Effective convergence bounds for Frobenius structures on connections

Kiran S. Kedlaya

Department of Mathematics, Massachusetts Institute of Technology; `kedlaya@mit.edu`
Department of Mathematics, University of California, San Diego

From p-adic differential equations to arithmetic algebraic geometry
on the occasion of Francesco Baldassarri's 60th birthday
Padova, February 4, 2010

Joint work with Jan Tuitman; manuscript in preparation. Slides available at `http://math.mit.edu/~kedlaya/papers/talks.shtml`.

Supported by NSF, DARPA, MIT, UCSD, MSRI.

Contents

Contents

Zeta functions

For X a scheme of finite type over $\mathbb{F}_q$,

$$\zeta_X(T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \#X(\mathbb{F}_{q^n})\right)$$

is a rational function of T (Dwork). For X given by equations, computing ζ_X from the definition is often impractical. Alternate methods are of interest both for theory (variants of mirror symmetry) and applications (elliptic/hyperelliptic curve cryptography).

Many cases of this problem can be treated well using p-adic cohomology; see the work of K., Lauder, Wan, Denef, Vercauteren, Castryck, Hubrechts, Gerkmann, Harvey, Voight, Sperber, Tuitman, Walker, Pancratz, Balakrishnan, Bradshaw...

Deformations in p-adic cohomology (after Lauder)

For $f : Y \to X$ a smooth morphism of smooth schemes over $\mathbb{Z}_p$, the relative de Rham cohomology $V = H^i_{\mathrm{dR}}(\widehat{Y}_{\mathbb{Q}_p}/\widehat{X}_{\mathbb{Q}_p})$ is a vector bundle on $\widehat{X}_{\mathbb{Q}_p}$ equipped with some extra structures: a *connection* ∇, and for each absolute Frobenius lift $\sigma : X \to X$, a *Frobenius structure* $F : \sigma^* V \cong V$ compatible with ∇. (In fact, F is *overconvergent*.)

Lauder suggests to arrange for one fibre of f to be of interest, and for another to have known Frobenius action on de Rham cohomology (e.g., because of automorphisms, or by explicit calculation). View the compatibility between F and ∇ as a differential equation for F, with initial condition given by the known fibre. Solve the DE for F, then specialize to the fibre of interest.

Deformations in practice: a general setup

In practice, one usually runs the deformation method starting from a smooth morphism $f : Y \to U$ of $\mathbb{Q}$-schemes for $U = \mathbb{P}^1_{\mathbb{Q}} - Z$. In this case, $V = H^i_{\mathrm{dR}}(Y/U)$ is a vector bundle on U equipped with a connection ∇. At each geometric point of Z, ∇ has a regular singularity with rational exponents.

By avoiding finitely many bad cases, we choose p so that:

(a) the points of Z are unramified over $\mathbb{Q}_p$ and have distinct images in $\mathbb{P}^1_{\mathbb{F}_p}$;

(b) the exponents of ∇ have denominators coprime to p;

(c) f admits a smooth integral model.

We obtain a Frobenius structure F on ∇ for the Frobenius lift $\sigma(t) = t^p$ on $\mathbb{P}^1_{\mathbb{Z}_p}$.

The pole order problem

Choose a basis for V, on which $\frac{d}{dt}, F$ act via matrices N, Φ for which

$$N\Phi + \frac{d}{dt}(\Phi) = pt^{p-1}\Phi\sigma(N).$$

The matrix N has entries in $\mathbb{Q}(t)$, does not depend on p, and may be computed (somewhat) easily. For $\lambda \in \overline{\mathbb{Q}_p}$ a Teichmüller lift, $\Phi(\lambda)$ is the matrix of Frobenius acting on the p-adic cohomology of the fibre $f_{\overline{\lambda}}$. Given $\Phi(\lambda)$ for one λ, we wish to solve for Φ and then specialize.

The entries of Φ belong to the p-adic completion of $\Gamma(U)$, and converge in some open annulus around z of outer radius 1. We wish to compute Φ modulo some p^m by solving in power series around some λ for which $\Phi(\lambda)$ is known. This can be done by computing enough terms *provided* that we can bound the poles of Φ modulo p^m at each $z \in Z$.

We have now arrived at a local problem in the (effective) theory of p-adic differential equations.

Contents

The local problem

Take z in a finite unramified extension $\mathbb{Q}_q$ of $\mathbb{Q}_p$. Let N be an $n \times n$ matrix over $\mathbb{Q}(t)$ such that $(t-z)N$ has no poles in the residue disc of z, and its reduction modulo $t-z$ has eigenvalues $\lambda_1, \dots, \lambda_n \in \mathbb{Q} \cap \mathbb{Z}_p$. Suppose that Φ is an $n \times n$ matrix over the subring of the p-adic completion of $\mathbb{Q}(t)$ consisting of series convergent in some open annulus around z of outer radius 1, and satisfies

$$N\Phi + \frac{d}{dt}(\Phi) = pt^{p-1}\Phi\sigma(N).$$

We may represent Φ as a Laurent series $\sum_{n \in \mathbb{Z}} c_n (t-z)^n$ in which for any $m \in \mathbb{Z}$, the set of n for which $v_p(c_n) \leq m$ is bounded below. We wish to find a lower bound on these n.

To make this problem well-posed, we add normalization conditions $v_p(N), v_p(\Phi) \geq 0$.

The case $z = 0$

Suppose that $z = 0$ and that $\lambda_1 = \cdots = \lambda_n = 0$. In this case, over the full ring of rigid analytic functions on the disc $|t - z| < 1$, we can find a basis on which $t\frac{d}{dt}$ acts via a nilpotent constant matrix (Dwork's trick). On such a basis, F must also act via a constant matrix. Consequently, the original matrix Φ is analytic over the disc $|t - z| < 1$, i.e., it has no poles at all!

If $z = 0$ but the λ_i are nonzero, we can reduce to the previous case by making a cyclic cover (i.e., adjoining a root of t) and then performing a *shearing transformation*. Since changing basis by U replaces Φ by $U^{-1}\Phi\sigma(U)$, we conclude that Φ is meromorphic on the disc $|t - z| < 1$ with pole order at most

$$\max_i\{\lambda_i\} - p\min_i\{\lambda_i\}.$$

Changing the Frobenius lift

If σ, σ' are two different Frobenius lifts and F is a Frobenius structure on a connection with respect to σ, one obtains a Frobenius structure F' with respect to σ' by parallel transport:

$$F' = \sum_{i=0}^{\infty} \frac{(\sigma'(t) - \sigma(t))^i}{i!} F \circ \left(\frac{d}{dt} \right)^i .$$

This preserves all rational invariants of F, e.g., the Newton polygon.

We use this formula to pass between the Frobenius lifts $\sigma(t-z) = (t-z)^p$ and $\sigma'(t) = (t)^p$. Since F is meromorphic on $|t-z| < 1$, poles at $t = z$ come from the contribution from exponents and from the simple pole of N at $t = z$.

Bounding the pole order

We may now bound the pole at $t = z$ of Φ modulo p^m by

$$\max_j\{\lambda_j\} - p\min_j\{\lambda_j\} + pi$$

for i the largest index such that the matrix of

$$\frac{(\sigma'(t) - \sigma(t))^i}{i!} F \circ \left(\frac{d}{dt}\right)^i$$

on the original basis has p-adic valuation less than m.

Since $v_p(\sigma'(t) - \sigma(t)) \geq 1$, this will give a usable bound if we check that the valuation of the matrix of action of $\frac{1}{i!} F \circ \left(\frac{d}{dt}\right)^i$ is at least $-f(i)$ for some sublinear function f of i.

Bounding using effective convergence bounds

One can bound the action of $\frac{1}{i!}F \circ \left(\frac{d}{dt}\right)^i$ in terms of the Taylor series for horizontal sections of ∇ around a generic point of radius 1. This gives a bound of the form $f(i) = c\lfloor \log_p i \rfloor$ using effective convergence bounds for solvable p-adic differential modules.

For instance, Dwork and Robba gave such a bound with $c = n - 1$. (An analogous result in the case of a disc with a singularity was given by Christol and Dwork; with some refinement, one again gets $c = n - 1$.)

A better bound has c equal to the difference between the maximum and minimum Hodge slopes of F. This is inspired by the work of Chiarellotto-Tsuzuki on Dwork's logarithmic growth problem.

Contents

Example: the Legendre family

Consider the relative de Rham cohomology of the Legendre elliptic curve

$$y^2 = x(x+1)(x+t+2)$$

and the basis

$$\frac{dx}{y^3}, \qquad \frac{x\,dx}{y^3}.$$

The resulting Picard-Fuchs equation is (up to translation) the Gaussian hypergeometric equation. It is regular with singularities at $-2, -1, \infty$.

Computations in the Legendre family

At $z = -2$, the exponents are $-2, 0$. For $p = 5, 7, 11$, we find experimentally that the pole order of Φ modulo p^m at z is at most $p(m+1) - 2$, with equality for most m.

By contrast, our upper bound is about $p(m+1) + \log_p m$. So the log term appears to be unnecessary! Similar phenomena appear in calculations with other families of elliptic and hyperelliptic curves.

In other words, it seems that logarithmic growth doesn't seem to contribute to the pole order. Is there an explanation for this?