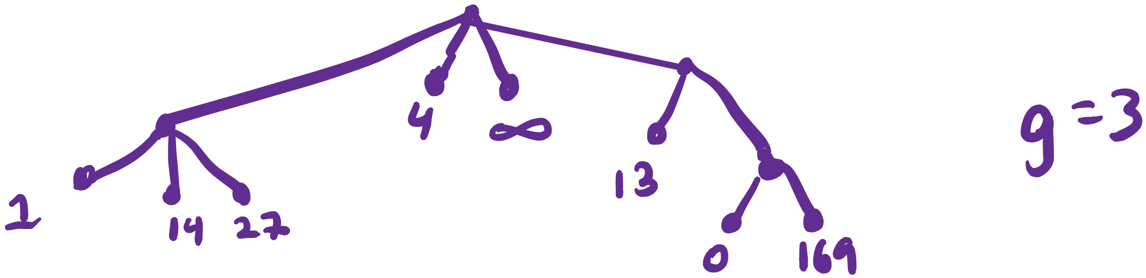
We say V is good if there exists a fractional linear transformation $i\colon \mathbb{P}^1 \to \mathbb{P}^1$ such that each point of $i(V \cap S)$ lies in a distinct residue disc.

We're just rescaling to keep roots in different residue discs.

Then $U = \pi^{-1}(V)$ can be embedded in a good reduction hyperelliptic curve.

Example

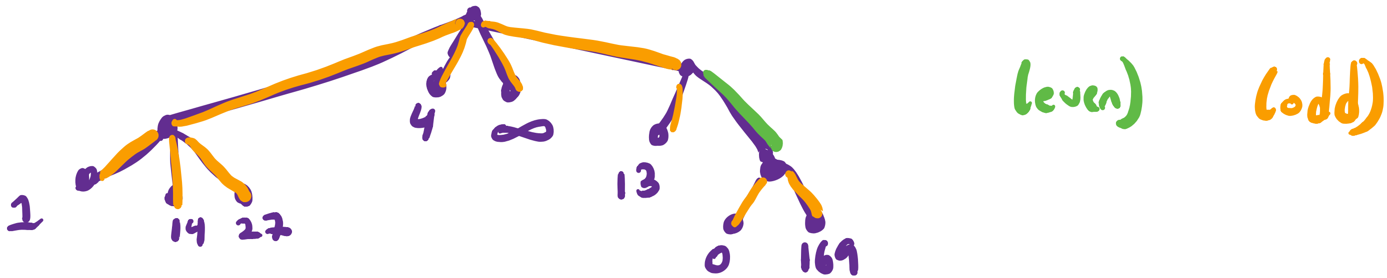
Here is a picture of zeroes of $f(x)$ In $\mathbb{Q}_{13}$ where elements of S are given by the ends. Vertices correspond to the V's.



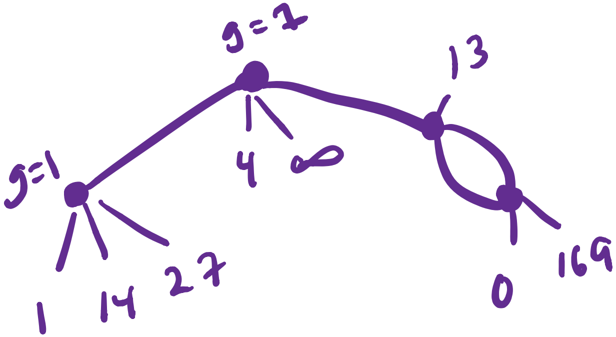
Edges correspond to annuli. This is the same combinatorial analysis as cluster pictures.
The set $\pi^{-1}(V_j)$ gives a covering of X. It has a dual graph. Now, $\pi^{-1}(V_i \cap V_j)$ is given by

$$y^2 = 1, \text{ or } y^2 = x$$

over an annulus $r \leq \|X\|_p \leq R$. Thus, it gives either one or two annuli. One if there are an odd number of elements of S on either side of the edge. Otherwise even.



Dual graph of X



Here there are 1 or 2 edges above each edge (Vertices could be doubled although they aren't in this example)

Restricting to good curves

We can automate construction of the tree by using Newton polygons and approximating roots.

Restricting from $\mathbb{P}^1$ to V is like replacing

$$y^2 = f(x) \text{ by } y^2 = g(x)\ell(x)^2$$

where $g(x)$ is a polynomial (with roots in distinct residue discs) and $\ell(x)$ is an analytic function. We are able to factor out roots away from V in pairs from $f(x)$ and then take the square root on V.

We can set $\tilde{y} = y/(\ell(x))$ and get $\tilde{y}^2 = g(x)$.

Then

$$\omega_i = \frac{x^i dx}{2y} = \frac{x^i dx}{2\tilde{y}}(\ell(x)).$$

We write a power series for $\ell(x)$ and interchange integration and summation.

Terms in the power series

A typical term in the power series expansion expansion for ω_i looks like

$$\eta = x^{n_\infty} \prod_{j=1}^{\ell} \frac{1}{(x-\beta_j)^{n_j}} \frac{dx}{2y}$$

We examine the principal parts over ∞ and β_j's to rewrite η in the form

$$\eta = dF + \sum_{i=0}^{d-2} c_i \omega_i + \sum_{j=1}^{k} d_j \nu_j$$

on $\pi^{-1}(V)$.
The principal part tells us which exact forms to subtract off to lower the order of poles (Tuitman's pole reduction algorithm) and then tells us the coefficients c_i and d_j. Fortunately, the system of linear equations is upper triangular!

Testing

We tested our algorithm by

1. Identifying torsion points on curves
2. Computing p-adic logarithms on elliptic curves.

Thank you!