REND. SEM. MAT. UNIV. PADOVA, Vol. 128 (2012)

Effective Convergence Bounds for Frobenius Structures on Connections

KIRAN S. KEDLAYA (*) - JAN TUITMAN (**)

ABSTRACT - Consider a meromorphic connection on $\mathbb{P}^1$ over a p-adic field. In many cases, such as those arising from Picard-Fuchs equations or Gauss-Manin connections, this connection admits a Frobenius structure defined over a suitable rigid analytic subspace. We give an effective convergence bound for this Frobenius structure by studying the effect of changing the Frobenius lift. We also give an example indicating that our bound is optimal.

1. Introduction

In recent years, much work has gone into using p-adic cohomology as an effective tool for numerical computation of zeta functions (and some related quantities) of algebraic varieties over finite fields. One important technique in this field is the *deformation method* of Lauder, in which one computes the zeta function of a variety by fitting it into a one-parameter family of varieties, constructing the associated Picard-Fuchs equation or Gauss-Manin connection, then exploiting the existence of a Frobenius structure on this differential equation to reduce the problem to another member of the family (the initial condition, so to speak). Another important technique is the *fibration method*, also introduced by Lauder, in which one uses similar techniques to compute the zeta function of the total space of a one-parameter family, again starting from a single fiber. See [4, 5] for further discussion.

(*) Indirizzo dell'A.: Department of Mathematics, University of California, San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093-0112, USA.

E-mail: kedlaya@ucsd.edu

(**) Indirizzo dell'A.: Mathematical Institute, University of Oxford, 24-29 St. Giles', Oxford OX1 3LB. UK.

E-mail: tuitman@maths.ox.ac.uk

To execute the deformation and fibration methods in practice, it is necessary to have not just the existence of a Frobenius structure, but explicit bounds on its convergence within a given residue disc. Concretely, these bounds are needed to enable the reconstruction of a rational function from a power series expansion, by bounding the degrees of its zero and pole divisors. One can often obtain crude bounds by direct calculations, but it is essential to have more accurate bounds in order to limit the required intermediate precision needed to achieve a final result to a given level of accuracy.

A technique for obtaining accurate bounds has been suggested by the first author in the preprint [3], under the assumptions (satisfied in many cases in practice) that the differential equation has at most one singularity in any residue disc, and that the exponents of the local monodromy at such a singularity are p-adically integral. The idea is to exploit the parallel transport of Frobenius structures between two choices of a Frobenius lift, to reduce the question of convergence within a given residue disc to the same question with the Frobenius lift centered around the singularity in the disc, a question which can be solved rather easily.

However, the bound given in [3, Theorem 6.5.10] is not best possible. A stronger bound was claimed in the original (2008) manuscript of [3], but the second author discovered that the proof was incomplete, as it relied on some unjustified assertions about the convergence of solutions of p-adic differential equations. In this paper, we give a corrected version of the original argument, thus giving a stronger version of [3, Theorem 6.5.10]. We also provide a numerical example which indicates that the resulting bound is sharp.

2. The theorem

We first introduce some notation and terminology.

Let p denote a prime, n a positive integer, and $\mathbb{F}_q$ the finite field with $q = p^n$ elements. We write $\mathbb{Q}_q$ for the unique unramified extension of degree n of the field of p-adic numbers $\mathbb{Q}_p$, and $\mathbb{Z}_q$ for the ring of integers of $\mathbb{Q}_q$. Let U be an open dense subscheme of $\mathbb{P}^1_{\mathbb{Q}_q}$ with nonempty complement Z. Suppose that $\mathcal{E}$ is a vector bundle on U equipped with a connection ∇, and let t denote some coordinate on $\mathbb{P}^1_{\mathbb{Q}_q}$.

We write σ for the standard p-th power Frobenius lift on $\mathbb{P}^1_{\mathbb{Q}_q}$ that is, the (semilinear) map that lifts the p-th power Frobenius map on $\mathbb{P}^1_{\mathbb{F}_q}$ and satisfies $\sigma(t) = t^p$.

Let V denote the rigid analytic subspace of $\mathbb{P}^1_{\mathbb{Q}_q}$ which is the complement of the union of the open disks of radius 1 around the points of Z, and $\mathcal{O}^\dagger(U)$ the ring of functions that converge on some strict neighbourhood of V. A *Frobenius structure* on $\mathcal{E}$ with respect to σ is an isomorphism $\mathcal{F} : \sigma^*\mathcal{E} \xrightarrow{\sim} \mathcal{E}$ of vector bundles with connection defined on some strict neighbourhood of V.

We fix a basis $[v_1, \dots, v_r]$ of sections of $\mathcal{E}$ on U, define matrices $N \in M_r(\mathcal{O}(U))$ and $\Phi \in M_r(\mathcal{O}^\dagger(U))$ such that

$$\nabla v_j = \sum_{i=1}^{r} N_{ij} v_i \otimes dt,$$

$$\mathcal{F} v_j = \sum_{i=1}^{r} \Phi_{ij} v_i,$$

and call these the matrices of ∇ and $\mathcal{F}$. Note, however, that ∇ and $\mathcal{F}$ are not $\mathcal{O}(U)$- and $\mathcal{O}^\dagger(U)$-linear, respectively. Instead, ∇ satisfies the Leibniz rule, and $\mathcal{F}$ is σ-semilinear as a map from $\mathcal{E}$ to itself.

Since $\mathcal{F}$ is a morphism of vector bundles with connection, it is horizontal with respect to ∇. This implies that the matrices N and Φ satisfy the differential equation

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

Now let z be a geometric point of Z, and suppose that the entries of N have at most a simple pole at z. When ∇ is a Gauss-Manin connection, by the regularity theorem we can always choose the basis $[v_1, \dots, v_r]$ so that this is the case (where the choice will in general depend on z). The *exponents* of ∇ at z with respect to $[v_1, \dots, v_r]$ are defined as the eigenvalues of the matrix $(t-z)N|_{t=z}$. When ∇ is a Gauss-Manin connection or admits a Frobenius structure, these are known to be rational numbers.

Let $|.|$ denote the norm on $\mathcal{O}^\dagger(U)$ induced by the supremum norm on V, and $v_p(.)$ the corresponding discrete valuation, so that $|.| = p^{-v_p(.)}$. Extend both of these to $M_r(\mathcal{O}^\dagger(U))$ in the usual way, i.e., as the maximum and minimum over the entries, respectively.

THEOREM 2.1. *Let z be an unramified geometric point of Z, and assume that Z does not contain any other points with the same reduction modulo p. Suppose that $[v_1, \dots, v_r]$ is a basis of $\mathcal{E}$ with respect to which the matrix N of ∇ has at most a simple pole at z, and the exponents $\{\lambda_1, \dots, \lambda_r\}$*

of ∇ at z are contained in $\mathbb{Q} \cap \mathbb{Z}_p$. Assume that $\mathcal{E}$ admits a Frobenius structure $\mathcal{F}$ with respect to σ, and let Φ be the matrix of $\mathcal{F}$ with respect to the basis $[v_1, \dots, v_r]$. For $i \in \mathbb{N}$, put

$$f(i) = \max\{(v_p(\Phi) + v_p(\Phi^{-1}))\lceil \log_p(i) \rceil, \qquad (r-1)v_p(N) + (v_p(\Phi) + v_p(\Phi^{-1}))\lfloor \log_p(i) \rfloor\},$$

and define

$$c = \begin{cases} 0 & \text{if } v_p(N) \geq 0 \\ \min\{0, i + f(i) : i \in \mathbb{N}\} & \text{if } v_p(N) < 0. \end{cases}$$

For $m \in \mathbb{N}$, put

$$g(m) = \max\{i \in \mathbb{N} \mid i + v_p(\Phi) + c + f(i) < m\},$$

and define

$$\alpha_1 = \lfloor -p \min_i\{\lambda_i\} + \max_i\{\lambda_i\} \rfloor,$$

$$\alpha_2 = \begin{cases} 0 & \text{if } N \text{ does not have a pole at } z, \\ 0 & \text{if } z \in \{0, \infty\}, \\ g(m) & \text{otherwise}. \end{cases}$$

Then Φ is congruent modulo p^m to a matrix of rational functions of order greater than or equal to $-(\alpha_1 + p\alpha_2)$ at z (that is, the entries of the difference between the two matrices all have p-adic valuation at least m).

The proof proceeds in several steps. We start with the following lemma.

Lemma 2.2. *Let $N = \sum_{i=-1}^{\infty} N_i t^i$ be an $r \times r$ matrix such that tN converges on the open unit disk and N_{-1} is a nilpotent matrix. Let $\Phi = \sum_{i=-\infty}^{\infty} \Phi_i t^i$ be an $r \times r$ matrix that converges on some open annulus of outer radius 1. Suppose that N, Φ satisfy equation (1). Then $\Phi_i = 0$ for all $i < 0$, so that Φ converges on the whole open unit disk.*

Proof. See [2, Proposition 17.5.1]. □

When the exponents of N at 0 are not necessarily zero, this can be generalized as follows.

Lemma 2.3. *Let $N = \sum_{i=-1}^{\infty} N_i t^i$ be an $r \times r$ matrix such that tN converges on the open unit disk and the eigenvalues $\lambda_1, \ldots, \lambda_r$ of N_{-1} are rational numbers with denominators coprime to p. Let $\Phi = \sum_{i=-\infty}^{\infty} \Phi_i t^i$ be an $r \times r$ matrix that converges on some open annulus of outer radius* 1. *Suppose that N, Φ satisfy equation* (1). *Then $\Phi_i = 0$ whenever*

$$i < p \min_j \{\lambda_j\} - \max_j \{\lambda_j\}.$$

Proof. First we may adjoin $t^{1/k}$ for k coprime to p (if necessary), to reduce to the case where $\lambda_1, \ldots, \lambda_r \in \mathbb{Z}$. In that case, by applying so-called *shearing transformations*, one can find an invertible $r \times r$ matrix W over $\mathbb{Q}_q(t)$ such that the matrix

$$N' = W^{-1} N W + W^{-1} \frac{dW}{dt}$$

still has (at most) a simple pole at $t = 0$, but now with all exponents equal to 0. Moreover, one can ensure that $t^b W$ and $t^{-a} W^{-1}$ do not have a pole at $t = 0$, for $a = \min_j \{\lambda_j\}$ and $b = \max_j \{\lambda_j\}$. More details on this can be found in [3, Lemma 5.1.6]. If we change basis to the basis given by the columns of W, then

$$\begin{aligned} &N \to N', \\ &\Phi \to \Phi' = W^{-1} \Phi \sigma(W). \end{aligned}$$

Now Lemma 2.2 can be applied to the pair N', Φ', so that $\Phi'_i = 0$ for all $i < 0$. Since $\Phi = W \Phi' \sigma(W^{-1})$, this implies that $\Phi_i = 0$ for all $i < pa - b$. □

Recall that we have chosen the standard p-th power Frobenius lift σ. However, we could just as well have chosen a different lift. The following lemma allows one to change from one Frobenius lift to another.

Lemma 2.4. *Let $\mathcal{D}$ denote the differential operator on $\mathcal{E}$ defined by $\nabla v = \mathcal{D} v \otimes dt$. Suppose that $\mathcal{E}$ admits a Frobenius structure $\mathcal{F}_1 : \sigma_1^* \mathcal{E} \xrightarrow{\sim} \mathcal{E}$ with respect to a Frobenius lift σ_1, and let σ_2 be some other Frobenius lift. Then $\mathcal{E}$ also admits a Frobenius structure $\mathcal{F}_2 : \sigma_2^* \mathcal{E} \xrightarrow{\sim} \mathcal{E}$ with respect to σ_2, defined by*

$$\mathcal{F}_2(v) = \sum_{i=0}^{\infty} (\sigma_2(t) - \sigma_1(t))^i \mathcal{F}_1\left(\frac{\mathcal{D}^i}{i!}(v)\right).$$

Proof. See [2, Proposition 17.3.1]. □

Finally, we need a bound on the matrices of the differential operators $\frac{\mathcal{D}^i}{i!}$ that appear in Lemma 2.4.

Lemma 2.5. *Let $\Delta^{(i)}$ be the matrix of the differential operator $\frac{\mathcal{D}^i}{i!}$ with respect to the basis $[v_1, \ldots, v_r]$, that is,*

$$\left(\frac{\mathcal{D}^i}{i!}\right) v_k = \sum_{j=1}^{r} \Delta_{jk}^{(i)} v_j.$$

Then we have

$$v_p(\Delta^{(i)}) \geq f(i),$$

where $f(i)$ is defined as in Theorem 2.1.

Proof. Let η denote a generic point of the disk of radius 1 around z. One can verify that the Taylor series

$$T(-t+\eta, v_j) = \sum_{i=0}^{\infty} (-t+\eta)^i \frac{\mathcal{D}^i(v_j)}{i!}$$

defines a horizontal section of ∇ that meets v_j at the point η. Form the matrix M whose j-th column consists of the expression of $T(-t+\eta, v_j)$ in terms of the basis $[v_1, \ldots, v_r]$, then expand $M = \sum_{i=0}^{\infty} M_i (t-\eta)^i$. Since ∇ does not have any singularities in the open disk of radius 1 around η, it follows from [2, Theorem 18.3.3] that

$$\min\{v_p(M_0), \ldots, v_p(M_i)\} \geq (v_p(\Phi) + v_p(\Phi^{-1}))\lceil \log_p(i) \rceil,$$

and from [2, Remark 18.3.4] (with $q = p$) that

$$\min\{v_p(M_0), \ldots, v_p(M_i)\} \geq (r-1)v_p(N) + (v_p(\Phi) + v_p(\Phi^{-1}))\lfloor \log_p(i) \rfloor.$$

Since $|\Delta^{(i)}|$ attains its maximum at η, and

$$M_i = (-1)^i \Delta^{(i)}(\eta) + (\text{terms coming from } \Delta^{(j)} \text{ with } j < i),$$

we deduce the bound by induction on i. □

Now we finally get to the proof of Theorem 2.1.

Proof of Theorem 2.1. We first note that in case $z = 0$ or $z = \infty$, the claim is clear from Lemma 2.3.

Suppose next that z is a point at which N has no pole, so that $\alpha_1 = \alpha_2 = 0$. If we use the Frobenius lift σ' with $\sigma'(t-z) = (t-z)^p$, then by Lemma 2.3 again (applied after translating z to the origin), the Frobenius matrix Φ' with respect to σ' is holomorphic at z. By Lemma 2.4 (with $\sigma_1 = \sigma', \sigma_2 = \sigma$), Φ is also holomorphic at z, proving the claim in this case.

Finally, suppose that N does have a pole at z. In this case, Lemma 2.3 implies that Φ' has order at least $-\alpha_1$ at z. We may again use Lemma 2.4 (with $\sigma_1 = \sigma', \sigma_2 = \sigma$) to convert back to the original Frobenius lift; this gives us the identity

$$\Phi = \sum_{i=0}^{\infty} p^i u^i \Phi' \sigma'(\Delta^{(i)}),$$

where $pu = (t-z)^p + \sigma(z) - t^p$ (with $v_p(u) \geq 0$), and $\Delta^{(i)}$ again denotes the matrix of the differential operator $\frac{\mathcal{D}^i}{i!}$ with respect to the basis $[v_1, \dots, v_r]$. In this identity, the summand at index i has order at least $-\alpha_1 - pi$ at z, and p-adic valuation at least $i + v_p(\Phi') + f(i)$ by Lemma 2.5. This will give the desired bound once we check that $v_p(\Phi') \geq v_p(\Phi) + c$. To see this, apply Lemma 2.4 with σ_1 and σ_2 interchanged to obtain

$$\Phi' = \sum_{i=0}^{\infty} \frac{p^i}{i!} (-u)^i \Phi \sigma(i! \Delta^{(i)}).$$

If $v_p(N) < 0$, we get the claim by invoking Lemma 2.5 again; if $v_p(N) \geq 0$, we instead note that $v_p(p^i/i!)$ and $v_p(i!\Delta^{(i)})$ are both nonnegative. □

The following corollary is often useful when the matrix N of ∇ with respect to some basis does not have a simple pole at z.

Corollary 2.6. *Suppose that $[v_1, \dots, v_r]$ is a basis for $\mathcal{E}$ as in Theorem 2.1, and let $[w_1, \dots, w_r]$ be another basis for $\mathcal{E}$, such that $v_j = \sum_{i=1}^{r} W_{ij} w_j$ with $W \in M_r(\mathbb{Q}_q(t))$. Then the matrix Φ' of $\mathcal{F}$ with respect to $[w_1, \dots, w_r]$ is congruent modulo $p^{m+v_p(W)+v_p(W^{-1})}$ to a matrix of rational functions of order greater than or equal to*

$$-(\alpha_1 + p\alpha_2(m)) + \mathrm{ord}_z(W) + p\,\mathrm{ord}_z(W^{-1})$$

at z.

Proof. The matrix Φ' satisfies

$$\Phi' = W \Phi \sigma(W)^{-1}.$$

□

REMARK 2.7. In some special cases Theorem 2.1 can still be improved a little.

1. If $\sigma(z) = z^p$ (such a z is called a *Teichmüller lift*), then $\sigma(t) - \sigma'(t)$ is divisible by $t - z$ in the proof of Theorem 2.1. So when we apply Lemma 2.4, some cancellation occurs, and modulo p^m the matrix Φ has order greater than or equal to $-(\alpha_1 + (p-1)\alpha_2(m))$ at z.

2. Suppose that $z \neq 0, \infty$. If we denote the residue matrix $(t-z)N|_{t=z}$ of N at z by R_z, and the identity matrix by I, then the leading term in the Laurent series expansion of the matrix $\Delta^{(i)}$ of $\frac{\mathcal{D}^i}{i!}$ at $(t-z)$ is given by

$$(R_z - (i-1)I)\dots(R_z - I)R_z \, \frac{(t-z)^{-i}}{i!}.$$

In many cases there exists $S \in GL_r(\mathbb{Q}_q)$ such that $S^{-1}R_zS$ is diagonal. Writing $\lambda_1, \dots, \lambda_r$ for the entries on the diagonal, the leading term can then be written as

$$S\begin{pmatrix} \frac{\lambda_1(\lambda_1-1)\dots(\lambda_1-(i-1))}{i!} & & 0 \\ & \ddots & \\ 0 & & \frac{\lambda_r(\lambda_r-1)\dots(\lambda_r-(i-1))}{i!} \end{pmatrix} S^{-1}(t-z)^{-i}.$$

However, since $\lambda_1, \dots, \lambda_r \in \mathbb{Q} \cap \mathbb{Z}_p$ by assumption, the matrix in the middle is easily seen to have entries in $\mathbb{Q} \cap \mathbb{Z}_p$ as well. This means that the valuation of the leading term in the the Laurent series expansion of $\Delta^{(i)}$ at z is bounded by $v_p(S) + v_p(S^{-1})$. Now when we apply Lemma 2.4, we see that if $g(m) + v_p(\Phi) + c + v_p(S) + v_p(S^{-1}) \geq m$, then modulo p^m the matrix Φ has order greater than or equal to $-(\alpha_1 + p(\alpha_2(m) - 1))$ at z. This is related to the improvement upon [2, Theorem 18.2.1] given by the theorem of Dwork and Robba on which it is based [1].

3. An example: a family of elliptic curves

We consider the family given by the affine equation

$$y^2 = x^3 + 1 + (t+1)(x^2 + x),$$

The closure of the zero locus of this equation in $\mathbb{P}^2_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}}$ defines a family X/U of elliptic curves over $U = \mathbb{P}^1_{\mathbb{Q}} - \{-2, 2\}$.

The relative algebraic de Rham cohomology $H^1_{dR}(X/U)$ is a vector bundle on U, and carries a natural Gauss-Manin connection ∇. Moreover, $H^1_{dR}(X/U)$ is of rank 2, and a basis is given by

$$\left[\frac{dx}{y}, \frac{xdx}{y}\right].$$

Let p be an odd prime number. The space $H^1_{dR}(X/U)$ equipped with ∇ coincides with the relative rigid cohomology $H^1_{rig}(X_p/U_p)$ of the reduction X_p/U_p of X/U modulo p, and therefore it admits a Frobenius structure $\mathcal{F}$ with respect to the standard lift σ of the p-th power Frobenius. Let N and Φ be the matrices of ∇ and $\mathcal{F}$ with respect to the above basis, respectively. We compute

$$N = \frac{1}{t^2-4}\begin{pmatrix} -\frac{t}{2}-\frac{1}{2} & \frac{t}{2}+\frac{3}{2} \\ -\frac{1}{2} & \frac{t}{2}+\frac{1}{2} \end{pmatrix}.$$

It is known that $v_p(\Phi) = 0$, and $v_p(\Phi^{-1}) = -1$ in this case, and clearly $v_p(N) = 0$, so in Theorem 2.1 we have

$$g(m) = \max\{i \in \mathbb{N} \mid i - \lfloor \log_p(i) \rfloor < m\}.$$

3.1 – $z = 2$

At $z = 2$ the exponents are $\{-1/4, 1/4\}$. The residue matrix R_2 is diagonalizable by integral matrices for $p \neq 5$. So by remark 2.7, for $p \neq 5$ the bound from Theorem 2.1 for the order of Φ modulo p^m can be improved to $-\left(\left\lfloor \frac{p+1}{4} \right\rfloor + p(g(m)-1)\right)$, while for $p = 5$ it remains $-(1 + 5g(m))$.

Experimentally, we find that for $p = 3$ the order is bounded by $1 - 3(m-1)$, for $p = 5$ it is bounded by $1 - 5(m-1)$, and for $p = 7$ it is bounded by $2 - 7(m-1)$, all for m up to 250 and with equality for many m.

3.2 – $z = -2$

At $z = -2$ the exponents are $\{0, 0\}$, so the bound from Theorem 2.1 for the order of Φ modulo p^m is given by $-pg(m)$.

Experimentally, we find that for $p=3$ the bound is sharp for $m=1,2,3,6,8,17,25,52,78,159,239$, for $p=5$ for $m=1,2,3,4,5,10,15,20,24,49,74,99,123,248$, and for $p=7$ for $m=1,2,3,4,5,6,7,14,21,28,35,42,48,97,146,195,244$, all for m up to 250.

Acknowledgments. Kedlaya was supported by NSF (CAREER grant DMS-0545904, grant DMS-1101343), DARPA (grant HR0011-09-1-0048), MIT (NEC Fund, Cecil and Ida Green professorship), and UCSD (Stefan E. Warschawski professorship). Tuitman was supported by the European Research Council (grant 204083).

REFERENCES

[1] B. Dwork - P. Robba, *Effective p-adic bounds for solutions of homogeneous linear differential equations*. Trans. Amer. Math. Soc., **259** (2) (1980), pp. 559–577.

[2] K. S. Kedlaya, *p-adic Differential Equations*. Cambridge University Press, 2010.

[3] K. S. Kedlaya, *Effective p-adic cohomology for cyclic cubic threefolds*. In Computational Algebraic and Analytic Geometry of Low-dimensional Varieties. Amer. Math. Soc., 2012. Available at http://math.mit.edu/~kedlaya/papers/.

[4] A. Lauder, *Rigid cohomology and p-adic point counting*. J. Théor. Nombres Bordeaux, **17** (2005), pp. 169–180.

[5] A. Lauder, *A recursive method for computing zeta functions of varieties*. LMS J. Comput. Math., **9** (2006), pp. 222–269.

Manoscritto pervenuto in redazione il 15 novembre 2011.