Contemporary Mathematics

Effective p-adic cohomology for cyclic cubic threefolds

Kiran S. Kedlaya

This paper is an updated form of notes from a series of six lectures given at a summer school on p-adic cohomology held in Mainz in the fall of 2008. (They may be viewed as a sequel to the author's notes from the Arizona Winter School in 2007 [**51**].) The goal of the notes is to describe how to use p-adic cohomology to make effective, provably correct numerical computations of zeta functions. More specifically, we discuss three techniques in detail:

- use of the Hodge filtration to infer the zeta function from point counts;
- the "direct cohomological method" of computing the Frobenius action on the p-adic cohomology of a single variety;
- the "deformation method" of computing the Frobenius structure on the p-adic cohomologies of a one-parameter family of varieties, using the associated Picard-Fuchs differential equation.

We demonstrate the effective nature of these methods by describing how to make them explicit for cyclic cubic threefolds, i.e., smooth cubic threefolds in $\mathbb{P}^4$ admitting an automorphism of order 3. This example has the features of being rich enough to allow us to illustrate some useful features of p-adic cohomology (e.g., behavior with respect to automorphisms, and effect of the Hodge filtration) while simple enough that the final computations are still tractable.

A number of references will be made to computations that can be made using the `Sage` open-source computer algebra system, including a numerical example over the field $\mathbb{F}_7$ to which we return frequently. We have prepared a worksheet containing all of these computations in the form of a `Sage` notebook available at the author's web site [**54**]; however, one key calculation requires the additional nonfree system `Magma` [**67**] to be installed. (It is also worth noting that our `Sage` code depends implicitly upon the commutative algebra package `Singular` [**89**], which `Sage` incorporates.) Timings quoted are based on executions on an AMD Opteron 246 (64-bit, 2 GHz) with 2 GB of RAM.

The structure of the six lectures is as follows. (Note that subsections marked "Optional" were not intended for presentation in the lectures.) In lecture 1, we recall some generalities about zeta functions of varieties over finite fields, specialize to the case of cyclic cubic threefolds, then demonstrate with the Fermat cubic

2010 *Mathematics Subject Classification.* Primary 14G10; Secondary 14F30.

The author was supported by NSF CAREER grant DMS-0545904, a Sloan Research Fellowship, and the NEC Fund of the MIT Research Support Committee.

and with a more generic example over $\mathbb{F}_7$. In lecture 2, we recall the formalism of algebraic de Rham cohomology, then make it explicit for cyclic cubic threefolds. In lecture 3, we recall the formalism of p-adic cohomology, including the divisibilities imposed on the zeta function by the Hodge filtration; we then apply this knowledge to our generic example of a cyclic cubic threefold, and fully recover the zeta function. In lecture 4, we describe how to directly compute the Frobenius action on the p-adic cohomology of a variety, and illustrate using our generic example; however, we do not include a computational demonstration because the method we had in mind at the time of preparation of these notes appears to be infeasible. (It subsequently became clear that this difficulty is not insurmountable; see Remark 4.4.8.) In lecture 5, we introduce relative de Rham cohomology and Picard-Fuchs-Manin (Gauss-Manin) connections, and compute an example for a pencil of cyclic cubic threefolds including our generic example. In lecture 6, we describe Frobenius structures on Picard-Fuchs-Manin connections, compute the Frobenius structure for the connection from the previous lecture, and recover the zeta function of our generic example. The appendix contains many references and remarks omitted from the main text in order to streamline the exposition.

Acknowledgments. Thanks to Duco van Straten, Ralf Gerkmann, and Kira Samol for organizing the summer school in Mainz, supported by SFB/TR 45 "Periods, Moduli Spaces, and Arithmetic of Algebraic Varieties". Thanks to Jim Carlson for the suggestion to consider cyclic cubic threefolds, to Alan Lauder for helpful discussions about Frobenius structures on connections, and to Jan Tuitman for pointing out an error in our original analysis of t-adic precision (now resolved in [**56**]).

1. Zeta functions: generalities

In this lecture, we recall the notion of the zeta function of an algebraic variety, and the formalism of Weil cohomology theories which can be used to interpret the Weil conjectures on zeta functions. We illustrate by computing the zeta function of the Fermat cubic threefold over $\mathbb{F}_7$; this example will be needed later as an initial condition for solving a Picard-Fuchs-Manin connection.

1.1. Zeta functions of algebraic varieties.

Definition 1.1.1. Let X be a variety (reduced separated scheme of finite type) over the finite field $\mathbb{F}_q$. The *zeta function* of X is the formal power series

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

we can also write $\zeta_X(T)$ as an Euler product

$$\zeta_X(T) = \prod_{x \in X} (1 - T^{[\kappa_x : \mathbb{F}_q]})^{-1}$$

over closed points x of X (where κ_x denotes the residue field of x), so $\zeta_X(T) \in \mathbb{Z}[\![T]\!]$.

Remark 1.1.2. One motivation for computing zeta functions of varieties over finite fields is that they can be used to compute L-functions of varieties over number fields, which carry enormous amounts of global arithmetic information. For

instance, for E an elliptic curve over $\mathbb{Q}$, for p a prime of good reduction, we have

$$\zeta_{E_{\mathbb{F}_p}}(T) = \frac{L_p(T)}{(1-T)(1-pT)}$$

for $L_p(T)$ a polynomial of the form $1 - a_pT + pT^2$. (Note that a_p can be computed as $p + 1 - \#E(\mathbb{F}_p)$.) For an appropriate definition of $L_p(T)$ for p not of good reduction, the L-function of an elliptic curve over $\mathbb{Q}$ is defined as the product

$$L(E, s) = \prod_p L_p(p^{-s}).$$

This product converges absolutely for $\mathrm{Real}(s) > 3/2$, but is now known to extend to an analytic function on all of $\mathbb{C}$. The conjecture of Birch and Swinnerton-Dyer predicts that the order of vanishing of $L(E, s)$ at $s = 1$ equals the rank of the group $E(\mathbb{Q})$ of rational points of E.

The methods developed in this paper can be used in particular to compute zeta functions for cyclic cubic threefolds. In subsequent work, we plan to use these techniques to gather some data concerning L-functions of cyclic cubic threefolds over $\mathbb{Q}$.

1.2. The Weil conjectures. The following theorem encompasses what were formerly (and still commonly) called the *Weil conjectures*. For historical details, see the references in the appendix.

THEOREM 1.2.1. *Let X be a variety (separated scheme of finite type) over the finite field $\mathbb{F}_q$. Then the zeta function of X is the power series representation of a rational function in T. Moreover, if X is smooth and proper over $\mathbb{F}_q$, then there is a unique way to write*

$$\zeta_X(T) = \prod_{i=0}^{2\dim(X)} P_i(T)^{(-1)^{i+1}} \tag{1.2.1.1}$$

for some polynomials $P_i(T) \in \mathbb{Z}[T]$ with $P_i(0) = 1$, satisfying the following conditions.

(i) *We have*

$$P_i(1/(q^iT)) = \pm q^{-i\deg(P_i)/2} T^{-\deg(P_i)} P_i(T),$$

with the sign being $+$ whenever i is odd. In other words, the roots of P_i are invariant under the map $r \mapsto q^{-i}/r$, and if i is odd then the multiplicities of $\pm q^{-i/2}$ are even.

(ii) *The roots of P_i in $\mathbb{C}$ all have complex absolute value $q^{-i/2}$. (This is commonly called the* Riemann hypothesis *for zeta functions of varieties over finite fields.)*

(iii) *If $X \cong \mathfrak{X}_{\mathbb{F}_q}$ for some smooth proper scheme $\mathfrak{X}$ over the local ring $R = \mathfrak{o}_{K,\mathfrak{p}}$ for some number field K and some prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$ with residue field $\mathbb{F}_q$, then for any embedding $K \hookrightarrow \mathbb{C}$,*

$$\deg(P_i) = \dim_{\mathbb{C}} H^i((\mathfrak{X} \times_R \mathbb{C})^{\mathrm{an}}, \mathbb{C}).$$

In other words, $\deg(P_i)$ equals the i-th Betti number of $\mathfrak{X} \times_R \mathbb{C}$.

REMARK 1.2.2. Using p-adic cohomology, one can refine assertion (iii) of Theorem 1.2.1 to take into account the Hodge numbers of X in addition to the Betti numbers. See Theorem 3.3.1.

When computing zeta functions, it will be helpful to account for the Riemann hypothesis using the following lemma from [**50**] (applied to the reverse of one of the P_i).

LEMMA 1.2.3. *Given positive integers q, d, j, and complex numbers $a_1, \dots, a_{j-1}$, there exists a certain explicit disc of radius $\frac{d}{j} q^{j/2}$ which contains every a_j for which we can choose $a_{j+1}, \dots, a_d \in \mathbb{C}$ so that the polynomial*

$$R(T) = 1 + \sum_{j=1}^{d} a_j T^j$$

has all roots on the circle $|T| = q^{-1/2}$.

By contrast, bounding a_{d-j} directly gives the far inferior bound

$$|a_{d-j}| \leq \binom{d}{j} q^{j/2}.$$

PROOF. Let s_j denote the sum of the $(-j)$-th powers of the roots of R. From the Newton-Girard identities,

$$s_j + j a_j = -\sum_{h=1}^{j-1} s_{j-h} a_h;$$

given $a_1, \dots, a_{j-1}$, we may explicitly compute $s_1, \dots, s_{j-1}$. Since $|s_j| \leq d q^{j/2}$, this limits a_j to an explicit disc of radius $\frac{d}{j} q^{j/2}$. □

REMARK 1.2.4. The bound in Lemma 1.2.3 is typically not very tight except when j is very small. See Remark 4.3.3 for an example in the context of these lectures, and [**50**] for additional examples.

1.3. Weil cohomology. We now recall Weil's proposed cohomological interpretation of Theorem 1.2.1. Our discussion is quite incomplete; see the references in the appendix for further details.

DEFINITION 1.3.1. Fix a finite field $\mathbb{F}_q$ and a field F of characteristic zero. A *Weil cohomology* over F consists of a collection of contravariant functors $H^i(\cdot)$ from smooth proper varieties X over $\mathbb{F}_q$ to finite dimensional F-vector spaces, satisfying a number of additional conditions which we will not list completely (see [**57**] for a full account). Instead, we will simply enumerate the ones we need as we use them.

For one, $H^i(X)$ is canonically isomorphic to $H^i(X_{\mathbb{F}_{q^n}})$ for any n. For another, if we let $F_q : X \to X$ denote the q-power Frobenius, and put

$$P_i(T) = \det(1 - T F_q, H^i(X)) \qquad (i = 0, \dots, 2\dim(X)),$$

then we must have that $P_i(T) \in \mathbb{Z}[T]$ and (1.2.1.1) holds. This last claim is equivalent to the *Lefschetz trace formula*: for any positive integer n,

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{Trace}(F_q^n, H^i(X)). \tag{1.3.1.1}$$

(This equivalence requires the coefficient field to have characteristic zero.)

We will make extensive use of a slightly stronger form of (1.3.1.1): for any automorphism ι of X,

$$\#\{x \in X(\overline{\mathbb{F}_q}) : (F_q \circ \iota)(x) = x\} = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{Trace}(F_q \circ \iota, H^i(X)). \tag{1.3.1.2}$$

Remark 1.3.2. The existence of a Weil cohomology, plus the Lefschetz trace formula (1.3.1.1), together imply the rationality of $\zeta_X(T)$. To deduce property (i) in Theorem 1.2.1, one needs Poincaré duality for Weil cohomology. For property (iii), one needs a comparison theorem between the given Weil cohomology and singular cohomology over $\mathbb{C}$. Property (ii) lies somewhat deeper; we will not discuss its proof here.

Remark 1.3.3. The Lefschetz trace formula (1.3.1.2) can be extended to more general endomorphisms, and even to correspondences, but the counting function on the left side must be replaced by a more complicated sum of local terms. In the case of $F_q \circ \iota$, the graph of the morphism has transverse intersection with the diagonal inside $X \times_{\mathbb{F}_q} X$, so the fixed points are isolated and occur with multiplicity 1. One other case in which one can describe the trace formula is for an automorphism of order prime to the characteristic of $\mathbb{F}_q$; in that case, the left side of the Lefschetz formula becomes the Euler characteristic of the fixed locus.

Remark 1.3.4. The first Weil cohomology to be constructed was *étale cohomology*, in which the coefficient field may be taken to be the ℓ-adic numbers $\mathbb{Q}_\ell$ for any prime ℓ distinct from the characteristic of K. See appendix for references.

1.4. Cyclic cubic threefolds. We now specialize the discussion to the particular class of varieties we will be using as examples in this paper.

Definition 1.4.1. Let K be a field of characteristic not equal to 3. A *cyclic cubic threefold* over K is a hypersurface of degree 3 in $\mathbb{P}^4_K$ invariant under the action of a cyclic group of order 3. Throughout these notes, when discussing cyclic cubic threefolds, we will take homogeneous coordinates w, x, y, z, a on $\mathbb{P}^4_K$ and restrict to cyclic cubic threefolds defined by polynomials of the form $S = a^3 - Q$ with $Q \in K[w, x, y, z]$ homogeneous of degree 3. (This is the most general form for K algebraically closed.)

Lemma 1.4.2. *The cyclic cubic threefold defined by $S = a^3 - Q$ is smooth if and only if the cubic surface in $\mathbb{P}^3_K$ defined by Q is smooth.*

Proof. Let S_w denote the partial derivative of the polynomial S with respect to the variable w, and so forth. Then

$$(S, S_w, S_x, S_y, S_z, S_a) = (a^3 - Q, Q_w, Q_x, Q_y, Q_z, 3a^2),$$

so the saturation of this ideal contains a and hence Q. Consequently, this ideal contains a power of (w, x, y, z, a) if and only if (Q, Q_w, Q_x, Q_y, Q_z) contains a power of (w, x, y, z). In other words, $(S, S_w, S_x, S_y, S_z, S_a)$ defines the empty subscheme of $\operatorname{Proj} K[w, x, y, z, a]$ if and only if (Q, Q_w, Q_x, Q_y, Q_z) defines the empty subscheme of $\operatorname{Proj} K[w, x, y, z]$; this is the desired result. □

Observation 1.4.3. Let X be a cyclic cubic threefold over $\mathbb{F}_q$. By the Lefschetz hyperplane section property of a Weil cohomology, for $i = 0, 1, 2, 4, 5, 6$, we have

a canonical isomorphism $H^i(X) \cong H^i(\mathbb{P}^3_{\mathbb{F}_q})$. Thus the zeta function of X has the form

$$\zeta_X(T) = \frac{P(T)}{(1-T)(1-qT)(1-q^2T)(1-q^3T)}$$

for $P(T) = \det(1 - TF_q, H^3(X))$. We will show using algebraic de Rham cohomology (see Observation 2.3.1) that the middle Betti number of any lift of X is 10, so $\dim H^3(X) = \deg(P) = 10$. It will then follow that

$$P(1/(q^3T)) = q^{-15}T^{-10}P(T),$$

and the complex roots of P lie on the circle $|T| = q^{-3/2}$.

Definition 1.4.4. Given a choice of a primitive cube root $\zeta_3 \in K$, we write $[\zeta_3]$ for the automorphism

$$[\zeta_3]([w : x : y : z : a]) = [w : x : y : z : \zeta_3 a]$$

on any cyclic cubic threefold X over K. In case $K = \mathbb{F}_q$ with $q \equiv 1 \pmod 3$, $[\zeta_3]$ splits $H^3(X)$ into two eigenspaces of dimension 5, on which $[\zeta_3]$ acts by multiplication by the two primitive cube roots of 1 in the coefficient field. (This will be apparent for rigid cohomology from the explicit description we will give; for an arbitrary Weil cohomology, this can be deduced from the Lefschetz trace formula for the automorphisms $[\zeta_3]$ and $[\zeta_3]^2$, as described in Remark 1.3.3.) Consequently, $P(T)$ factors over $\mathbb{Z}[\zeta_3]$ into two factors of degree 5.

In case $K = \mathbb{F}_q$ with $q \equiv 2 \pmod 3$, $[\zeta_3]$ is not defined over $\mathbb{F}_q$, so it does not commute with F_q; rather, we have $F_q \circ [\zeta_3] = [\zeta_3]^2 \circ F_q$. In fact, we may see explicitly that $\#X(\mathbb{F}_q) = \#\mathbb{P}^3(\mathbb{F}_q)$: for each w, x, y, z, the equation $a^3 = Q(w, x, y, z)$ has exactly one solution $a \in \mathbb{F}_q$. Hence $\mathrm{Trace}(F_q, H^3(X)) = 0$, and similarly for any odd power of F_q. This forces $P(T)$ to be a polynomial of degree 5 in T^2, which we can recover by computing the zeta function of $X_{\mathbb{F}_{q^2}}$. We will thus concentrate mainly on the case $q \equiv 1 \pmod 3$ hereafter.

Remark 1.4.5. The dichotomy we have just encountered is analogous to the situation of an elliptic curve with complex multiplication. In that case, whether the curve has ordinary or supersingular reduction is determined by whether the prime of reduction is split or inert in the CM field.

1.5. A special example: the Fermat cubic threefold. As an explicit illustration of the properties of zeta functions, we compute the action of Frobenius on the Weil cohomology of a very special cubic threefold.

Definition 1.5.1. Let K be a field of characteristic not equal to 3. The *Fermat cubic threefold* over K is the threefold X in $\mathbb{P}^4_K$ defined by the polynomial $w^3 + x^3 + y^3 + z^3 + a^3 = 0$; we will identify it with the cyclic cubic threefold defined by $S = a^3 - Q$ for $Q = w^3 + x^3 + y^3 + z^3$.

If K contains a primitive cube root ζ_3, the analysis of the Fermat cubic threefold is aided greatly by the action of the group $G = \mu_3^5$ acting by

$$(\zeta_3^{c_0}, \dots, \zeta_3^{c_4})[w : x : y : z : a] = [\zeta_3^{c_0} w : \cdots : \zeta_3^{c_4} a].$$

This action on X factors through the quotient by the diagonal subgroup generated by $(\zeta_3, \dots \zeta_3)$. However, we prefer to use G instead of the quotient so we can have also an action on homogeneous polynomials.

PROCEDURE 1.5.2. Consider the Fermat cubic threefold X over $\mathbb{F}_q$ with $q \equiv 1 \pmod 3$; then the action of G is defined over $\mathbb{F}_q$, so it commutes with F_q. We can then compute the trace of F_q on each of the eigenspaces of $H^3(X)$ for G using the Lefschetz trace formula (1.3.1.2), as follows.

Choose a cubic nonresidue r in $\mathbb{F}_q$ with $\zeta_3 = r^{(q-1)/3}$. Fix also a cube root $r^{1/3}$ of r in $\overline{\mathbb{F}_q}$. For $c = (\zeta_3^{c_0}, \dots, \zeta_3^{c_4}) \in G$ with $c_4 = 0$, put

$$\tilde{P}_c = r^{-c_0} w^3 + r^{-c_1} x^3 + r^{-c_2} y^3 + r^{-c_3} z^3$$

and let $\tilde{X}_c$ denote the corresponding cyclic cubic threefold.

The variety $\tilde{X}_c$ is a *twist* of X; that is, it is isomorphic to X over $\overline{\mathbb{F}_q}$. Specifically, we may identify the $\overline{\mathbb{F}_q}$-points of X with those of $\tilde{X}_c$ via the map

$$[w : x : y : z : a] \mapsto [r^{c_0/3} w : r^{c_1/3} x : r^{c_2/3} y : r^{c_3/3} z : a].$$

Under this identification, the fixed points of $F_q \circ c$ on X are identified with the fixed points of F_q on $\tilde{X}_c$. Thus (1.3.1.2) may be rewritten in this case as

$$\begin{aligned} \#\tilde{X}_c(\mathbb{F}_q) &= \sum_{i=0}^{6} (-1)^i \operatorname{Trace}(F_q \circ c, H^i(X)) \\ &= 1 + q + q^2 + q^3 - \operatorname{Trace}(F_q \circ c, H^3(X)). \end{aligned}$$

We can thus compute $\operatorname{Trace}(F_q \circ c, H^3(X))$ by counting the points of $\#\tilde{X}_c(\mathbb{F}_q)$. For q small, we may as well do this by enumerating the points themselves; for some procedures that make more sense when q is large, see Procedure 1.7.1 and Remark 1.7.3.

We may describe the character group $\widehat{G}$ of G as $(\mathbb{Z}/3\mathbb{Z})^5$, where the character $(d_0, \dots, d_4) : G \to \mu_3$ acts as

$$(d_0, \dots, d_4)(\zeta_3^{c_0}, \dots, \zeta_3^{c_4}) = \zeta_3^{c_0 d_0 + \cdots + c_4 d_4}.$$

Given a primitive cube root of unity $\zeta_{3,F} \in F$, we may embed μ_3 into F and separate $H^3(X)$ into eigenspaces for the characters of G. In particular, for the eigenspace corresponding to the character $d = (d_0, \dots, d_4) \in (\mathbb{Z}/3\mathbb{Z})^5$, we compute the trace on that eigenspace as

$$\frac{1}{3^4} \sum_{c_0, c_1, c_2, c_3 = 0}^{2} \zeta_3^{-c_0 d_0 - c_1 d_1 - c_2 d_2 - c_3 d_3} \operatorname{Trace}(F_q \circ c, H^3(X)).$$

EXAMPLE 1.5.3. For $q = 7$, we may carry out Procedure 1.5.2 by explicitly counting the $\mathbb{F}_7$-points of all of the $\tilde{X}_c$ (see worksheet). We fix the cube root $\zeta_3 = 2$ in $\mathbb{F}_7$. For the eigenspaces corresponding to the characters

(1.5.3.1) $\quad (2,1,1,1,1), (1,2,1,1,1), (1,1,2,1,1), (1,1,1,2,1), (2,2,2,2,1),$

(1.5.3.2) $\quad (1,1,1,1,2), (1,2,2,2,2), (2,1,2,2,2), (2,2,1,2,2), (2,2,2,1,2),$

we obtain the traces

(1.5.3.3) $\quad 21\zeta_{3,F} + 7, \quad 21\zeta_{3,F} + 7, \quad 21\zeta_{3,F} + 7, \quad 21\zeta_{3,F} + 7, \quad -21\zeta_{3,F} - 14,$

(1.5.3.4) $\quad 21\zeta_{3,F}^2 + 7, \quad 21\zeta_{3,F}^2 + 7, \quad 21\zeta_{3,F}^2 + 7, \quad 21\zeta_{3,F}^2 + 7, \quad -21\zeta_{3,F}^2 - 14,$

respectively. It follows that each of these eigenspaces is one-dimensional, there are no other eigenspaces, and the polynomial $P(T)$ in the zeta function of X equals the product of $1 - \alpha T$ for α running over the values in (1.5.3.3) and (1.5.3.4).

REMARK 1.5.4. One has the same eigenspace decomposition, with the same characters, for any $q \equiv 1 \pmod 3$. For a general Weil cohomology, this can be proved using the Lefschetz trace formula for the elements of G (Remark 1.3.3; compare Definition 1.4.4). For rigid cohomology, this will follow from an explicit description using algebraic de Rham cohomology (Example 2.3.2) and the comparison theorem with rigid cohomology (Theorem 3.2.1).

REMARK 1.5.5. The general formalism of Weil cohomologies does not provide a specific way to match up the primitive cube roots of unity in $\mathbb{F}_q$ and F. We will see later that the formalism of p-adic cohomology does provide such a matching.

1.6. A generic example. We now introduce a less special example, to which we will return throughout the lectures.

EXAMPLE 1.6.1. Consider the polynomial

$$Q = w^3 + x^3 + y^3 + z^3 + (w+x)(w+2y)(w+3z) + 3xy(w+x+z)$$

over $\mathbb{F}_7$. One computes (see worksheet) that the Jacobian ideal (Q_w, Q_x, Q_y, Q_z) of Q is zero-dimensional, so Q is nonsingular. Consequently, we have a cyclic cubic threefold X over $\mathbb{F}_7$ with defining equation $S = a^3 - Q$.

We fix the choice $\zeta_3 = 2$ in $\mathbb{F}_7$, and let $\zeta_{3,F}$ be a primitive cube root of 1 in the coefficient field F. Let H_1, H_2 be the eigenspaces of $[\zeta_3]$ on $H^3(X)$ with eigenvalues $\zeta_{3,F}, \zeta_{3,F}^2$, respectively. Let $b \in \mathbb{F}_7$ be a cubic nonresidue with $b^{(7-1)/3} = 2$, and fix a cube root $b^{1/3}$ of b in $\overline{\mathbb{F}_q}$. As in Procedure 1.5.2, for $k = 0, 1, 2$, we identify the $\mathbb{F}_q$-rational points of the cubic threefold $X_{q,k}$ defined by $b^{-k}a^3 - Q$ with the fixed points of $F_q \circ [\zeta_3]^k$, via the map

$$[w : x : y : z : a] \mapsto [w : x : y : z : b^{-k/3}a].$$

Using the extended Lefschetz trace formula (1.3.1.2), we find that for $j = 1, 2$,

$$\mathrm{Trace}(F_q, H_j) = -\frac{1}{3}\sum_{k=0}^{2} \zeta_{3,F}^{-jk} \# X_{q,k}(\mathbb{F}_q).$$

By enumerating points (see worksheet), we obtain the following table after about 15 minutes of computation. (Note that we infer the counts for $k = 2$ from the other two columns, using the fact that each row must sum to $3(q^3 + q^2 + q + 1)$.)

$\#X_{q,k}(\mathbb{F}_q)$	$k=0$	$k=1$	$k=2$
$q = 7$	407	365	428
$q = 7^2$	120933	118728	120639
$q = 7^3$	40464740	40484291	40465769

We thus obtain the series approximations

$$\det(1 - TF_q, H_1) = 1 + (3\zeta_{3,F} + 2)(7T) + (8\zeta_{3,F} + 5)(7T)^2 + (7\zeta_{3,F} - 14)(7T)^3 + O(T^4)$$
$$\det(1 - TF_q, H_2) = 1 + (3\zeta_{3,F}^2 + 2)(7T) + (8\zeta_{3,F}^2 + 5)(7T)^2 + (7\zeta_{3,F}^2 - 14)(7T)^3 + O(T^4).$$

Since each of these is a polynomial of degree 5, we do not have enough data from the point counts alone to determine $\zeta_X(T)$. This would remain true even if we computed a fourth row of the table; we estimate that this would have taken us about one week of computation. (We did not attempt to combine this data with the Riemann hypothesis bound using Lemma 1.2.3; see appendix for discussion.)

1.7. Optional: Counting points on diagonal threefolds. For completeness, we describe some more intelligent procedures for counting points on diagonal cubic threefolds. We start with a procedure that is still simple but improves greatly upon counting points directly for q of moderate size.

PROCEDURE 1.7.1. Recall that we wish to count the $\mathbb{F}_q$-points of the twisted Fermat cubic threefold $\tilde{X}_c$ corresponding to the polynomial

$$\tilde{P} = r^{-c_0}w^3 + r^{-c_1}x^3 + r^{-c_2}y^3 + r^{-c_3}z^3,$$

for $q \equiv 1 \pmod 3$. For $j, j' \in \mathbb{Z}$, let $a_{j,j'}$ be the number of $x \in \mathbb{F}_q^\times$ such that $r^j x^3 + 1$ equals $r^{j'}$ times a nonzero cubic residue; this only depends on j, j' modulo 3. The $a_{j,j'}$ can be computed using cubic Jacobi sums (see Remark 1.7.3 for the case $q = p$); for now, we instead compute $a_{0,1}, a_{0,2}$ by iterating over all $x \in \mathbb{F}_q$, then use the identities

$$a_{j,j'} = a_{j',j}$$
$$a_{j,j'} = a_{-j,j'-j}$$
$$\sum_{j'} a_{j,j'} = \begin{cases} q-4 & j \equiv 0 \pmod 3 \\ q-1 & j \not\equiv 0 \pmod 3 \end{cases}$$

to infer the other $a_{j,j'}$.

For $i \in \{0,1,2,3,4\}$ and $j \in \{0,1,2\} \cup \{*\}$, put

$$C_{i,j} = \#\left\{(u_0, \dots, u_i) \in \mathbb{F}_q^{i+1} : r^{-c_0}u_0^3 + \cdots + r^{-c_i}u_i^3 \in \begin{cases} r^{-j}(\mathbb{F}_q^\times)^3 & j = 0,1,2 \\ \{0\} & j = * \end{cases}\right\}.$$

For $i = 0,1,2,3,4$ in succession, we compute the $C_{i,j}$ for all j as follows. For $i = 0$, we have

$$C_{0,*} = 1, \qquad C_{0,j} = \frac{q-1}{3} \quad (j = 0,1,2).$$

Given the $C_{i-1,j}$ for some $i > 0$, we compute

$$C_{i,j} = C_{i-1,j} + \sum_{k=0,1,2} C_{i-1,k}a_{c_i-k,c_i-j} + \begin{cases} (q-1)C_{i-1,*} & j \equiv c_i \pmod 3 \\ 0 & j \not\equiv c_i \pmod 3 \end{cases}$$
$$C_{i,*} = C_{i-1,*} + 3C_{i-1,c_i}.$$

Then we have

$$\tilde{X}(\mathbb{F}_q) = \frac{1}{q-1}(C_{4,0} - 1).$$

OBSERVATION 1.7.2. If $q \equiv 2 \pmod 3$, there is no need to count anything over $\mathbb{F}_q$ because all diagonal cubics have as many points as projective space itself. However, one may wish to carry out Procedure 1.7.1 over $\mathbb{F}_{q^2}$. In this case, the base calculation of $a_{j,j'}$ is made somewhat easier by the fact that $a_{0,1} = a_{0,2}$. Hence it suffices to calculate $a_{0,0}$, but this is also easy: since the elliptic curve $x^3 + 1 = y^3$ over $\mathbb{F}_q$ has zeta function

$$\frac{1 + qT^2}{(1-T)(1-qT)} \qquad (q \equiv 2 \pmod 3),$$

we have

$$a_{0,0} = \frac{q^2 + 2q - 8}{3}, \qquad a_{0,1} = a_{0,2} = \frac{q^2 - q - 4}{3}.$$

We next describe a computation of the $a_{j,j'}$ based on cubic Jacobi sums in the case $q = p \equiv 1 \pmod 3$.

REMARK 1.7.3. For two Dirichlet characters χ_1, χ_2 on $\mathbb{F}_p$, define the *Jacobi sum*

$$J(\chi_1, \chi_2) = \sum_{u,v \in \mathbb{F}_p : u+v=1} \chi_1(u)\chi_2(v)$$

We may interpret $3a_{j,j'}$ as the number of pairs $(x, y) \in (\mathbb{F}_p^\times)^2$ for which $r^j x^3 + r^{j'} y^3 = 1$. Let χ be the cubic Dirichlet character on $\mathbb{F}_p$ sending r to ζ_3. Then

$$\begin{aligned}
&\#\{(x,y) \in \mathbb{F}_p^2 : r^j x^3 + r^{j'} y^3 = 1\} \\
&\quad = \sum_{u+v=1} \sum_{i=0}^{2} \zeta_3^{-ij} \chi^i(u) \sum_{i'=0}^{2} \zeta_3^{-i'j'} \chi^{i'}(v) \\
&\quad = \sum_{i,i'} \zeta_3^{-ij-i'j'} J(\chi^i, \chi^{i'}) \\
&\quad = q - \zeta_3^{-j-2j'} - \zeta_3^{-2j-j'} + \zeta_3^{-j-j'} J(\chi,\chi) + \zeta_3^{-2j-2j'} J(\chi^2, \chi^2),
\end{aligned}$$

where the last line follows from the one before by standard identities [**42**, §8.3, Theorem 1]. By [**3**, Theorem 3.1.3], we have

$$J(\chi,\chi) = \frac{1}{2}(\alpha + i\beta\sqrt{3})$$

where α, β are uniquely determined by the requirements

$$\begin{aligned}
\alpha^2 + 3\beta^2 &= 4p \\
\alpha &\equiv 1 \pmod 3 \\
\beta &\equiv 0 \pmod 3 \\
3\beta &\equiv (2r^{(p-1)/3} + 1)\alpha \pmod p.
\end{aligned}$$

These α and β can be found in time polylogarithmic in p, e.g., by performing the Euclidean algorithm on p and $\tilde{r}^{(p-1)/3} - \zeta_3$ in $\mathbb{Z}[\zeta_3]$ for any $\tilde{r} \in \mathbb{Z}$ lifting r.

REMARK 1.7.4. In the case $q = p$, an explicit (but complicated) formula to compute the $C_{i,j}$ directly can be found in [**3**, Theorem 10.6.1].

2. Algebraic de Rham cohomology

We next describe the formalism of algebraic de Rham cohomology, then specialize to the case of cyclic cubic threefolds. This will be used for our explicit descriptions of p-adic cohomology in the next lecture.

2.1. Cohomology of smooth varieties. We first recall the definition of algebraic de Rham cohomology for smooth varieties.

DEFINITION 2.1.1. Let X be a smooth variety over a field K of characteristic 0. Let $\Omega_{X/K}$ be the sheaf of Kähler differentials; since X is smooth, by the Jacobian criterion $\Omega_{X/K}$ is coherent and locally free of rank $\dim(X/K)$. Let $\Omega^i_{X/K}$ be the i-th exterior power of $\Omega_{X/K}$ over the structure sheaf $\mathcal{O}_{X/K}$, so in particular $\Omega^0_{X/K} = \mathcal{O}_{X/K}$ and $\Omega^1_{X/K} = \Omega_{X/K}$. There is a universal derivation $d : \mathcal{O}_{X/K} \to \Omega_{X/K}$,

using which we obtain maps $d : \Omega^i_{X/K} \to \Omega^{i+1}_{X/K}$ satisfying $d \circ d = 0$. We thus obtain the *de Rham complex* of sheaves

$$0 \to \Omega^0_{X/K} \to \Omega^1_{X/K} \to \cdots .$$

The *algebraic de Rham cohomology* $H^i_{\mathrm{dR}}(X)$ of X is defined to be the hypercohomology $\mathbb{H}^i(\Omega^{\cdot}_{X/K})$ of this complex. If X is affine, this coincides with the cohomology of the complex of global sections (so in particular $H^i_{\mathrm{dR}}(X)$ vanishes for $i > \dim(X)$); otherwise the coherent cohomology of each $\Omega^{\cdot}_{X/K}$ intervenes, so we only have the weaker vanishing result that $H^i_{\mathrm{dR}}(X) = 0$ for $i > 2\dim(X)$.

By recalling how to compute hypercohomology, we identify an important extra structure on de Rham cohomology.

Definition 2.1.2. Let $\{U_l\}$ be a finite cover of X by affine open subschemes. Let $C^{i,j}$ be the j-th term of the Čech complex (with differentials $\check{d}$) associated to the sheaf $\Omega^i_{X/K}$ and the cover $\{U_l\}$. We may view $C^{i,j}$ as a double complex with differentials d and $\check{d}$; the total complex with differential on $C^{i,j}$ given by $d + (-1)^i \check{d}$ computes the hypercohomology $\mathbb{H}^i(\Omega^{\cdot}_{X/K}) = H^i_{\mathrm{dR}}(X)$.

More precisely, $H^i_{\mathrm{dR}}(X)$ consists of classes supported on $C^{s,i-s}$ for $s = 0, \dots, i$. We may define a descending filtration $\mathrm{Fil}^j H^i_{\mathrm{dR}}(X)$ by taking classes supported only on $C^{s,i-s}$ for $s = j, \dots, i$; this defines the *Hodge filtration* on $H^i_{\mathrm{dR}}(X)$, which turns out to be independent of the choice of the affine covering. For instance, $\mathrm{Fil}^i H^i_{\mathrm{dR}}(X)$ consists of classes represented by holomorphic i-forms on X. More generally, $\mathrm{Fil}^j H^i_{\mathrm{dR}}(X)$ is the image in $H^i_{\mathrm{dR}}(X)$ of the hypercohomology of the truncated de Rham complex

$$0 \to \Omega^j_{X/K} \to \cdots \to \Omega^{\dim(X)}_{X/K} \to 0$$

in which $\Omega^h_{X/K}$ is still placed in degree h.

Theorem 2.1.3 (Grothendieck). *Given an embedding $K \hookrightarrow \mathbb{C}$, we obtain canonical isomorphisms from $H^i_{\mathrm{dR}}(X) \otimes_K \mathbb{C}$ to the following:*

- *the singular cohomology of X with coefficients in $\mathbb{C}$;*
- *the smooth de Rham cohomology of X with coefficients in $\mathbb{C}$;*
- *the holomorphic de Rham cohomology (Dolbeaut cohomology) of X.*

Moreover, the Hodge filtration on algebraic de Rham cohomology coincides with Hodge's filtration on smooth de Rham cohomology (defined using harmonic forms).

Remark 2.1.4. Hodge actually defined a decomposition, not just a filtration, on smooth de Rham cohomology. However, only the filtration admits an algebraic description.

2.2. The Griffiths-Dwork construction. In general, computing the algebraic de Rham cohomology of a nonaffine variety can be awkward, due to the need to consider hypercohomology. In the case of a smooth hypersurface in projective space, one can get around this awkwardness by passing to a related affine variety.

Definition 2.2.1. Again, let K be a field of characteristic 0. Let S be a homogeneous polynomial of degree d in $K[u_0, \dots, u_n]$ which is nonsingular (i.e., the ideal generated by S and its partial derivatives contains a power of $(u_0, \dots, u_n)$). Then S defines a smooth hypersurface X in the projective space $\mathbb{P}^n_K$. Put $U =$

$\mathbb{P}^n_K \setminus X$, so that U is affine with coordinate ring equal to the degree 0 part of the localization $K[u_0, \dots, u_n, S^{-1}]$.

THEOREM 2.2.2. *There is a canonical map $H^{n-1}(X) \to H^n(U)$; if n is even, then this map is an isomorphism, otherwise it is surjective with one-dimensional kernel spanned by the Lefschetz class $c(\mathcal{O}(1))^{(n-1)/2}$, where c denotes the first Chern class. (In other words, $H^n(U)$ computes the* primitive part *of $H^{n-1}(X)$.)*

PROOF. This follows from the excision property for algebraic de Rham cohomology. □

DEFINITION 2.2.3. Put

$$\Omega = \sum_{i=0}^{n} (-1)^i u_i \, du_0 \wedge \cdots \wedge \widehat{du_i} \wedge \cdots \wedge du_n,$$

where the hat denotes omission. It is straightforward to check that $H^n(U)$ may be identified with the quotient of the group of n-forms $A\Omega/S^i$, where i is an arbitrary positive integer and $A \in K[u_0, \dots, u_n]$ is homogeneous of degree $id - n - 1$, by the subgroup generated by

$$\frac{(\partial_j A)\Omega}{S^i} - i\frac{A(\partial_j S)\Omega}{S^{i+1}} \tag{2.2.3.1}$$

for all nonnegative integers i, all $j \in \{0, \dots, n\}$, and all homogeneous polynomials $A \in K[u_0, \dots, u_n]$ of degree $id - n$. (Here ∂_j is shorthand for $\frac{\partial}{\partial u_j}$.)

Besides giving an explicit description of the cohomology of X, this construction also makes the Hodge filtration readily apparent.

THEOREM 2.2.4 (Griffiths). *Define $\mathrm{Fil}^{n-1-i} H^n(U)$ as the image in $H^n(U)$ of the set of forms $A\Omega/S^{i+1}$ with A homogeneous of degree $id-n-1$. Then $\mathrm{Fil}^{\cdot} H^n(U)$ corresponds to the Hodge filtration on the primitive part of $H^{n-1}(X)$.*

REMARK 2.2.5. More generally, there is a similar recipe for computing the algebraic de Rham cohomology of a smooth complete intersection inside any toric variety.

2.3. Cyclic cubic threefolds. We now use the Griffiths-Dwork recipe to study the de Rham cohomology of a cyclic cubic threefold.

OBSERVATION 2.3.1. Suppose that X is a cyclic cubic threefold as in Definition 1.4.1. Using Griffiths's theorem, we recover the Hodge numbers

$$h^{0,3} = h^{3,0} = 0, \qquad h^{1,2} = h^{2,1} = 5. \tag{2.3.1.1}$$

In particular, $\dim_K H^3(X) = 10$. We also see that the action of $[\zeta_3]$ splits $H^3_{\mathrm{dR}}(X)$ into two subspaces $H_1 \oplus H_2$, where H_1 transforms like a and has $\dim_K(H_1 \cap \mathrm{Fil}^2 H^3_{\mathrm{dR}}(X)) = 4$, while H_2 transforms like a^2 and has $\dim_K(H_2 \cap \mathrm{Fil}^2 H^3_{\mathrm{dR}}(X)) = 1$. More explicitly, if b is a generator of the degree 4 subspace of the Jacobian ring

$$J_X = K[w, x, y, z]/(Q_w, Q_x, Q_y, Q_z),$$

then a basis for H_1 is given by

$$\frac{w\Omega}{S^2}, \frac{x\Omega}{S^2}, \frac{y\Omega}{S^2}, \frac{z\Omega}{S^2}, \frac{b\Omega}{S^3},$$

with the first four basis elements spanning $\mathrm{Fil}^2 H_1$. Similarly, if b_1, b_2, b_3, b_4 form a basis of the degree 3 subspace of J_X, then a basis for H_2 is given by

$$\frac{a\Omega}{S^2}, \frac{ab_1\Omega}{S^3}, \frac{ab_2\Omega}{S^3}, \frac{ab_3\Omega}{S^3}, \frac{ab_4\Omega}{S^3},$$

with the first basis element spanning $\mathrm{Fil}^2 H_2$.

In this light, let us consider our special and generic examples.

Example 2.3.2. For the Fermat cubic, we may make particularly convenient choices of b, b_1, b_2, b_3, b_4 in Observation 2.3.1: we take

$$b = wxyz, \quad b_1 = xyz, \quad b_2 = wyz, \quad b_3 = wxz, \quad b_4 = wxy.$$

Using the chosen bases, H_1 and H_2 split into eigenspaces for the G-action with characters

$$H_1 : (2,1,1,1,1), (1,2,1,1,1), (1,1,2,1,1), (1,1,1,2,1), (2,2,2,2,1)$$
$$H_2 : (1,1,1,1,2), (1,2,2,2,2), (2,1,2,2,2), (2,2,1,2,2), (2,2,2,1,2),$$

as predicted by Example 1.5.3.

Example 2.3.3. In Example 1.6.1, one checks (see worksheet) that $b = wxyz$ and $b = wxyz + w^4$ have nonzero images in the Jacobian ring, so give rise to good bases of H_1. Similarly, one checks (see worksheet) that $b_1 = xyz, b_2 = wyz, b_3 = wxz, b_4 = wxy$ are linearly independent in the Jacobian ring, so give rise to a good basis of H_2.

2.4. Optional: Intermediate Jacobians. We recall a construction of Clemens and Griffiths [**15**].

Definition 2.4.1. For X any smooth cubic threefold in $\mathbb{P}^4$ (not necessarily cyclic), there exists a canonical abelian variety A and a canonical isomorphism $H^3(X) \cong H^1(A)(1)$ respecting all extra structures, e.g., the Hodge filtration if K is of characteristic zero, or the action of Frobenius if K is a p-adic field and X has good reduction (see next section). We call A the *intermediate Jacobian* of X.

Remark 2.4.2. We amplify Remark 1.1.2 slightly: our intended application of the calculation of p-adic cohomology of cyclic cubic threefolds is to compute the L-function of the intermediate Jacobian of a cyclic cubic threefold over $\mathbb{Q}$. Note that the intermediate Jacobian inherits the action of ζ_3 on X.

3. de Rham cohomology and p-adic cohomology

We now give a brief description of one particular Weil cohomology theory, Berthelot's theory of p-adic rigid cohomology, then explain how it can be computed in many cases using algebraic de Rham cohomology. This comparison leads to a relationship between the Hodge filtration of a variety and its zeta function; we will use this to finish the computation of the zeta function of our generic example of a cyclic cubic threefold, as initiated in Example 1.6.1.

3.1. Rigid cohomology.

DEFINITION 3.1.1. For q a power of the prime p, we write $\mathbb{Q}_q$ for the unramified extension of the p-adic field $\mathbb{Q}_p$ having residue field $\mathbb{F}_q$. We write $\mathbb{Z}_q$ for the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_q$.

DEFINITION 3.1.2. For X a variety over the finite field $\mathbb{F}_q$, let $H^i_{\mathrm{rig}}(X)$ denote the i-th *rigid cohomology* of X. This is a Weil cohomology which we will not construct explicitly in general; instead, we will describe some special cases in detail, and refer for the rest to the book of le Stum [**66**] (and to additional references discussed in the appendix). The construction of rigid cohomology is contravariantly functorial, so in particular the p-power Frobenius morphism $F_p : X \to X$ induces an endomorphism of $H^i_{\mathrm{rig}}(X)$. This endomorphism on cohomology is σ_p-semilinear for σ_p the Witt vector Frobenius on $\mathbb{Q}_q$; raising to the power $\log_p(q)$ gives a q-power Frobenius morphism F_q which on cohomology is $\mathbb{Q}_q$-linear.

REMARK 3.1.3. In these notes, we will mostly consider the case $q = p$ in examples. However, in some applications (notably, in the use of hyperelliptic curves in cryptography) one wishes to take q to be a large power of p. In these cases, it is much more efficient to compute with the p-power Frobenius first, then extrapolate results for the q-power Frobenius, than to work with the q-power Frobenius directly.

3.2. Comparison theorems. In the computations described in these lectures, we access rigid cohomology via the following comparison theorem.

THEOREM 3.2.1 (Berthelot, Baldassarri-Chiarellotto). *Let (X, Z) be a smooth proper pair over $\mathbb{Z}_q$ (i.e., X is smooth proper over $\mathbb{Z}_q$ and Z is a relative normal crossings divisor). Then there is a canonical isomorphism*

$$H^i_{\mathrm{dR}}(X_{\mathbb{Q}_q} \setminus Z_{\mathbb{Q}_q}) \cong H^i_{\mathrm{rig}}(X_{\mathbb{F}_q} \setminus Z_{\mathbb{F}_q}).$$

In order to control p-adic precision in computations, we need also an integral comparison theorem.

THEOREM 3.2.2 (Berthelot, Shiho). *Let (X, Z) be a smooth proper pair over $\mathbb{Z}_q$. Then there is a canonical isomorphism*

$$H^i_{\mathrm{dR}}(X, Z) \cong H^i_{\mathrm{crys}}(X_{\mathbb{F}_q}, Z_{\mathbb{F}_q}),$$

where the left side denotes the hypercohomology of the logarithmic de Rham complex, while the right side denotes logarithmic crystalline cohomology.

Again, the right side in this isomorphism carries an action of Frobenius, so the image of the map $H^i_{\mathrm{dR}}(X, Z) \to H^i_{\mathrm{dR}}(X_{\mathbb{Q}_q} \setminus Z_{\mathbb{Q}_q})$ is a lattice stable under the Frobenius action.

3.3. p-adic divisibility and the Hodge filtration. When computing zeta functions, it is often helpful to account for the following theorem of Mazur, which relates the Hodge filtration to p-adic divisibility of the Frobenius matrix.

THEOREM 3.3.1. *Let X be a smooth proper scheme over $\mathbb{Z}_q$. Assume that $p > i$. Then for $j = 0, \dots, i$, the image of $\mathrm{Fil}^j H^i_{\mathrm{dR}}(X)$ under the action of the p-power Frobenius on $H^i_{\mathrm{crys}}(X_{\mathbb{F}_q})$ is divisible by p^j.*

COROLLARY 3.3.2. *Let X be a smooth proper scheme over $\mathbb{Z}_q$. Assume that $p > i$. Let $p^{e_1} \leq \cdots \leq p^{e_d}$ denote the elementary divisors of the matrix of the q-power Frobenius acting on some basis of $H^i_{\mathrm{crys}}(X_{\mathbb{F}_q})$. Then for $j = 1, \dots, d$, e_j is at least the j-th partial sum of the sequence consisting of $h^{0,i}$ copies of $0 \cdot \log_p(q)$, $h^{1,i-1}$ copies of $1 \cdot \log_p(q)$, and so on. Moreover, equality holds for $j = d$.*

COROLLARY 3.3.3. *Let X be a smooth proper scheme over $\mathbb{Z}_q$. Assume that $p > i$. Then the Newton polygon of the characteristic polynomial of the q-power Frobenius on $H^i_{\mathrm{rig}}(X_{\mathbb{F}_q})$ lies on or above the Hodge polygon, with the same endpoints. (The* Hodge polygon *is defined to have slope $j \log_p(q)$ with multiplicity $h^{j,i-j}$.)*

REMARK 3.3.4. Beware that the analogue of Theorem 3.3.1 for the q-power Frobenius is false for $q \neq p$. However, Corollary 3.3.2 is nonetheless correct as written: the relationship between the Hodge polygon and the elementary divisors of the q-power Frobenius matrix can be deduced from the p-power case, but this does not say anything about the action of Frobenius relative to the Hodge filtration.

We will later use the following lemma to take into account the Hodge divisibility in the Frobenius matrix.

LEMMA 3.3.5. *Let Φ be a $d \times d$ matrix over $\mathbb{Z}_q$ whose reduction modulo q has rank e. Then for any matrix $\Delta \in q^m \mathbb{Z}_q$, the coefficients of T^i in $\det(1 - T\Phi)$ and $\det(1 - T(\Phi + \Delta))$ differ by a multiple of $q^{\max\{m, m+i-e-1\}}$.*

PROOF. See [**53**, Theorem 4.4.2] or [**1**, Proposition 1.6.3]. □

3.4. p-adic cohomology of cyclic cubic threefolds. We make the previous discussion explicit for cyclic cubic threefolds over finite fields, including our special and generic examples.

OBSERVATION 3.4.1. Suppose $q \equiv 1 \pmod 3$ and that $\mathbb{F}_q$ has characteristic $p \geq 5$. Let X be a cyclic cubic threefold over $\mathbb{F}_q$ defined by the polynomial Q. By Theorem 3.2.1, the rigid cohomology of X is isomorphic to the de Rham cohomology of the cyclic cubic threefold defined by any cubic polynomial $\tilde{Q} \in \mathbb{Z}_q[w, x, y, z]$ lifting Q. By Theorem 3.2.2, the matrix Φ of action of F_q on our chosen basis has entries in $\mathbb{Z}_q$. (This requires $p \geq 5$ to ensure that the basis we wrote down is indeed a basis of the *integral* de Rham cohomology module.) Moreover, since $h^{0,3} = h^{3,0} = 0$ (Observation 2.3.1), Φ is divisible by q.

Since the cyclic automorphism lifts, we see that the spaces H_1 and H_2 of Observation 2.3.1 are stable under F_q. We may thus use Theorem 3.3.1 to deduce divisibilities in $\det(1 - TF_q, H_i)$ for $i = 1, 2$, provided that we correctly match up the cube roots of unity in $\mathbb{F}_q$ and $\mathbb{Q}_q$. The correct matching is to match a cube root r of 1 in $\mathbb{F}_q$ with its Teichmüller lift $\tilde{r}$ in $\mathbb{Q}_q$; this has the effect of distinguishing one of the two prime ideals $\mathfrak{p}$ in $\mathbb{Z}[\zeta_3]$ above p. Put $a = \log_p q$ and $\mathfrak{q} = \mathfrak{p}^a$.

With this in mind, write

$$\det(1 - q^{-1}TF_q, H_1) = 1 + a_1 T + \cdots + a_5 T^5$$
$$\det(1 - q^{-1}TF_q, H_2) = 1 + b_1 T + \cdots + b_5 T^5,$$

so that $a_j, b_j \in \mathbb{Z}[\zeta_3]$ are conjugates for $j = 1, \dots, 5$. Taking into account the intersection of $\mathrm{Fil}^2 H^3_{\mathrm{rig}}(X)$ with H_1 and H_2, we see that a_j is divisible by the ideal $\mathfrak{q}^{j-1}$ for $j = 2, 3, 4, 5$, while b_5 is divisible by $\mathfrak{q}$ (so a_5 is divisible by $\overline{\mathfrak{q}}$).

Example 3.4.2. In the case of the Fermat cubic threefold over $\mathbb{F}_7$, we may check the consistency of Theorem 3.3.1 with the computation of Example 1.5.3. In (1.5.3.1), the first four entries correspond to the eigenspaces in H_1 belonging to $\mathrm{Fil}^2 H^3_{\mathrm{rig}}(X)$; correspondingly, the first four eigenvalues in (1.5.3.3) are divisible by $7(\zeta_3 - 2)$ (see worksheet). Similarly, in (1.5.3.2), the fifth entry corresponds to the single eigenspace of H_2 belonging to $\mathrm{Fil}^2 H^3_{\mathrm{rig}}(X)$; correspondingly, the fifth eigenvalue in (1.5.3.4) is divisible by $7(\zeta_3 - 2)$ (see worksheet).

Example 3.4.3. In the case of our generic example (Example 1.6.1), we can use Observation 3.4.1 to completely determine the zeta function. What we know so far from the computation in Example 1.6.1 is that

$$\det(1 - 7^{-1}TF_q, H_1) = 1 + (3\zeta_3 + 2)T + (8\zeta_3 + 5)T^2 + (7\zeta_3 - 14)T^3 + a_4T^4 + a_5T^5$$
$$\det(1 - 7^{-1}TF_q, H_2) = 1 + (3\zeta_3^2 + 2)T + (8\zeta_3^2 + 5)T^2 + (7\zeta_3^2 - 14)T^3 + \overline{a_4}T^4 + \overline{a_5}T^5$$

for some $a_4, a_5 \in \mathbb{Z}[\zeta_3]$. From Observation 3.4.1, we get the additional information that a_4 is divisible by $(\zeta_3 - 2)^3$ while a_5 is divisible by $7(\zeta_3 - 2)^3$.

Using the symmetry of the zeta function, we also have

$$P(T/7) = 1+T+9T^2+2T^3+?T^4+?T^5+?T^6+98T^7+3087T^8+2401T^9+16807T^{10}.$$

This gives us the equations

$$\begin{aligned} 16807 &= a_5\overline{a_5} \\ 2401 &= a_4\overline{a_5} + a_5\overline{a_4} \\ 3087 &= a_4\overline{a_4} + (7\zeta_3^2 - 14)a_5 + (7\zeta_3 - 14)\overline{a_5}. \end{aligned}$$

Since $7(\zeta_3 - 2)^3$ already has norm $16807 = 7^5$, the first equation only has the solutions

$$a_5 = (-\zeta_3)^k 7(\zeta_3 - 2)^3 \qquad (k = 0, \dots, 5).$$

The second and third equations can be viewed as computing the trace and norm of $a_4\overline{a_5}/7^4 \in \mathbb{Z}[\zeta_3]$; namely,

$$\begin{aligned} &\mathrm{Trace}(a_4\overline{a_5}/7^4) = 1 \\ &\mathrm{Norm}(a_4\overline{a_5}/7^4) = -2, 11, 22, 20, 7, -4 \qquad (k = 0, \dots, 5) \end{aligned}$$

(see worksheet for the second computation). We thus have

$$a_4\overline{a_5}/7^4 \in \left\{ \frac{1}{2} \pm i\sqrt{x - \frac{1}{4}} : x = -2, 11, 22, 20, 7, -4 \right\},$$

but only the value $x = 7$ leads to an element of $\mathbb{Z}[\zeta_3]$. We thus must take $k = 4$, yielding $a_5 = -133\zeta_3 - 126$ and $a_4 \in \{16\zeta_3 - 39, -35\zeta_3 + 21\}$. Only the first choice is consistent with the equation

$$98 = (8\zeta_3 + 5)\overline{a_5} + (7\zeta_3 - 14)\overline{a_4} + (7\zeta_3^2 - 14)a_4 + (8\zeta_3^2 + 5)a_5$$

(see worksheet) so we compute

$$\begin{aligned} \det(1 - 7^{-1}TF_q, H_1) &= 1 + (3\zeta_3 + 2)T + (8\zeta_3 + 5)T^2 + (7\zeta_3 - 14)T^3 \\ &\quad + (16\zeta_3 - 39)T^4 + (-133\zeta_3 - 126)T^5 \\ \det(1 - 7^{-1}TF_q, H_2) &= 1 + (3\zeta_3^2 + 2)T + (8\zeta_3^2 + 5)T^2 + (7\zeta_3^2 - 14)T^3 \\ &\quad + (16\zeta_3^2 - 39)T^4 + (-133\zeta_3^2 - 126)T^5 \end{aligned}$$

and

$$P(T/7) = 1 + T + 9T^2 + 2T^3 - 31T^4 - 45T^5 \\ - 217T^6 + 98T^7 + 3087T^8 + 2401T^9 + 16807T^{10}$$

(see worksheet). One checks that $P(T/7)$ indeed has all complex roots of norm $7^{-1/2}$ (see worksheet).

4. The direct method for cyclic cubic threefolds

In this lecture, we describe one application of the direct method for using p-adic cohomology to compute zeta functions, in the case of cyclic cubic threefolds. This will be only a theoretical discussion, however; we will see that the direct method is rather impractical for cyclic cubic threefolds, at least in the form given here. (Recent work of David Harvey suggests that the direct method may ultimately be practical in cases like this; see Remark 4.4.8 and the appendix for discussion.)

4.1. Frobenius actions on affine varieties. The direct method is based on an explicit description of the Frobenius action on the rigid cohomology of an affine variety, via the interpretation of rigid cohomology in terms of Monsky-Washnitzer cohomology.

Definition 4.1.1. Let (X, Z) be a smooth proper pair over $\mathbb{Z}_q$ such that $U = X \setminus Z$ is affine. Let $A = \Gamma(U, \mathcal{O}_U)$ be the coordinate ring of U. Let $\widehat{A}$ be the p-adic completion of A. Let $A^\dagger$ be the subring of $\widehat{A}$ defined by the following condition: we have $x \in A^\dagger$ if and only if there exists some $a > 0$ such that for each positive integer n, the reduction of x modulo p^n has poles of order at most an along each component of Z. (The ring $A^\dagger$ is also known as the *weak p-adic completion* of A.)

Theorem 4.1.2 (Berthelot). *There is a canonical isomorphism between $H^i_{\mathrm{rig}}(U_{\mathbb{F}_q})$ and the cohomology of the de Rham complex of $A^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$. Moreover, if (X', Z') is another smooth proper pair, and we define $(A')^\dagger$ similarly, then any ring homomorphism $f : A^\dagger \to (A')^\dagger$ induces the functoriality morphism $H^i_{\mathrm{rig}}(U_{\mathbb{F}_q}) \to H^i_{\mathrm{rig}}(U'_{\mathbb{F}_q})$ corresponding to the map $X'_{\mathbb{F}_q} \to X_{\mathbb{F}_q}$ given by reducing f mod p. (Note that the morphism $A^\dagger \to (A')^\dagger$ need not be induced by a map $X' \to X$; even if such a map exists, that map need not carry Z' into Z.)*

4.2. The direct method. We now describe how to execute the direct method for computing the zeta function of a cyclic cubic threefold. This is a summary of the approach described in more detail (and in more generality) in [**1**].

Procedure 4.2.1. Suppose q is a power of a prime $p \geq 5$. Let X be the cyclic cubic threefold over $\mathbb{F}_q$ associated to the nonsingular polynomial $Q \in \mathbb{F}_q[w, x, y, z]$. Let $\mathfrak{o}$ be the ring of integers in some number field, such that there exists an ideal $\mathfrak{p}$ of $\mathfrak{o}$ unramified above p with residue field $\mathbb{F}_q$; we identify the $\mathfrak{p}$-adic completion of $\mathfrak{o}$ with $\mathbb{Z}_q$. Choose a homogeneous cubic polynomial $\tilde{Q} \in \mathfrak{o}[w, x, y, z]$ lifting Q, and put $\tilde{S} = a^3 - \tilde{Q} \in \mathfrak{o}[w, x, y, z, a]$. Let $\tilde{X}$ be the cyclic cubic threefold over the local ring $\mathfrak{o}_{\mathfrak{p}}$ associated to $\tilde{Q}$.

To compute the numerator $P(T)$ of the zeta function of $X \cong \tilde{X}_{\mathbb{F}_q}$, we use the comparisons

$$H^3_{\mathrm{rig}}(\tilde{X}_{\mathbb{F}_q}) \cong H^3_{\mathrm{dR}}(\tilde{X}_{\mathbb{Q}_q}) \cong H^4_{\mathrm{dR}}(\tilde{U}_{\mathbb{Q}_q}) \cong H^4_{\mathrm{rig}}(\tilde{U}_{\mathbb{F}_q})$$

for $\tilde{U} = \mathbb{P}^4_{\mathbb{Z}_q} \setminus \tilde{X}$. Note however that the Frobenius action on $H^4_{\mathrm{rig}}(U)$ is not quite the same as the one on $H^4_{\mathrm{rig}}(X_{\mathbb{F}_q})$; rather, it is twisted by an extra factor of q. Consequently, we compute the action of $q^{-1}F_q$ on $H^4_{\mathrm{rig}}(U)$ rather than that of F_q.

We split the integral de Rham cohomology $H^3_{\mathrm{dR}}(X)$ as a direct sum $H_1 \oplus H_2$ of eigenspaces for the action of $[\zeta_3]$. We obtain integral bases of both H_1 and H_2 by applying the recipes from Observation 2.3.1 modulo p and lifting to elements of the same degree. (This succeeds in giving integral bases because $p \geq 5$.)

We apply Theorem 4.1.2 to the map induced by the algebraic map F_q on $\mathbb{P}^4_{\mathbb{Z}_q}$ acting on the variables by

$$* \mapsto *^q \qquad (* = w, x, y, z, a).$$

The induced action on $\tilde{S}^{-1}$ carries it to

(4.2.1.1)

$$\tilde{S}^{-q}\left(1 + \frac{F_q(\tilde{S}) - \tilde{S}^q}{\tilde{S}^q}\right)^{-1} = \sum_{i=0}^{\infty} \binom{-1}{i} (a^{3q} - \tilde{Q}(w^q, x^q, y^q, z^q) - (a^3 - \tilde{Q})^q)^i \tilde{S}^{-q(i+1)}.$$

Note that this map does not carry $\tilde{X}$ into itself, but Theorem 4.1.2 requires no such hypothesis. All that matters is that the powers of p in the numerator of the summand accrue at a linear rate compared to the powers of $\tilde{S}$ in the denominator.

To compute the Frobenius matrix, apply the map F_q formally to each basis vector, using the formula

$$q^{-1}F_q(\Omega) = q^3(wxyza)^{q-1}\Omega.$$

The result is an infinite series, so we cannot compute it exactly; we must neglect those terms divisible by a sufficiently large power of p. This has the effect of eliminating terms with sufficiently many factors of $\tilde{S}$ in the denominator, so we obtain an algebraic differential; we use the relations (2.2.3.1) to rewrite the resulting algebraic differential as an exact differential plus a $\mathbb{Q}$-linear combination of basis vectors. For instance, this can be done by first eliminating the poles of highest order, then the next highest order, and so on.

The end result is a p-adic approximation of the matrix of Frobenius on $H^3_{\mathrm{rig}}(X_{\mathbb{F}_q})$; we must make some side analysis to determine exactly how accurate this matrix is. This gives a p-adic approximation of the characteristic polynomial of this matrix, again with some known precision; if this precision is sufficient, there will be a unique monic polynomial with coefficients in $\mathbb{Z}$ and complex roots of absolute value $q^{3/2}$ agreeing with this approximation. The reverse of this polynomial must then equal $P(T)$.

This completes the description aside from the analysis of the initial and final precision needed for the computation. We address these issues later in this lecture.

Remark 4.2.2. When $q \neq p$, one normally computes the p-power Frobenius first and then recovers the q-power Frobenius. The most important thing to remember is that the p-power Frobenius is not linear on scalars; it acts via the Witt vector Frobenius map. See [**1**] for more details.

4.3. Final precision. Of the two precision questions in Procedure 4.2.1, the easier one to answer is how much p-adic precision is needed in an approximation of the Frobenius matrix in order to uniquely determine its characteristic polynomial; we answer this using the Riemann hypothesis condition.

Observation 4.3.1. Retain notation as in Procedure 4.2.1. Let Φ denote the matrix of action of Frobenius on an integral basis of $H^3_{\mathrm{rig}}(X)$. We have noted earlier (Observation 3.4.1) that Φ is divisible by q, so we work with $q^{-1}\Phi$ instead.

We are trying to determine the degree 10 polynomial $P(T/q) = \det(1-q^{-1}T\Phi)$. Thanks to the symmetry $P(1/(q^3T)) = q^{-15}T^{-10}P(T)$, it is enough to determine the coefficients of T^j in $P(T/q)$ for $j = 1, 2, 3, 4, 5$. Lemma 1.2.3 implies that once we determine the coefficients of T^k for $k < j$, the possible coefficients of T^j lie in a disc of radius $\frac{10}{j}q^{j/2}$. It thus suffices to determine T^j modulo an integer strictly greater than twice this radius.

Suppose we have carried enough precision in Procedure 4.2.1 to compute Φ modulo q^m, or equivalently $q^{-1}\Phi$ modulo q^{m-1}. In case

$$q^{m-1} > \frac{20}{j}q^{j/2} \qquad (j = 1, 2, 3, 4, 5),$$

then we can uniquely reconstruct $P(T/q)$. For $q > 16$, this occurs as soon as $m \geq 4$ (see worksheet); for $q = 7$, we instead must take $m = 5$.

Observation 4.3.2. In case $q \equiv 1 \pmod 3$, we can do better by computing the matrix Φ_1 via which F_q acts on the chosen basis of H_1, as follows. Let $\mathfrak{q}$ be the ideal defined in Observation 3.4.1; in particular, $\mathfrak{q}$ has norm q, and ζ_3 reduces modulo $\mathfrak{q}$ to the chosen cube root of 1 in $\mathbb{F}_q$.

Suppose we have computed Φ_1 modulo q^m, or equivalently $q^{-1}\Phi_1$ modulo q^{m-1}. By Lemma 3.3.5, the coefficient of T^j in $\det(1 - q^{-1}T\Phi_1)$ is determined modulo

$$\mathfrak{q}^{m-1}, \mathfrak{q}^{m-1}, \mathfrak{q}^m, \mathfrak{q}^{m+1}, \mathfrak{q}^{m+2} \qquad (j = 1, 2, 3, 4, 5).$$

On the other hand, the entries of $q^{-1}\Phi_1$ have relative precision at least q^{m-2}; that is, each is known to be a particular power of p times a unit in $\mathbb{Z}_q$ which is known modulo q^{m-2}. It follows that the same is true of the entries of $q(q^{-1}\Phi_1)^{-1} = q^2\Phi_1^{-1}$. Since this matrix has entries in $\mathbb{Z}_q$, it is known modulo q^{m-2}. Hence by Lemma 1.2.3, the coefficient of T^j in $\det(1 - q^2T\Phi_1^{-1})$ is determined modulo

$$\mathfrak{q}^{m-2}, \mathfrak{q}^{m-2}, \mathfrak{q}^{m-2}, \mathfrak{q}^{m-2}, \mathfrak{q}^{m-1} \qquad (j = 1, 2, 3, 4, 5).$$

However, these coefficients are the complex conjugates of the coefficients of $\det(1 - q^{-1}T\Phi_1)$. Hence the latter are determined modulo

$$q^{m-2}\mathfrak{q}, q^{m-2}\mathfrak{q}, q^{m-2}\mathfrak{q}^2, q^{m-2}\mathfrak{q}^3, q^{m-1}\mathfrak{q}^3 \qquad (j = 1, 2, 3, 4, 5).$$

The minimum complex norm of a nonzero element of one of these ideals is the square root of the norm of the ideal. Hence if we have the five inequalities

$$\begin{aligned} q^{m-3/2} &> 10q^{1/2} \\ q^{m-3/2} &> 5q \\ q^{m-1} &> \frac{10}{3}q^{3/2} \\ q^{m-1/2} &> \frac{5}{2}q^2 \\ q^{m+1/2} &> 2q^{5/2} \end{aligned}$$

then we can reconstruct $\det(1 - q^{-1}T\Phi_1)$ and hence all of the zeta function.

For q sufficiently large, these five inequalities hold for $m = 3$; for $q = 7$, they hold for $m = 4$ (see worksheet). These are each one less than the bounds obtained

in Observation 4.3.1; this will lead to significant runtime improvements in our calculations.

REMARK 4.3.3. As noted in Remark 1.2.4, one can sometimes compute zeta functions using less p-adic precision than one might initially predict, by accounting for the Riemann hypothesis condition. We can see this explicitly for the zeta function computed in Example 3.4.3, using the `Sage` package associated to the paper [**50**]. For example, we find that the polynomial $P(T/7)$ is already determined uniquely when $m = 4$ (i.e, by its reduction modulo 7^3; see worksheet), whereas Observation 4.3.1 only predicts this for $m = 5$. For another example, if we take $m = 3$, then $P(T/7)$ is determined within a list of 7 possibilities, but six of these have irreducible factors over $\mathbb{Q}(\zeta_3)$ of degree greater than 5 (see worksheet). So again $P(T/7)$ is uniquely determined.

4.4. Initial precision. It remains to specify how much initial precision is needed in the calculation of the Frobenius action on forms in Procedure 4.2.1, in order to obtain a specific precision on the resulting Frobenius matrix. This analysis of *precision loss* is one of the trickiest aspects of the direct method.

REMARK 4.4.1. The analysis of precision loss serves two functions. On one hand, it is needed in order to make *provably correct* calculations. On the other hand, even if one is merely interested in experimental results which are probably correct, one would like to generate these efficiently; analysis of precision loss suggests how to balance speed against precision in order to avoid generating garbage data.

In the case of cyclic cubic threefolds, we first recast the precision loss problem as follows.

PROBLEM 4.4.2. *Given a form $A\Omega/\tilde{S}^i$ for A a polynomial with coefficients in $\mathbb{Z}_p$, bound the denominators appearing when this form is written as an exact differential plus a $\mathbb{Q}_q$-linear combination of basis forms.*

Given a good enough solution of Problem 4.4.2, we can bound the precision of the error term created by omitting terms with $\tilde{S}^j$ for $j \geq i$ in the denominator. We can then determine where this truncation may be made to achieve the desired final precision.

EXAMPLE 4.4.3. In the case of cyclic cubic threefolds, simply counting divisions by p gives a bound on the denominator in Problem 4.4.2 which is linear in i. This is not good enough; by a somewhat complicated argument using an analysis of integral logarithmic de Rham cohomology [**1**, Proposition 3.4.6], one obtains the following bound which is logarithmic in i.

PROPOSITION 4.4.4. *Any form $A\Omega/\tilde{S}^i$, with $A \in \mathbb{Z}_p[w, x, y, z, a]$, is cohomologous to a linear combination of integral basis vectors with coefficients in $p^{-c}\mathbb{Z}_p$ for*

$$c = \sum_{j=1}^{4} \lfloor \log_p \max\{1, i - j\} \rfloor.$$

EXAMPLE 4.4.5. Suppose that we wish to compute the matrix Φ modulo p^m. We can write each basis differential as $A\Omega/\tilde{S}^3$ for some polynomial A; by (4.2.1.1),

its image under Frobenius is

(4.4.5.1)

$$p^3(wxyza)^{p-1}F_p(A)\sum_{i=0}^{\infty}\binom{-3}{i}(a^{3p}-\tilde{Q}(w^p,x^p,y^p,z^p)-(a^3-\tilde{Q})^p)^i\tilde{S}^{-p(i+3)}.$$

We wish to compute a quantity N such that if if we consider the terms of (4.4.5.1) for which $i \geq N$, then their reductions to the basis vectors have coefficients in $p^m\mathbb{Z}_p$. The i-th term in the sum is divisible by p^{3+i}, so it would suffice to have

$$3+i-m \geq 4\lfloor \log_p(p(i+3)-1)\rfloor \qquad (i=N,N+1,\dots). \tag{4.4.5.2}$$

For $p=7$, we know by Observation 4.3.2 that it suffices to take $m=4$ to recover the zeta function. In this case, (4.4.5.2) holds for $N=9$ but not for any smaller value (see worksheet for a check up to $i=75$).

Remark 4.4.6. By further accounting for the Frobenius action [**1**, Proposition 3.4.9], one gets a bound which is asymptotically $3\log_p(i)$. While this is suspected to be asymptotically optimal, it seems to be suboptimal for small values. Improving the bound may lead to significant runtime improvements in practice, by reducing the degrees of the polynomial approximations needed in the truncations of Frobenius.

In the particular case of Example 1.6.1, taking $p=7$ and $m=3$ (as in Remark 4.3.3), we may apply [**1**, Algorithm 3.4.10] (using the associated Magma code from [**1**]) to see that we can ignore all terms in the expansion divisible by p^9. In our notation, this means we may take $N=6$.

However, even this level of precision is difficult to achieve in practice; we must work with polynomials in five variables with coefficients in $\mathbb{Z}/7^n\mathbb{Z}$ for n at least 9, of total degree $3\cdot p\cdot(N-1)=105$. We will thus not carry out any demonstration of the direct method here. (See the associated `Magma` code of [**1**] for a demonstration for surfaces, where the situation is somewhat less dire. See also Remark 4.4.8 below.)

Remark 4.4.7. The analogous analysis of precision loss in Kedlaya's algorithm is [**47**, Lemmas 2 and 3]; however, note the erratum which corrects the latter. The erratum also points out that the analysis in [**47**], while not phrased in terms of integral de Rham cohomology, can indeed be interpreted this way.

Remark 4.4.8. After the original version of these notes was prepared, David Harvey proposed an alternate reduction algorithm for de Rham cohomology in this setting, in which one structures the reduction in order to use only *sparse* polynomials. This may render the direct cohomological method much more practical than we had previously anticipated. See the appendix for further discussion.

5. Picard-Fuchs-Manin connections

In this lecture, we discuss the relative version of algebraic de Rham cohomology. This gives rise to certain special differential systems classically called *Picard-Fuchs systems*, and often nowadays called *Gauss-Manin connections*. We will use these in the next lecture to execute the deformation method for computing zeta functions.

5.1. Connections on vector bundles. Before describing Picard-Fuchs-Manin connections, we recall the general notion of a connection on a vector bundle over a subset of $\mathbb{P}^1$.

Definition 5.1.1. Let K be a field of characteristic zero. Let B be a nonempty open subscheme of $\mathbb{P}^1_K$. Let $\mathcal{E}$ be a vector bundle over B. A *connection* on $\mathcal{E}$ is a bundle map $\nabla : \mathcal{E} \to \mathcal{E} \otimes \Omega_{B/K}$ which is additive and satisfies the Leibniz rule: for $V \subseteq B$ open, $s \in \Gamma(V, \mathcal{O})$, and $\mathbf{v} \in \Gamma(V, \mathcal{E})$,

$$\nabla(s\mathbf{v}) = s\nabla(\mathbf{v}) + \mathbf{v} \otimes ds.$$

Observation 5.1.2. In order to compute with connections, we will describe them in terms of matrices as follows. Keep notation as in Definition 5.1.1, but assume now that $\infty \notin B$ and that $\mathbf{v}_1, \dots, \mathbf{v}_n$ is a basis of sections of $\mathcal{E}$. Define the $n \times n$ matrix N over $\Gamma(B, \mathcal{O})$ by the equation

$$\nabla(\mathbf{v}_j) = \sum_{i=1}^{n} N_{ij} \mathbf{v}_i \otimes dt \qquad (j = 1, \dots, n).$$

By additivity and the Leibniz rule, we can recover ∇ from N. The simplest way to express that statement is to use the basis to identify sections of $\mathcal{E}$ with column vectors of functions; then

$$\nabla \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} d(f_1) \\ \vdots \\ d(f_n) \end{pmatrix} + N \begin{pmatrix} f_1\, dt \\ \vdots \\ f_n\, dt \end{pmatrix}.$$

In other words, $\nabla = d + N\, dt$.

Observation 5.1.3. The effect of changing basis in Observation 5.1.2 is as follows. Let $\mathbf{w}_1, \dots, \mathbf{w}_n$ be a second basis of $\mathcal{E}$. Define the change of basis matrix U from $\mathbf{v}_1, \dots, \mathbf{v}_n$ to $\mathbf{w}_1, \dots, \mathbf{w}_n$ to be the $n \times n$ matrix satisfying

$$\mathbf{w}_j = \sum_{i=1}^{n} U_{ij} \mathbf{v}_i \qquad (j = 1, \dots, n). \tag{5.1.3.1}$$

Then the matrix representing the connection in terms of $\mathbf{w}_1, \dots, \mathbf{w}_n$ is

$$U^{-1} N U + U^{-1} \frac{d}{dt}(U).$$

We will be interested in a special class of connections.

Definition 5.1.4. With notation as in Observation 5.1.2, and $z \in K^{\mathrm{alg}}$, we say the basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ is *regular at* z (or *Fuchsian at* z) if the matrix $(t - z)N$ is holomorphic in a neighborhood of z. We say that $\mathcal{E}$ is *regular at* z if it admits a regular basis on some neighborhood of z. Another way to say this is that $\mathcal{E}$ can be extended across z so that the connection has only *logarithmic singularities* at z.

This definition is invariant under automorphisms of $\mathbb{P}^1$. It thus makes sense to extend it to $z = \infty$ by using any coordinate change moving ∞ to a finite point (since the resulting definition will not depend on the choice of the coordinate change). For instance, we may use the substitution $t \mapsto t^{-1}$; it then follows that a basis is regular at ∞ if and only if each entry of the matrix N has a zero at $t = \infty$. In concrete terms, for each entry of N, the degree of the numerator must be strictly less than the degree of the denominator.

Definition 5.1.5. With notation as in Observation 5.1.2, and $z \in K^{\mathrm{alg}}$, suppose that the basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ is regular at z. The *residue matrix at* z of this basis is the matrix obtained from $(t - z)N$ by reducing modulo $t - z$; if $z \in B$, this matrix is zero. The *exponents at* z of the basis are the eigenvalues of the residue matrix.

Note that one can change from one regular basis to another without preserving the exponents; for instance, changing basis to $(t-z)\mathbf{v}_1, \dots, (t-z)\mathbf{v}_n$ replaces N by $N+(t-z)^{-1}I_n$, which increases each exponent by 1. However, it can be shown that as a multisubset of the quotient group $K^{\mathrm{alg}}/\mathbb{Z}$, the set of exponents of a regular basis is independent of the choice of the regular basis; we call this the set of *exponents* of $\mathcal{E}$ at z.

If $z = \infty$, we may define the residue matrix to be the matrix obtained from $-tN$ by reducing modulo t^{-1}, and proceeding similarly.

The following lemma demonstrates the use of *shearing transformations*.

LEMMA 5.1.6. *With notation as in Definition 5.1.5, suppose that the exponents of the basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ at some $z \in K^{\mathrm{alg}}$ are integers in the range $\{-a, \dots, b\}$. Then there exists an invertible $n \times n$ matrix U over $K(t)$ such that $(t-z)^b U$ and $(t-z)^a U^{-1}$ are regular at z, and the basis $\mathbf{w}_1, \dots, \mathbf{w}_n$ of $\mathcal{E}$ (over some neighborhood of z) defined by* (5.1.3.1) *is regular at z with all exponents equal to* 0.

PROOF. This reduces to the fact that one can shift the largest exponent down by 1 using a change of basis matrix U such that $(t-z)U$ and U^{-1} are regular at z. We may first use a change of basis defined over K (which acts on N by simple conjugation, since its derivative vanishes) to ensure that the reduction of $(t-z)N$ modulo $(t-z)$ is a block matrix with each block corresponding to the generalized eigenspace of a different eigenvalue. We then change basis by the block diagonal matrix U which is $(t-z)^{-1}$ times the identity on the block with the largest exponent, and the identity on the other blocks. □

REMARK 5.1.7. Associated to a connection is a representation of the topological fundamental group $\pi_1(B, x)$ called the *monodromy representation*. It is defined as follows. Construct a basis of local horizontal sections at the base point x of the fundamental group. For any loop in B, analytically continue these horizontal sections along the loop. The image of the monodromy representation on this loop is the linear transformation on the fibre $\mathcal{E}_x$ taking the restriction to x of each basis section to the restriction of x of its analytic continuation.

In general, it is somewhat hard to identify the eigenvalues of a monodromy transformation. However, if $\mathcal{E}$ is regular at z with exponents $\lambda_1, \dots, \lambda_n$, then the eigenvalues of the monodromy transformation corresponding to a loop going counterclockwise once around z (and enclosing no other points of $\mathbb{P}^1 \setminus B$) are $e^{-2\pi i\lambda_1}, \dots, e^{-2\pi i\lambda_n}$.

5.2. Relative de Rham cohomology.

DEFINITION 5.2.1. Let $f : X \to B$ be a smooth morphism over a field K of characteristic zero, for B a nonempty open subscheme of $\mathbb{P}^1_K$. The *relative de Rham cohomology* of X/B is the collection of sheaves $H^q_{\mathrm{dR}}(X/B)$ whose sections over an open affine $V \subset B$ are the hypercohomology of the relative de Rham complex $\Omega^{\cdot}_{X/V}$. The fact that this gives a sheaf follows from the preservation of coherent cohomology under flat base change. For f proper, this construction also commutes with *arbitrary* base change; this follows from Grothendieck's comparison theorem (Theorem 2.1.3). This fails if f is not proper; consider

$$\operatorname{Spec} K[x,y,z]/((x+y)(x-y)z-1) \mapsto \operatorname{Spec} K[x],$$

in which the Betti numbers of the fibre $x = 0$ differ from the generic values.

Since mixed partial derivatives commute and the computation of relative de Rham cohomology only involves "vertical" differentiation (along fibres), the result should carry an action of "horizontal" differentiation (along the base). This is in fact the case; this is captured by a construction of Katz and Oda.

DEFINITION 5.2.2. Equip the de Rham complex $\Omega^{\cdot}_{X/K}$ with the decreasing filtration

$$F^i = \mathrm{image}[\Omega^{\cdot-i}_{X/K} \otimes_{\mathcal{O}_X} \pi^*(\Omega^i_{B/K}) \to \Omega^{\cdot}_{X/K}],$$

then form the corresponding spectral sequence. The E_1 term of the result has

$$E_1^{p,q} = \Omega^p_{B/K} \otimes_{\mathcal{O}_B} H^q_{\mathrm{dR}}(X/B);$$

the *algebraic Picard-Fuchs-Manin (Gauss-Manin) connection* is the differential $d_1 : E_1^{0,q} \to E_1^{1,q}$.

REMARK 5.2.3. In practice, we will compute only in the case where X is affine. In this case, the definition of d_1 amounts to the following: lift a relative cohomology class to an absolute differential form (no longer a cocycle), differentiate, and project the result back into relative cohomology.

DEFINITION 5.2.4. Suppose that K is a subfield of $\mathbb{C}$. Then the fibration $f : X \to B$ is locally trivial in the category of real differentiable manifolds. On a contractible open subset of B, we may canonically identify the complex homology classes of the fibres; this gives a real differentiable connection on $H^q_{\mathrm{dR}}(X/B)$, called the *topological Picard-Fuchs-Manin connection*. It turns out that this is holomorphic (see [**31**]), and that it agrees with the algebraic Picard-Fuchs-Manin connection (see [**46**]).

THEOREM 5.2.5. *With notation as in Definition 5.2.2, the algebraic Picard-Fuchs-Manin connection is regular at every geometric point of $\mathbb{P}^1_K$, with all exponents in $\mathbb{Q}/\mathbb{Z}$.*

5.3. Pencils of cyclic cubic threefolds. We now explain how to compute the Picard-Fuchs-Manin connection for certain families of cyclic cubic threefolds.

PROCEDURE 5.3.1. Let K be a field of characteristic zero. Take $Q_0 = w^3+x^3+y^3+z^3$, and let $Q \in K[w,x,y,z]$ be a second homogeneous polynomial of degree 3 such that $Q_1 = Q_0 + Q$ is nonsingular. Put $Q_t = Q_0 + tQ$. For $t \in K^{\mathrm{alg}}$, let

$$J_t = K[w,x,y,z]/(Q_{t,w}, Q_{t,x}, Q_{t,y}, Q_{t,z})$$

be the Jacobian ring of Q_t. (Here $Q_{t,w}$ denotes the partial derivative with respect to w of the polynomial Q_t, and similarly.)

We wish to consider the pencil $\pi : X \to \mathbb{P}^1_K$ of cyclic cubic threefolds defined by $S = a^3 - Q_t$, as well as the complementary family $\tau : U \to \mathbb{P}^1_K$ for $U = \mathbb{P}^3_{\mathbb{P}^1_K} \setminus X$. By Lemma 1.4.2, a fibre X_t is smooth if and only if the cubic surface defined by Q_t is smooth; in particular, the fibres X_0, X_1 are smooth.

Let $B \subset \mathbb{P}^1_K$ be the open subscheme over which π is smooth; since $0, 1 \in B$, B is nonempty. Put $\mathcal{E} = H^3_{\mathrm{dR}}(X_B/B)$, which we will also interpret as $H^4_{\mathrm{dR}}(U_B/B)$. Using the order 3 automorphism $a \mapsto \zeta_3 a$, we split $\mathcal{E} = \mathcal{E}_1 \oplus \mathcal{E}_2$ with $\mathcal{E}_i$ transforming like a^i. The Picard-Fuchs-Manin connection on $\mathcal{E}$ splits into separate connections for $\mathcal{E}_1$ and $\mathcal{E}_2$, which we now describe individually.

Let us start with $\mathcal{E}_1$. Choose $b \in K[w,x,y,z]$ such that b generates the degree 4 subspace of J_0, J_1. Let B_1 be the open subscheme of B consisting of those t for which b spans the degree 4 subspace of J_t; by construction, $0, 1 \in B_1$.

Now differentiate each of the basis elements

$$\frac{w\Omega}{S^2}, \frac{x\Omega}{S^2}, \frac{y\Omega}{S^2}, \frac{z\Omega}{S^2}, \frac{b\Omega}{S^3}$$

with respect to t, obtaining

$$\frac{2wQ\Omega}{S^3}, \frac{2xQ\Omega}{S^3}, \frac{2yQ\Omega}{S^3}, \frac{2zQ\Omega}{S^3}, \frac{3bQ\Omega}{S^4},$$

then reduce each of these back into the desired form using the relations

$$\frac{A_i\Omega}{S^j} \equiv -j\frac{(3i^2 + tQ_i)A\Omega}{S^{j+1}} \qquad (i \in \{w,x,y,z\}). \tag{5.3.1.1}$$

This amounts to a large linear algebra calculation over $K(t)$, and for best results it may be preferable to implement it that way. However, we found it easiest to implement this using Gröbner basis methods to express a form as a linear combination of terms amenable to (5.3.1.1). In any case, the entries of the resulting matrix N_1 will belong to the coordinate ring of B_1.

Let us now consider $\mathcal{E}_2$. Choose $b_1, b_2, b_3, b_4 \in K[w,x,y,z]$ which span the degree 3 subspace of J_0, J_1. Let B_2 be the open subscheme of B of those t for which b_1, b_2, b_3, b_4 span the degree 3 subspace of J_t; again by construction, $0, 1 \in B_2$.

Again, differentiate each of the basis elements

$$\frac{a\Omega}{S^2}, \frac{ab_1\Omega}{S^3}, \frac{ab_2\Omega}{S^3}, \frac{ab_3\Omega}{S^3}, \frac{ab_4\Omega}{S^3}$$

with respect to t, obtaining

$$\frac{2aQ\Omega}{S^3}, \frac{3ab_1Q\Omega}{S^4}, \frac{3ab_2Q\Omega}{S^4}, \frac{3ab_3Q\Omega}{S^4}, \frac{3ab_4Q\Omega}{S^4},$$

then reduce each of these back into the desired form using the relations

$$\frac{aA_i\Omega}{S^j} \equiv -j\frac{a(3i^2 + tQ_i)A\Omega}{S^{j+1}} \qquad (i \in \{w,x,y,z\}). \tag{5.3.1.2}$$

This time, the entries of the resulting matrix N_2 will belong to the coordinate ring of B_2.

Example 5.3.2. We calculate the matrix N_1 for $K = \mathbb{Q}$,

$$Q_1 = w^3 + x^3 + y^3 + z^3 + (w+x)(w+2y)(w+3z) + 3xy(w+x+z)$$

(as in Example 1.6.1), and $b = wxyz$ (see worksheet). This computation was carried out using Gröbner basis methods over the coefficient field $\mathbb{Q}(t)$, as implemented in `Magma` (see Remark 5.3.4 for the reason why); it required about twenty seconds to complete.

We then analyze the singular points of the connection as follows. The matrix N_1 has entries in $\mathbb{Q}(t)$, and the least common denominator $\Delta \in \mathbb{Z}[t]$ of the entries factors as $\Delta = \Delta_1\Delta_2\Delta_3$ where $\Delta_1 = t + 3$, Δ_2 is a polynomial of degree 23, and Δ_3 is a polynomial of degree 26 (see worksheet). In particular, Δ is squarefree, so our chosen basis is regular at all finite points.

We next compute the exponents at each of these singular points. For $i = 1, 2, 3$, we compute the characteristic polynomial of $N_1 \Delta / \Delta'(t)$ in $\mathbb{Q}[t]/(\Delta_i)$; we get

$$\begin{aligned} x^3 (x+1) \left(x + \frac{1}{2}\right) \qquad & (i = 1) \\ x^4 (x-1) \qquad & (i = 2) \\ x^4 \left(x + \frac{7}{6}\right) \qquad & (i = 3) \end{aligned}$$

(see worksheet). In particular, the points of Δ_1, Δ_3 have a nonintegral exponent and so must be true singularities of the connection, whereas we cannot tell about Δ_2. We will see below (Example 5.3.3) that in fact the singularities at Δ_2 can be eliminated by a change of basis.

Finally, we analyze the situation at infinity. The given basis is not regular here, because the last row contains entries which are regular but nonvanishing at $t = \infty$ (see worksheet). However, if we change basis using the matrix

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & t \end{pmatrix},$$

then we get a regular basis (see worksheet). Computing the characteristic polynomial of the residue matrix yields

$$\left(x - \frac{3}{2}\right) \left(x - \frac{4}{3}\right) \left(x - \frac{5}{3}\right)^3$$

(see worksheet).

Example 5.3.3. We calculate the connection matrix again as in Example 5.3.2, but this time with $b = wxyz + w^4$ (see worksheet). Let $\tilde{N}_1$ be the new connection matrix, and let $\tilde{\Delta}$ be the least common denominator of the entries of $\tilde{N}_1$. Then we compute that $\gcd(\Delta, \tilde{\Delta}) = \Delta_1 \Delta_3$ (see worksheet); we deduce that the singularities of N_1 at Δ_2 can be removed by changing basis (i.e., they are so-called *apparent singularities*).

Remark 5.3.4. The reason that we used `Magma` instead of `Sage` for this calculation is that we use Gröbner bases for polynomials over the field $\mathbb{Q}(t)$, which are well supported in `Magma`. By contrast, `Sage` does not support such polynomials directly; one can directly call `Singular` to work with such polynomials, but this does not work well in the version of `Sage` that we tried, as even basic operations take an unacceptably long time to complete. (By contrast, working over $\mathbb{F}_q(t)$ causes no such problems.)

5.4. Optional: Exponents in a pencil of cyclic cubic threefolds. We include some discussion of the possible exponents of a Picard-Fuchs-Manin connection associated to a pencil of cyclic cubic threefolds.

Observation 5.4.1. By Theorem 5.2.5, the exponents of the Picard-Fuchs-Manin connection associated to a family of cyclic cubic threefolds at any (necessarily regular) singular point are rational numbers. We may bound the lowest common denominator of these numbers as follows. The exponents of the full connection are

the union of the exponents of $\mathcal{E}_1$ and $\mathcal{E}_2$. The corresponding sets of local monodromy eigenvalues are interchanged by any automorphism in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which does not fix ζ_3.

Hence, any ζ_n with n not divisible by 3, if it occurs at all, occurs together with all of its conjugates in each of $\mathcal{E}_1$ and $\mathcal{E}_2$. This can only happen if $\phi(n) \leq 5$, i.e., if $n \in \{1, 2, 4, 5, 8, 10\}$. If n is divisible by 3, then ζ_n and its conjugates split between $\mathcal{E}_1$ and $\mathcal{E}_2$; we must still have $\phi(n) \leq 10$, so $n \in \{3, 6, 9, 12, 15, 18, 24, 30\}$.

Definition 5.4.2. A *Lefschetz pencil* is a pencil of hypersurfaces in which each singular fibre contains a single rational double point and no other singularities. Unfortunately, a pencil of *cyclic* cubic threefolds can never be a Lefschetz pencil, because the generic degeneration is a rational triple point. However, we can ask for the underlying pencil of cubic surfaces to be a Lefschetz pencil; in that case, a Hodge-theoretic argument shows that the denominators of the exponents (in the Picard-Fuchs-Manin connection for the family of cyclic cubic threefolds) in fact always divide 6. (Thanks to Jim Carlson for pointing this out.)

6. The deformation method for cyclic cubic threefolds

In this lecture, we describe the Frobenius actions on Picard-Fuchs-Manin connections obtained by relating relative de Rham cohomology to relative rigid cohomology. We then execute the deformation method for computing the zeta function for our generic example of a cyclic cubic threefold. This amounts to solving the differential equation imposed on the Frobenius structure by its compatibility with the connection, using the Frobenius matrix of the Fermat cubic as an initial condition.

6.1. Frobenius structures.

Definition 6.1.1. Let q be a prime power. Let $\sigma : \mathbb{P}^1_{\mathbb{Q}_q} \to \mathbb{P}^1_{\mathbb{Q}_q}$ denote the map induced by the σ_q-semilinear map carrying t to t^q, for σ_q the Witt vector q-Frobenius. That is, if $x = \sum_i c_i t^i$ with $c_i \in \mathbb{Q}_q$, then the pullback $\sigma^*(x)$ equals $\sum_i \sigma_q(c_i) t^{qi}$. We will normally use the case $q = p$, in which case σ_q is the identity map and σ is just the substitution $t \mapsto t^p$.

Definition 6.1.2. Let V be a rigid (or Berkovich) analytic subspace of $\mathbb{P}^1_{\mathbb{Q}_q}$ such that $\sigma^{-1}(V) \subseteq V$. Let $\mathcal{E}$ be a vector bundle with connection on V. A *Frobenius structure* on $\mathcal{E}$ is an isomorphism $F : \sigma^*\mathcal{E} \cong \mathcal{E}$ of vector bundles with connection on $\sigma^{-1}(V)$. We typically view F as a σ-semilinear map on $\mathcal{E}$; that is, for f a section of $\mathcal{O}$ and s a section of $\mathcal{E}$, $F(fs) = \sigma(f)F(s)$.

Most Frobenius structures arise from the following construction.

Theorem 6.1.3 (Berthelot). *Let $\mathfrak{B}$ be an open formal subscheme of the completion of $\mathbb{P}^1_{\mathbb{Z}_q}$ along its special fibre. Let $\Pi : \mathfrak{X} \to \mathfrak{B}$ be a smooth proper morphism of formal schemes over $\operatorname{Spf} \mathbb{Z}_q$. Let X, B be the Raynaud generic fibres of $\mathfrak{X}, \mathfrak{B}$, in the category of rigid analytic spaces. Let V be the subspace of B consisting of points with reduction in $\mathfrak{B}_{\mathbb{F}_q}$. Then the restriction of $H^i_{\mathrm{dR}}(X/B)$ to V admits a Frobenius structure with the property that for any $t \in \mathfrak{B}_{\mathbb{F}_q}$, for $[t] \in B^{\mathrm{an}}$ the Teichmüller lift of t, the restriction of F to $\Pi_{[t]}$ gives the Frobenius action on $H^i_{\mathrm{rig}}(\mathfrak{X}_t)$.*

Observation 6.1.4. In order to compute with a Frobenius structure, we need to make explicit how it acts in terms of differential systems. Let us do this now.

Suppose $\mathbf{v}_1, \dots, \mathbf{v}_n$ is a basis of $\mathcal{E}$, and that N is the matrix of action of $\frac{d}{dt}$ as in Observation 5.1.2. Define the $n \times n$ matrix Φ by setting

$$F(\mathbf{v}_j) = \sum_{i=1}^{5} \Phi_{ij} \mathbf{v}_i \qquad (j = 1, \dots, 5).$$

The matrix Φ will have entries in the p-adic completion of $\mathbb{Q}_q(t)$ for the Gauss norm (that is, the norm of a polynomial is the maximum norm of any of its coefficients). More precisely, modulo any power of p, the entries of Φ will be congruent to rational functions with no poles in V.

The action of Φ on column vectors is given by

$$F \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \Phi \begin{pmatrix} \sigma(f_1) \\ \vdots \\ \sigma(f_n) \end{pmatrix}.$$

Hence the effect of changing basis by a matrix U is to replace Φ by

$$U^{-1} \Phi \sigma(U).$$

The fact that Φ is an isomorphism of vector bundles with connection, not just an isomorphism of vector bundles, is expressed by the compatibility equation

$$N\Phi + \frac{d}{dt}(\Phi) = q t^{q-1} \Phi \sigma(N). \tag{6.1.4.1}$$

Given N, this expresses Φ as the solution of a differential system; that observation is the basis of the deformation method.

Example 6.1.5. In the case of cyclic cubic threefolds, the Frobenius structure and the cyclic automorphisms interact via the commutation relation

$$F \circ [\zeta_3] = [\zeta_3]^q \circ F.$$

(compare Definition 1.4.4). If $q \equiv 1 \pmod 3$, this means that the Frobenius structure acts separately on $\mathcal{E}_1$ and $\mathcal{E}_2$. That is, when written in terms of a basis as in Procedure 5.3.1, the matrix Φ splits as a block diagonal matrix in which the diagonal blocks Φ_1, Φ_2 describe the Frobenius structures on the chosen bases of $\mathcal{E}_1, \mathcal{E}_2$.

If $q \equiv 2 \pmod 3$, then $\mathcal{E}_1$ and $\mathcal{E}_2$ are interchanged rather than preserved by the Frobenius structure. Thus Φ is again a block matrix, but now it is the off-diagonal blocks which are nonzero.

6.2. Solving for the Frobenius structure. As noted above, the compatibility equation (6.1.4.1) imposes a differential equation on the entries of the matrix describing a Frobenius structure on a connection. To solve this equation, it is convenient to first solve the connection itself; we may do this using power series expansions around a point.

Lemma 6.2.1. *Let $N = \sum_{i=0}^{\infty} N_i t^i$ be an $n \times n$ matrix over $\mathbb{Q}_q[\![t]\!]$. Then there is a unique $n \times n$ matrix $U = \sum_{i=0}^{\infty} U_i t^i$ over $\mathbb{Q}_q[\![t]\!]$ with $U_0 = I_n$ satisfying*

$$NU + \frac{d}{dt}(U) = 0. \tag{6.2.1.1}$$

PROOF. (Compare [**53**, Proposition 7.3.6].) Extracting the coefficient of t^{i-1} on the left side of (6.2.1.1) gives the equation

$$iU_i = -\sum_{j=0}^{i-1} N_{i-j}U_j,$$

which determines U_i in terms of $U_0, \dots, U_{i-1}$. □

DEFINITION 6.2.2. With notation as in Lemma 6.2.1, we call U the *fundamental solution matrix* of N.

REMARK 6.2.3. One can give a quadratically convergent algorithm to compute U, in the manner of the Newton-Raphson method of approximating roots of polynomials. Start with $U = I_n$, then repeatedly replace U with

$$U\left(I_n - \int (U^{-1}NU + U^{-1}\frac{d}{dt}(U))\,dt\right).$$

After i iterations, U will agree with the fundamental solution matrix modulo t^{2^i}. However, if one is working with p-adic approximate numbers rather than exact rationals, one must be careful about p-adic numerical precision; see Remark 6.4.6 below.

We can now compute the Frobenius matrix given the initial condition of its value at $t = 0$, as follows.

LEMMA 6.2.4. *Let $N = \sum_{i=0}^{\infty} N_i t^i$ and $\Phi = \sum_{i=0}^{\infty} \Phi_i t^i$ be $n \times n$ matrices over $\mathbb{Q}_q[\![t]\!]$ satisfying* (6.1.4.1). *Let U be the fundamental solution matrix for N. Then*

$$\Phi = U\Phi_0\sigma(U)^{-1}. \tag{6.2.4.1}$$

PROOF. The compatibility equation (6.1.4.1) is preserved by the change of basis $N \mapsto U^{-1}NU + U^{-1}\frac{d}{dt}(U)$, $\Phi \mapsto U^{-1}\Phi\sigma(U)$. This implies $\frac{d}{dt}(U^{-1}\Phi\sigma(U)) = 0$; since $U \equiv I_n \pmod{t}$, we must have $U^{-1}\Phi\sigma(U) = \Phi_0$. This proves the claim. □

6.3. The deformation method. We can now describe the deformation method in the case of cyclic cubic threefolds.

PROCEDURE 6.3.1. Retain notation as in Procedure 4.2.1, but assume that $q \equiv 1 \pmod 3$. Use Procedure 5.3.1 to compute the Picard-Fuchs-Manin connection associated to the pencil of cyclic cubic threefolds in which the fibre at $t = 0$ is the Fermat cubic, while the fibre at $t = 1$ is the cyclic cubic threefold associated to the polynomial $\tilde{Q}$. Let N_1 denote the matrix of action of $\frac{d}{dt}$ on the chosen basis of $\mathcal{E}_1$. Let Φ_1 denote the matrix of action of the Frobenius structure constructed using Theorem 6.1.3 on the chosen basis of $\mathcal{E}_1$.

At $t = 0$, each basis vector is an eigenvector for the group action on the Fermat cubic given in Procedure 1.5.2. Hence we may read off the matrix $\Phi_1(0)$ as the diagonal matrix with eigenvalues computed as in Procedure 1.5.2, once we remember our choice of the identification of $\mathbb{Z}[\zeta_3]$ with a subring of $\mathbb{Z}_q$ (see Observation 3.4.1).

We now compute a t-adic approximation to the fundamental solution matrix U of N_1, to a precision to be specified later (Subsection 6.5). In $\mathbb{Q}_q[\![t]\!]$, we may thus write $\Phi_1 = U\Phi_1(0)\sigma(U)^{-1}$ by Lemma 6.2.4.

By Theorem 3.3.1 applied at the generic point, Φ_1 has entries in $\mathbb{Z}_q[\![t]\!]$. Modulo q^m, we may identify the reduction of Φ_1 as the series expansion of a rational function

with all poles congruent modulo p to poles of N_1. (This requires having a bound on the number of these poles, so we can be sure to have carried enough t-adic precision. See Subsection 6.5.)

With this done, we can evaluate this rational function at $t = 1$ to obtain the Frobenius matrix on $H^3_{\mathrm{rig}}(X)$ modulo q^m. For m as in Observation 4.3.2, this suffices to determine the zeta function of X.

Let us now carry out this computation for our chosen example of a cyclic cubic threefold over $\mathbb{F}_7$ (Example 1.6.1). For this computation, we take $m = 3$; while this is not quite enough to be sure *a priori* of uniquely determining the zeta function (Observation 4.3.2 only guarantees this for $m = 4$), we know from our previous computation that it suffices in this case (Remark 4.3.3). (Note that we also need to know that we have an integral basis of each of $\mathcal{E}_1, \mathcal{E}_2$; this follows from the fact that the basis conditions in Observation 2.3.1 are satisfied over $\mathbb{F}_7$.)

Example 6.3.2. We first compute an approximation modulo t^{500} to the fundamental solution matrix U for N_1 (see worksheet), using a quadratically convergent algorithm (Remark 6.2.3). It is somewhat time-consuming to compute this series with exact rational coefficients; since we will end up reducing modulo a small power of 7 later, we work with 7-adic coefficients with maximum relative precision 150. Even so, this requires about 15 minutes; however, it should be possible to speed this up substantially. See Remark 6.4.6.

Note that the minimum 7-adic valuation of any coefficient appearing in our approximation of U is only -3 (see worksheet). By contrast, the proof of Lemma 6.2.1 only guarantees that the entries of U modulo t^{500} have coefficients with 7-adic valuation at least

$$-\left\lfloor \frac{500}{7} \right\rfloor - \left\lfloor \frac{500}{7^2} \right\rfloor - \left\lfloor \frac{500}{7^3} \right\rfloor = -82.$$

This discrepancy is explained qualitatively by the fact that the existence of a Frobenius structure forces the entries of U to converge for t in the whole open unit disc. It is explained more quantitatively by certain explicit convergence bounds for p-adic differential equations; see Theorem 6.4.3.

Example 6.3.3. We next compute the matrix Φ_1 of action of the Frobenius structure on the chosen basis of $\mathcal{E}_1$, using the formula (6.2.4.1). In this equation, U is as computed in the previous example, while $\Phi_1(0)$ is the Frobenius matrix for the Fermat cubic threefold. By Proposition 1.5.2, the latter matrix is diagonal with diagonal entries

$$21\zeta_3 + 7, 21\zeta_3 + 7, 21\zeta_3 + 7, 21\zeta_3 + 7, -21\zeta_3 - 14$$

as computed in Example 1.5.3. Here we identify ζ_3 with the Teichmüller lift of 2 in $\mathbb{Q}_7$.

After computing Φ_1, we check (see worksheet) that $7^{-1}\Phi_1$ has entries in $\mathbb{Z}_7[\![t]\!]$, and all of the columns except the rightmost one have entries in $7\mathbb{Z}_7[\![t]\!]$.

Example 6.3.4. We next reduce $7^{-1}\Phi_1$ modulo 7^2 and multiply by the degree 218 polynomial $\Delta_1^{13}\Delta_2\Delta_3^7$. In the resulting matrix, each entry is congruent modulo t^{500} to a polynomial of degree at most 211 (see worksheet). This suggests that we have carried enough t-adic precision to identify these series as rational functions with divisors no less than

$$-13(\Delta_1) - (\Delta_2) - 7(\Delta_3) + 7(\infty).$$

We will prove that this is the case in Subsection 6.5.

EXAMPLE 6.3.5. Finally, we evaluate these polynomials at $t = 1$, then divide by $(\Delta_1^{13}\Delta_2\Delta_3^7)(1)$ to get a 7-adic matrix which is congruent to $7^{-1}\Phi_1$ modulo 7^2. Let A be a lift of this matrix to $\mathbb{Z}$. Then the coefficient of T^j in $\det(1-TA)$ agrees with the expected answer

$$1 + (3\zeta_3 + 2)T + (8\zeta_3 + 5)T^2 + (7\zeta_3 - 14)T^3 + (16\zeta_3 - 39)T^4 + (-133\zeta_3 - 126)T^5$$

from Example 3.4.3 modulo

$$\mathfrak{p}^3, \mathfrak{p}^2, \mathfrak{p}^3, \mathfrak{p}^4, \mathfrak{p}^5 \qquad (j = 1, 2, 3, 4, 5)$$

(see worksheet). Here as before, $\mathfrak{p}$ is the prime ideal $(\zeta_3 - 2)$ of $\mathbb{Z}[\zeta_3]$, which has norm 7. This is consistent with Observation 4.3.2, which predicts this agreement modulo

$$\mathfrak{p}^2, \mathfrak{p}^2, \mathfrak{p}^3, \mathfrak{p}^4, \mathfrak{p}^5 \qquad (j = 1, 2, 3, 4, 5)$$

Meanwhile, the coefficient of T^j in $\det(1-7TA^{-1})$ agrees with the expected answer

$$1 + (3\zeta_3^2 + 2)T + (8\zeta_3^2 + 5)T^2 + (7\zeta_3^2 - 14)T^3 + (16\zeta_3^2 - 39)T^4 + (-133\zeta_3^2 - 126)T^5$$

from Example 3.4.3 modulo

$$\mathfrak{p}, \mathfrak{p}, \mathfrak{p}, \mathfrak{p}, \mathfrak{p}^2 \qquad (j = 1, 2, 3, 4, 5)$$

(see worksheet). This is also consistent with Observation 4.3.2.

6.4. p-adic precision. One can significantly reduce the p-adic precision required for computing Frobenius structures by using effective bounds for convergence of solutions of fundamental solution matrices.

NOTATION 6.4.1. Let $\mathbb{Q}_q[\![t]\!]_0$ be the subring of $\mathbb{Q}_q[\![t]\!]$ consisting of series with bounded coefficient; that is,

$$\mathbb{Q}_q[\![t]\!]_0 = \mathbb{Z}_q[\![t]\!] \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$$

Let $|\cdot|$ denote the supremum norm.

Even without accounting for Frobenius structures, one obtains an extremely strong effective convergence bound for convergent solutions of bounded nonsingular differential equations on the unit disc.

THEOREM 6.4.2 (Dwork-Robba). *For $i \geq 0$, define*

$$f(i) = \sum_{j=i-n+2}^{i} \lfloor \log_p \max\{1, j\} \rfloor.$$

Let $N = \sum_{i=0}^{\infty} N_i t^i$ be an $n \times n$ matrix over $\mathbb{Q}_q[\![t]\!]_0$. Let $U = \sum_{i=0}^{\infty} U_i t^i$ be the fundamental solution matrix of N. Suppose that the entries of U and U^{-1} are convergent on the open unit disc (but not necessarily bounded). Then

$$|U_i| \leq p^{f(i)} \max\{1, |N|^{n-1}\} \qquad (i \geq 0).$$

However, it is better in general to account for Frobenius structures when possible, as follows.

THEOREM 6.4.3. *For $i \geq 0$, define*

$$g(i) = f(\lfloor iq^{-\lfloor \log_q i \rfloor} \rfloor),$$

for $f(i)$ as in Theorem 6.4.3. Let σ denote the σ_q-semilinear substitution $t \mapsto t^q$ on $\mathbb{Q}_q[\![t]\!]$. Let $N = \sum_{i=0}^{\infty} N_i t^i$ be an $n \times n$ matrix over $\mathbb{Q}_q[\![t]\!]_0$. Let $A = \sum_{i=0}^{\infty} A_i t^i$ be a matrix over $\mathbb{Q}_q[\![t]\!]_0$ with A_0 invertible, and suppose that

$$NA + \frac{d}{dt}(A) = qt^{q-1} A\sigma(N).$$

Then:

(a) *the fundamental solution matrix U of N satisfies*

$$U^{-1} A\sigma(U) = A_0;$$

(b) *we have*

$$|U_i| \leq |N|^{n-1} p^{g(i)} (|A_0^{-1}||A|)^{\lfloor \log_q i \rfloor};$$

in particular, U converges on the open unit disc.

EXAMPLE 6.4.4. In Example 6.3.2, the matrix N_1 has supremum norm bounded by 1. Theorem 6.4.2 predicts that the fundamental solution matrix modulo t^{500} has coefficients of valuation at least $-4\lfloor \log_7(500) \rfloor = -12$. On the other hand, we have a Frobenius structure given by a matrix A with $|A| = 1$ and $|A^{-1}| = 7$, so Theorem 6.4.3 implies that the fundamental solution matrix modulo t^{500} has coefficients of valuation at least -3. The latter agrees with the computed value from Example 6.3.2.

REMARK 6.4.5. The quantity $|A_0^{-1}||A|$ in Theorem 6.4.3 is determined by the difference between the greatest and least Hodge slopes of A. In case the Newton polygon of A lies strictly above the Hodge polygon, one can refine the bounds by replacing the Frobenius structure by a power of itself, whose Hodge slopes are closer to the Newton slopes (as in [**44**, Corollary 1.4.4]). We will not take advantage of this refinement here.

REMARK 6.4.6. In the situation of Theorem 6.4.2, one would like to able to compute U in a manner which is p-adically *numerically stable*, i.e., which does not require as much intermediate p-adic precision as is needed in the case when the entries of U really do have fast-growing denominators. The best one can hope for, in case $|N| = 1$, is to compute U modulo (p^m, t^N) given N modulo (p^{h+m}, t^N), where h is the number of factors of p appearing in the denominators of U modulo t^N. The algorithm of Remark 6.2.3 is quite far from this; one can do slightly better by taking p into account in a limited fashion. For instance, one can proceed as in Remark 6.2.3 but first eliminating only terms t^i with i not divisible by p, then with i not divisible by p^2, and so on. A much better algorithm would be to directly imitate a proof of Theorem 6.4.3 (see references in the appendix), but this is somewhat more complicated to implement.

In the context of Picard-Fuchs-Manin connections, one can usually maintain p-adic numerical stability by writing the differential equation as a linear recursion of *finite length* (with matrix coefficients). That way, one can control the p-adic precision loss rather directly; for instance, see [**61**, Theorem 5.1] or [**40**, Theorem 2].

6.5. t-adic precision. To complete the description of the deformation method, we must explain how to bound the degree of a rational function given by reducing a Frobenius matrix modulo a power of p, so that we can provably recover this rational function by computing some specific number of coefficients of its Taylor expansion around $t = 0$. We start with a qualitative result.

DEFINITION 6.5.1. Set notation as in Theorem 6.1.3. A *strict neighborhood* of V is a rigid analytic subspace W of $\mathbb{P}^1_{\mathbb{Q}_q}$ containing V, consisting of a closed disc of radius strictly greater than 1 around the origin, minus finitely many open discs of discs of radius strictly less than 1 centered at points in the closed unit disc. In more geometric terms, W is a neighborhood of V within $\mathbb{P}^1_{\mathbb{Q}_q}$ containing V in its relative interior.

THEOREM 6.5.2 (Berthelot). *Set notation as in Theorem 6.1.3. Then the Frobenius structure F extends over some strict neighborhood of V.*

REMARK 6.5.3. This implies that the reduction of the matrix Φ modulo p^n is a rational function of total degree bounded by some linear function of n. However, we do not obtain an effective bound either on the slope or the constant term of this linear function. For this, we need the quantitative Theorem 6.5.10 below.

REMARK 6.5.4. In the language of p-adic cohomology, Theorem 6.5.2 asserts that the relative rigid cohomology in this setting forms an *overconvergent F-isocrystal* on the smooth locus of the family. For more discussion of this concept, see the appendix.

To obtain a quantitative refinement of Theorem 6.5.10, one could apply known precision bounds for the direct method (Subsection 4.4) to the generic fibre. However, since these bounds are known experimentally to be suboptimal, this will result is a suboptimal refinement. One can do much better by making a careful analysis of Frobenius structures on connections over a p-adic disc, as follows.

We first observe that we can convert the Frobenius structure from one Frobenius lift to another, using Taylor series.

THEOREM 6.5.5. *With notation as in Theorems 6.1.3 and 6.5.2, let $\sigma' : \mathbb{P}^1_{\mathbb{Q}_q} \to \mathbb{P}^1_{\mathbb{Q}_q}$ be any σ_q-semilinear map carrying t to something congruent to t^q mod p. Then $H^i_{\mathrm{dR}}(X/B)$ also admits a Frobenius structure F' on a strict neighborhood of V with respect to σ', defined by*

$$F'(\mathbf{v}) = \sum_{i=0}^{\infty} \frac{1}{i!}(\sigma'(t) - \sigma(t))^i F\left(\frac{d^i}{dt^i}(\mathbf{v})\right). \tag{6.5.5.1}$$

This computes the Frobenius matrix on a fibre $\mathfrak{X}_t$ by specialization to the unique lift of t carried to its σ_q-image by σ'.

PROOF. The series converges on a strict neighborhood because the presence of the Frobenius structure forces the generic radius of convergence of the connection to equal 1 [**53**, Proposition 17.2.3]. Given that, the Leibniz rule implies first that on the trivial connection module (i.e., functions on $\mathbb{P}^1_{\mathbb{Q}_q}$),

$$F'(t) = t + (\sigma'(t) - \sigma(t))F(t) = \sigma'(t).$$

(This observation is a good way to remember the formula (6.5.5.1).) The Leibniz rule then implies that on any connection module, F is semilinear for σ'. For more details, see references in the appendix. □

EXAMPLE 6.5.6. In the situation of Example 6.3.2, we compute the Frobenius structure with respect to the map σ' given by

$$\sigma'(t) = (t+3)^7 - 3,$$

modulo 7^3. Let Φ_1' be the matrix of action on our chosen basis. Given the series representation of the matrix $7^{-1}\Phi_1$ modulo 7^3, we compute by (6.5.5.1)

$$\begin{aligned} 7^{-1}\Phi_1' \equiv 7^{-1}\Phi_1 + ((t+3)^7 - 3 - t^7)7^{-1}\Phi_1\sigma(N_1) \\ + \frac{1}{2}((t+3)^7 - 3 - t^7)^2 7^{-1}\Phi_1\sigma\left(N_1^2 + \frac{d}{dt}(N_1)\right) \pmod{7^3}. \end{aligned}$$

To recover the characteristic polynomial of the fibre of $\mathfrak{X}_{\mathbb{F}_7}$ above $t = 1$, we must specialize Φ_1' to the unique point in that residue disc which is fixed by the map $t \mapsto (t+3)^7 - 3$. This point is none other than $\zeta_3^2 - 3 \equiv 15 \pmod{7^3}$ (see worksheet). Clearing denominators and then evaluating at this point, we obtain another characteristic polynomial with the same accuracy as in Example 6.3.5 (see worksheet).

The point of converting the Frobenius structure is to be able to take advantage of the following fact [**53**, Proposition 17.5.1].

LEMMA 6.5.7. *Let $N = \sum_{i=-1}^{\infty} N_i t^i$ be an $n \times n$ matrix such that the entries of tN are power series over $\mathbb{Q}_q$ convergent on the open unit disc, and N_{-1} is a nilpotent matrix. Let $\Phi = \sum_{i=-\infty}^{\infty} \Phi_i t^i$ be an $n \times n$ matrix whose entries are Laurent series over $\mathbb{Q}_q$ convergent on some open annulus with outer radius 1. Suppose that N, Φ satisfy* (6.1.4.1). *Then $\Phi_i = 0$ for $i < 0$, so Φ converges on the whole open unit disc.*

COROLLARY 6.5.8. *Retain notation as in Lemma 6.5.7, except now assume only that the eigenvalues $\lambda_1, \dots, \lambda_n$ of N_{-1} are rational numbers with denominators coprime to p. Then $\Phi_i = 0$ whenever*

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

PROOF. We may adjoin $t^{1/m}$ for m coprime to p if necessary, to reduce to the case where $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$. In that case, by Lemma 5.1.6, we can find an invertible $n \times n$ matrix U over $\mathbb{Q}_q(t)$ such that $U^{-1}tNU + U^{-1}t\frac{d}{dt}(U)$ is holomorphic at $t = 0$ and its reduction modulo t is nilpotent; we can moreover ensure that $t^b U$ and $t^{-a}U^{-1}$ are holomorphic at $t = 0$, for $a = \min_i\{\lambda_i\}$ and $b = \max_i\{\lambda_i\}$. Under this change of basis, Φ is replaced by $U^{-1}\Phi\sigma(U)$, which by Lemma 6.5.7 is holomorphic at $t = 0$. The claim follows. □

EXAMPLE 6.5.9. In Example 6.5.6, the new Frobenius lift sends $t+3$ to $(t+3)^7$, so we may apply Corollary 6.5.8 by translating the point -3 to the origin. By so doing, we deduce that the new Frobenius structure has a pole of order at worst

$$\lfloor 7 \cdot 1 - 0 \rfloor = 7.$$

In fact, if we compute modulo 7^3, we only see a pole of order 6 (see worksheet).

We can now state a quantitative refinement of Theorem 6.5.2. This result is not best possible; see Remark 6.5.12 and the optional part of this lecture.

THEOREM 6.5.10. *Assume $p > 2$. Fix a positive integer m. Let B be an open dense subscheme of $\mathbb{P}^1_{\mathbb{Q}_q}$ whose complement Z consists of points with distinct reductions modulo p, one of which is the point ∞. Let $\mathcal{E}$ be a vector bundle with*

connection on B which is everywhere regular, with all exponents in $\mathbb{Q} \cap \mathbb{Z}_p$. Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ be a basis of $\mathcal{E}$, and let N be the matrix of action of $\frac{d}{dt}$ on this basis.

For $z \in Z$, define the quantities $f(z)$ and $g(z)$ as follows. Choose a matrix U over $\mathbb{Q}_q(t)$ such that the basis $\mathbf{w}_j = \sum_i U_{ij}\mathbf{v}_i$ is regular at z. Let $\lambda_{z,1}, \dots, \lambda_{z,n}$ be the exponents of this basis at z. Put

$$f(z) = \lfloor -qv_t(U^{-1}) - v_t(U) - q \min_j\{\lambda_j\} + \max_j\{\lambda_j\} \rfloor,$$

where v_t denotes the $(t-z)$-adic valuation, and $v_t(U) = \min_{i,j}\{v_t(U_{ij})\}$. Put $g(z) = 0$ if the residue matrix of $\mathbf{w}_1, \dots, \mathbf{w}_n$ vanishes at z, or if $z \in \{0, \infty\}$; otherwise, let $g(z)$ be the least nonnegative integer i for which $i - \lfloor (i-1)/(p-1) \rfloor \geq m-1$.

Let V be the rigid analytic subspace of $\mathbb{P}^1_{\mathbb{Q}_q}$ given as the complement of the residue discs containing points of Z. Suppose that $\mathcal{E}$ admits a Frobenius structure F on a strict neighborhood of V, and that the matrix Φ of action of F on $\mathbf{v}_1, \dots, \mathbf{v}_n$ has nonnegative Gauss valuation. Then Φ is congruent modulo p^m to a rational function with divisor bounded below by

$$\sum_{z \in Z} -(f(z) + qg(z))(z).$$

PROOF. It suffices to check that the contribution of each $z \in Z$ to the divisor is at least $-(f(z) + qg(z))(z)$. To see this, we see that using a Frobenius lift carrying $(t-z)$ to $(t-z)^q$, we get a pole of order at most $f(z)$ at z by Corollary 6.5.8. We then apply Theorem 6.5.5 to convert back to the original Frobenius (this step being unnecessary if $z = 0, \infty$), noting that the p-adic valuation of the term $(\sigma'(t) - \sigma(t))^i/i!$ is at least $i - \lfloor (i-1)/(p-1) \rfloor$. □

EXAMPLE 6.5.11. In Example 6.3.4, we use Theorem 6.5.10 to bound the pole divisor of $7^{-1}\Phi_1$ modulo 7^2; this is valid because the poles are distinct mod 7. In concrete terms, the roots of $\Delta_1\Delta_3$ in an algebraic closure of $\mathbb{Q}_7$ lie in the integral closure of $\mathbb{Z}_7$ and are distinct modulo 7 (see worksheet).

For z a root of $\Delta_1, \Delta_2, \Delta_3$ or the value ∞, using the computation of exponents in Example 5.3.2, we compute respectively

$$f(z) = 7, 1, 8, -7$$
$$g(z) = 1, 0, 1, 0.$$

The values of g are clear, but it is worth explaining where the values of f came from.

For $z = -3$ the unique root of Δ_1, we computed $f(z) = 7$ in Example 6.5.9. For z a root of Δ_2, we have $f(z) = 1 - 7 \cdot 0 = 1$ because the exponents are $0, 1$. For z a root of Δ_3, we have

$$f(z) = \left\lfloor 0 - 7 \cdot \left(-\frac{7}{6} \right) \right\rfloor = \left\lfloor \frac{49}{6} \right\rfloor = 8.$$

For $z = \infty$, we get a contribution of 1 from the change of basis matrix U to a regular basis, and a contribution of

$$\left\lfloor \frac{5}{3} - 7 \cdot \frac{4}{3} \right\rfloor = \left\lfloor -\frac{23}{3} \right\rfloor = -8$$

from the exponents.

We thus get a lower bound of

$$-14(\Delta_1) - (\Delta_2) - 15(\Delta_3) + 7(\infty)$$

for the pole divisor. In particular, this divisor has degree $-14 \cdot 1 - 1 \cdot 23 - 15 \cdot 26 + 8 \cdot 1 = -419$, so we need the Taylor series expansions around $t = 0$ within $O(t^{420})$ to guarantee that we have correctly identified the rational functions. Since we computed to order $O(t^{500})$ in Example 6.3.4, the computation is validated.

REMARK 6.5.12. Note the discrepancy between the lower bound

$$-14(\Delta_1) - (\Delta_2) - 15(\Delta_3) + 7(\infty)$$

given in Example 6.5.11 and the computed divisor

$$-13(\Delta_1) - (\Delta_2) - 7(\Delta_3) + 7(\infty).$$

This correctly suggests that there is a lot more work to be done in the area of analyzing the pole orders of Frobenius structures of Picard-Fuchs-Manin connections. We make a few remarks in the optional addendum to this lecture, but otherwise the subject is very much open.

REMARK 6.5.13. By making the substitution $t_1 = t^2 - 3$ and changing basis on the Frobenius matrix in Example 6.5.9, we can get a matrix which is holomorphic at $t_1 = 0$. The reduction modulo t_1 has eigenvalues congruent to

$$21, 161, 35, 14, 324 \pmod{7^3}$$

(see worksheet). The last of these is the reduction of ζ_3 modulo $\mathfrak{p}$. The other four are supposed to appear in the zeta function of the singular cubic threefold defined by $a^3 = Q_{-3}$ over $\mathbb{F}_7$. (To prove this relationship requires either an appeal to Dwork's deformation theory for singular hypersurfaces, or a comparison theorem between de Rham cohomology and Hyodo-Kato cohomology which does not seem to have been written down yet.)

6.6. Optional: Further analysis of t-adic precision. In some cases, the following refinement of Corollary 6.5.8 may be useful.

LEMMA 6.6.1. *With notation as in Corollary 6.5.8, for each $\alpha \in \mathbb{Q}$, put*

$$S_\alpha = \{\lambda_1, \dots, \lambda_n\} \cap (\alpha + \mathbb{Z}).$$

If

$$i < p \min S_\alpha - \max S_\alpha$$

for all α, then $\Phi_i = 0$.

PROOF. We first check that there exists a matrix $V = \sum_{i=0}^{\infty} V_i t^i$ with entries in $\mathbb{Q}_q[\![t]\!]$ such that $N' = V^{-1}NV + V^{-1}\frac{d}{dt}(V) = \sum_{i=-1}^{\infty} N'_i t^i$ is block diagonal, any two eigenvalues of N'_{-1} in the same block differ by an integer, and no two eigenvalues of N'_{-1} occurring in different blocks differ by an integer. To show this, we first choose V_0 so that $V_0^{-1}N_{-1}V_0$ is block diagonal with blocks corresponding to different classes in $\mathbb{Q}/\mathbb{Z}$. Next suppose $V_0, \dots, V_{j-1}$ have been chosen to put N into the right form modulo t^{j-1}. Put $N_W = W^{-1}NW + W^{-1}\frac{d}{dt}(W)$ for $W = \sum_{i=0}^{j-1} V_i t^i$, and write $N_W = \sum_{i=0}^{\infty} N_{W,i} t^i$.

If we change basis on N_W using $I_n + t^j X$, modulo t^j we get

$$N_W + t^{j-1}(-XN_{-1} + N_{-1}X + jX).$$

For X concentrated in a single off-diagonal block corresponding to the congruence classes $\alpha + \mathbb{Z}$, $\beta + \mathbb{Z}$, the operation $X \mapsto -XN_{-1} + N_{-1}X + jX$ has eigenvalues in the set $\pm\{\alpha - \beta + \mathbb{Z}\}$, which does not contain zero. We can thus choose X so that changing basis using $W(I_n + t^j X)$ puts N into the correct form modulo t^j. We may thus proceed by induction to deduce the claim.

If we apply Lemma 6.5.7 to the result of changing basis by a suitably t-adically close approximation of V, we may now deduce the desired result. □

Remark 6.6.2. If one has a family of pencils of varieties, one gets a family of Picard-Fuchs-Manin connections admitting Frobenius structures. If one can use Theorem 6.5.10 to bound the pole orders of the Frobenius modulo p^n for a generic member of this family, the same bound will apply to each special member, even if it does not have all of its poles in distinct residue classes mod p. In practice, this may significantly improve the range of applicability of the deformation method.

Remark 6.6.3. In light of Remark 6.6.2, it would be useful to have a completely general analogue of Theorem 6.5.10 that makes no hypothesis on the poles of the connection being distinct mod p. Some more experimentation may be necessary in order to correctly formulate an appropriate conjecture.

Remark 6.6.4. One can improve the bound in Theorem 6.5.10 so that $g(z) - m$ is only logarithmic in m, rather than linear in m, by using effective convergence bounds for p-adic differential equations, as in Theorem 6.4.3. (This would allow allow for the use of $p = 2$, which is impossible with a bound of the form given in Theorem 6.5.10.) See [**56**].

Appendix A. Notes and further reading

In this appendix, we provide references omitted in the main text, in a sequence of subsections keyed to the six lectures. We finish with suggestions for further reading.

A.1. Zeta functions: generalities. There is a useful, if brief, introduction to zeta functions and the Weil conjectures in Hartshorne's algebraic geometry textbook [**35**, Appendix C]. See also the survey by Osserman [**78**].

The analytic continuation of the L-function of an elliptic curve over $\mathbb{Q}$ was proved by Breuil, Conrad, Diamond, and Taylor [**8**] following the method introduced by Wiles [**95**] and Taylor-Wiles [**91**].

Lemma 1.2.3 is taken from [**50**], where it is used to give an algorithm (implemented in `Sage`) for searching for Weil polynomials subject to congruence conditions. However, this algorithm is only designed to handle polynomials over $\mathbb{Z}$; we are not aware of any algorithms designed to handle situations where a Weil polynomial is known to have a factorization over a larger field, as happens for cyclic cubic threefolds.

The strongest notion of a Weil cohomology theory includes Poincaré duality, cycle class maps, the Künneth decomposition theorem, a Lefschetz hyperplane theorem, plus additional compatibilities. See [**57**] for more details.

For a development of étale cohomology, see the books of Freitag and Kiehl [**27**], Milne [**73**], and Tamme [**90**]. The course notes of Milne [**74**] may also be helpful.

The computation of the zeta function of diagonal hypersurfaces is originally due to Weil. It was one of the two main justifications for his original assertion

of the Weil conjectures, the other being his proof of the conjectures for curves (generalizing Hasse's theorem bounding the number of points on an elliptic curve over a finite field).

For further discussion of Jacobi sums, including the case $q \neq p$, the definitive reference is [**3**].

A.2. Algebraic de Rham cohomology. The standard development of algebraic de Rham cohomology is that of Hartshorne [**34**]. However, it might be helpful to become acquainted with the complex-analytic situation first, by reading about it in Griffiths and Harris [**31**]. For Grothendieck's comparison theorem (Theorem 2.1.3), see [**32**].

To compute the algebraic de Rham cohomology of a smooth complete intersection inside a toric variety, one has a generalization of the Griffiths-Dwork method; this calculation has become fashionable of late because it can be used to generate putative instances of mirror symmetry. See Cox and Katz [**17**].

A.3. de Rham cohomology and p-adic cohomology. A useful overview of p-adic cohomologies is the survey of Illusie [**41**]. The subject has developed considerably since that survey was written; a more recent but more advanced survey is [**52**].

Before the book of le Stum [**66**] appeared, there was no proper foundational treatise on rigid cohomology; instead, one was forced to infer much of the theory from the articles of Berthelot. Fortunately, these are quite readable, and even now may prove helpful; we suggest in particular the introductory article [**4**] for the general construction, and the later article [**5**] for details on the comparisons between rigid cohomology, Monsky-Washnitzer cohomology, and crystalline cohomology. Theorem 3.2.1 is a logarithmic version of Berthelot's original comparison theorem, given by Baldassarri and Chiarellotto [**2**]. The integral version (Theorem 3.2.2) is due in the logarithmic case to Shiho [**84, 85**].

The fact that p-adic cohomology is a Weil cohomology includes a great many assertions, some of which were only proved quite recently. For example, finite dimensionality was established by Berthelot in [**5**], while Poincaré duality and the Künneth formula were established by Berthelot [**6**]. The Riemann hypothesis component of the Weil conjectures in p-adic cohomology was originally proved by Katz and Messing [**45**] by reducing to Deligne's ℓ-adic version [**19**]; see [**12**] for a similar argument. Purely p-adic proofs were later given by Faltings [**26**] and Kedlaya [**49**]. The construction of cycle classes is due to Petrequin [**79**]; this is needed for the full Lefschetz trace formula (Remark 1.3.3).

Mazur's theorem comparing the Hodge filtration with divisibility in the Frobenius matrix (originally a conjecture of Katz) was originally announced in [**69**] and proved in [**70**]. Another treatment is given by Berthelot and Ogus in [**7**]. See also the discussion in [**41**].

A.4. The direct method for cyclic cubic threefolds. The Frobenius action on affine varieties comes from the comparison between rigid and Monsky-Washnitzer cohomology. The original development of the latter occurs in the three papers [**77, 75, 76**]; compare also [**94**]. One may also use this comparison to deduce the cases of the Lefschetz trace formula in rigid cohomology that we need, as the proof for the Frobenius map given in [**76**] extends to cover the composition of Frobenius with an automorphism. (This only applies to affine varieties; to deduce

the general case, one must first apply Poincaré duality to switch to cohomology with compact supports, then use the excision property there.)

The original use of p-adic methods for computing zeta functions arose in the context of finding suitable curves for elliptic curve cryptography, namely those for which the group of rational points has order equal to a prime number times a very small cofactor. Methods introduced in this setting include the canonical lift method of Satoh [**82**] and the AGM iteration of Mestre [**72**]. These can in principle be extended to higher genus (see for example [**65**] for a higher genus version of Mestre's method), but the dependence on the genus is quite poor; most practical interest has concentrated on genera 2 and 3, which also have some relevance for cryptography. (See [**16**] for a survey of elliptic and hyperelliptic curve cryptography circa 2005.)

The first attempt to use p-adic methods to give more general algorithms for computing zeta functions was given by Lauder and Wan [**64**]. They gave a general algorithm based on Dwork's proof of the rationality of the zeta function. This can be interpreted as an application of p-adic cohomology, but where one computes not in the cohomology but in the chain complex, in which the the terms are infinite-dimensional vector spaces which must be truncated appropriately. The first algorithm involving a calculation on p-adic cohomology itself was Kedlaya's algorithm for hyperelliptic curves in odd characteristic [**47**]; see also the exposition by Edixhoven [**25**], and note the correction to the precision bound given in the errata to [**47**]). An analogous algorithm for characteristic 2 was given by Denef and Vercauteren [**21**]. The method has been generalized to rather general families of curves (nondegenerate curves in toric surfaces) by Castryck, Denef, and Vercauteren [**10**]. (See [**48**] for a survey of this subject circa 2004.)

Less work has been carried out in higher dimensions, partly because the case of curves carried some external interest from cryptography, and partly because in higher dimensions the deformation method has better asymptotic complexity. The approach we describe here was given by Abbott, Kedlaya, and Roe in [**1**], but that paper only gives experimental results for surfaces. A closer analogue of Kedlaya's original algorithm, for cyclic covers of projective spaces, has been implemented by de Jong [**18**] but currently lacks rigorous error bounds. (We expect that one can adapt the analysis of [**1**] to de Jong's situation, but to our best knowledge no one has attempted to do so.) It might be feasible to use de Jong's method to compute zeta functions of cyclic cubic threefolds, but we did not investigate this thoroughly; we used the approach from [**1**] instead so that we could reuse the setup to derive the Picard-Fuchs-Manin connection.

It is also worth mentioning the work of Harvey [**36**], who found a restructuring of Kedlaya's algorithm for hyperelliptic curve that reduces the complexity in the characteristic p of the finite field from linear to square-root. This has had the effect of making p-adic cohomology applicable in far larger characteristics than had been previously expected; this was demonstrated experimentally for hyperelliptic curves of genus 2 and 3 by Kedlaya and Sutherland [**55**]. (Interestingly, Harvey's motivation was not computing zeta functions, but rather computing cyclotomic p-adic canonical heights of elliptic curves over $\mathbb{Q}$ using the method of Mazur, Stein and Tate [**71**].)

Even more recently, Harvey has described a higher-dimensional analogue of his work for hyperelliptic curves, which might make the direct method feasible for

such examples as cyclic cubic threefolds. One key difference from [**1**] is that the reduction algorithm is translated from a problem of commutative algebra into a reasonably compact problem of linear algebra. This has the effect of avoiding the use of dense multivariate polynomials, leading to improved asymptotic behavior especially as the characteristic grows. As of this writing, Harvey's work is still in preparation, but see [**37**].

A.5. Picard-Fuchs-Manin connections. We are not sure where the name "Gauss-Manin connection" comes from. In [**32**, footnote 13], Grothendieck proposes the existence of a "canonical connection" on relative algebraic de Rham cohomology, inspired by Manin's use of such a construction in his proof of the analogue of the Mordell conjecture over complex function fields [**68**]. (Grothendieck suggests that such a connection could be used to define a Leray spectral sequence; Definition 5.2.2 shows that the reverse is actually what happens!) This explains the inclusion of Manin's name; the reference to Gauss appears to invoke the theory of hypergeometric differential equations while skipping over the intervening history of Picard-Fuchs differential equations.

For the holomorphicity of the topological Picard-Fuchs-Manin connection, see [**31**]. For the fact that it agrees with the algebraic connection, see [**46**].

Theorem 5.2.5 is a theorem originally due to Griffiths, but many proofs are possible. See [**30**, Theorem 3.1] for an overview.

For more on the use of Lefschetz pencils in algebraic geometry, see Katz's exposés in SGA 7 [**20**, Exposés XVII, XVIII].

A.6. The deformation method for cyclic cubic threefolds. The existence of a Frobenius structure on a Picard-Fuchs-Manin connection was originally observed in a number of examples by Dwork, notably including the Legendre family of elliptic curves [**22**]. See van der Put [**94**] for a modern treatment of this example. Theorem 6.1.3 is a corollary of Theorem 6.5.2, for more on which see below.

The original idea of using the Frobenius structure on a Picard-Fuchs-Manin connection to compute zeta functions is due to Lauder [**59**], who described an algorithm for smooth projective hypersurfaces using Dwork cohomology. Lauder later gave an alternate development using relative Monsky-Washnitzer cohomology [**60**]; a similar development was given by Gerkmann [**28**], and this is what we have followed in these notes.

The deformation method has also been used by Hubrechts [**38**] to give more efficient point counting algorithms for elliptic curves than is possible using the direct method. Additional work has been done for hyperelliptic curves by Hubrechts [**39, 40**], and for $C_{a,b}$ curves by Castryck, Hubrechts, and Vercauteren [**11**]. (It is worth studying Hubrechts's work for its significant improvements over what we have described here, in the space and memory requirements used for carrying out the deformation method.)

It is an interesting open question whether there is an analogue of Harvey's method (reducing the dependence on p to square-root) for the deformation method. The recent work of Hubrechts on memory-efficient use of the deformation method [**40**] provides a clue, as it uses the same baby step-giant step trick (due to Chudnovsky and Chudnovsky) as in Harvey's method; however, there is an additional step needed of repackaging the algorithm so that one never explicitly writes down a power series involving $O(p)$ terms.

Theorem 6.4.2 is due to Dwork and Robba [**24**]; see also [**23**, Theorem IV.3.1]. Theorem 6.4.3 is an effective version due to Kedlaya [**53**, Theorem 18.3.3] of a bound due to Chiarellotto and Tsuzuki [**13**, Proposition 6.10].

Theorem 6.5.2 is due to Berthelot [**4**, Théorème 5]. A conjecture of Berthelot (in the constant coefficient case) and Shiho (in general) asserts that more generally, for any smooth proper morphism between varieties over a field of characterisic $p > 0$, the relative rigid cohomology should exist as an overconvergent F-isocrystal. This is known in certain cases by work of Tsuzuki [**93**] and Shiho [**86, 87, 88**]; it is likely to be proved soon using Caro's construction of a category of p-adic coefficients (overholonomic arithmetic $\mathcal{D}$-modules), as completed recently by Caro and Tsuzuki [**9**].

In previous published work on the deformation method, e.g. [**28**], the t-adic precision is controlled by the method suggested above Theorem 6.5.5, i.e., by using p-adic precision loss bounds in the direct method as applied over the generic fibre of the base. To the best of our knowledge, the method described here has not been used previously, though Alan Lauder informs us that he is using it currently. (See also [**63**] for another appearance of this technique.)

Theorem 6.5.5 is implicit in the work of Berthelot [**4**]; it follows from the overconvergence of the Taylor series map, which is built into Berthelot's definition of an overconvergent F-isocrystal. The argument has been made explicit several times in the literature, e.g., [**92**, Theorem 3.4.10] and [**53**, Proposition 17.3.1].

A.7. Additional suggestions. These notes are loosely inspired by the author's notes for the 2007 Arizona Winter School [**51**]. We have attempted here to focus more on computational aspects of the deformation method; consequently, comparing the two documents may be profitable.

For varieties of dimension greater than 1, Lauder has also introduced a "fibration method" for computing zeta functions [**61**]. This shares the advantage held by the deformation method of involving only one-dimensional varieties at any given step, but does not require the auxiliary construction of the Frobenius structure on an entire Picard-Fuchs-Manin connection. Lauder has obtained good experimental results in the case of elliptic surfaces; these appear in [**62**].

In principle, all three of the approaches to effective p-adic cohomology (direct, deformation, fibration) should be applicable to appropriate classes of mildly singular varieties, but a fair bit of care must be applied. Some analysis along these lines, including some positive numerical results, has been made by Kloosterman [**58**]. Dealing with singular fibres properly requires effective convergence bounds for logarithmic connections with nilpotent residues (improving upon work of Christol-Dwork); these can be found in [**53**, Chapter 18]. It also requires checking some compatibilities between Hyodo-Kato Frobenius actions and Picard-Fuchs-Manin connections; to our knowledge, these have not been checked in general.

References

[1] T.G. Abbott, K.S. Kedlaya, and D. Roe, Bounding Picard numbers of surfaces using p-adic cohomology, in *Arithmetic, Geometry and Coding Theory (AGCT 2005)*, Séminaires et Congrès 21, Societé Mathématique de France, 2009, 125–159.

[2] F. Baldassarri and B. Chiarellotto, Algebraic versus rigid cohomology with logarithmic coefficients, in *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, Perspect. Math. 15, Academic Press, San Diego, 1994, 11–50.

[3] B.C. Berndt, R.J. Evans, and K.S. Williams, *Gauss and Jacobi Sums*, Canadian Math. Soc. Monographs 21, Wiley-Interscience, 1998.
[4] P. Berthelot, Géométrie rigide et cohomologie des variétés algébriques de caractéristique p, Introductions aux cohomologies p-adiques (Luminy, 1984), *Mém. Soc. Math. France* **23** (1986), 7–32.
[5] P. Berthelot, Finitude et pureté cohomologique en cohomologie rigide, *Invent. Math.* **128** (1997), 329–377.
[6] P. Berthelot, Dualité de Poincaré et formule de Künneth en cohomologie rigide, *C.R. Acad. Sci. Paris Sér. I Math.* **325** (1997), 493–498.
[7] P. Berthelot and A. Ogus, *Notes on Crystalline Cohomology*, Princeton Univ. Press, Princeton, 1978.
[8] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.
[9] D. Caro and N. Tsuzuki, Overholonomicity of overconvergent F-isocrystals on smooth varieties, arXiv:0803.2015v1 (2008).
[10] W. Castryck, J. Denef, and F. Vercauteren, Computing zeta functions of nondegenerate curves, *Int. Math. Res. Papers* **2006**, article ID 72017 (57 pages).
[11] W. Castryck, H. Hubrechts, and F. Vercauteren, Computing zeta functions in families of $C_{a,b}$ curves using deformation, in *Algorithmic Number Theory (ANTS VIII)*, Lecture Notes in Computer Science 5011, Springer, New York, 2008, 296–311.
[12] B. Chiarellotto and B. le Stum, Sur la pureté de la cohomologie cristalline, *C. R. Acad. Sci. Paris Sér. I Math.* **326** (1998), 961–963.
[13] B. Chiarellotto and N. Tsuzuki, Logarithmic growth and Frobenius filtrations for solutions of p-adic differential equations, *J. Inst. Math. Jussieu* **8** (2009), 465–505.
[14] G. Christol and B. Dwork, Effective p-adic bounds at regular singular points, *Duke Math. J.* **62** (1991), 689–720.
[15] C.H. Clemens and P.A. Griffiths, The intermediate Jacobian of the cubic threefold, *Ann. of Math.* **95** (1972), 281–356.
[16] H. Cohen and G. Frey (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2005.
[17] D.A. Cox and S. Katz, *Mirror Symmetry and Algebraic Geometry*, Math. Surveys and Monographs 68, Amer. Math. Soc., 1999.
[18] A.J. de Jong, Frobenius project; see `http://math.columbia.edu/~dejong/`.
[19] P. Deligne, La conjecture de Weil. I, *Publ. Math. IHÉS* **43** (1974), 273–307.
[20] P. Deligne and N. Katz (eds.), *Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II): Groupes de monodromie en géométrie algébrique. II*, Lecture Notes in Math. 340, Springer-Verlag, Berlin, 1973.
[21] J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2, *J. Cryptology* **19** (2006), 1–25.
[22] B. Dwork, *Lectures on p-adic Differential Equations*, Grundlehren 253, Springer-Verlag, 1982.
[23] B. Dwork, G. Gerotto, and F. Sullivan, *An Introduction to G-Functions*, Annals of Math. Studies 133, Princeton University Press, Princeton, 1994.
[24] B. Dwork and P. Robba, Effective p-adic bounds for solutions of homogeneous linear differential equations, *Trans. Amer. Math. Soc.* **259** (1980), 559–577.
[25] B. Edixhoven, Point counting after Kedlaya, course notes at `http://www.math.leidenuniv.nl/~edix/oww/mathofcrypt/`.
[26] G. Faltings, F-isocrystals on open varieties: results and conjectures, in *The Grothendieck Festschrift, Vol. II*, Progr. Math., 87, Birkhüser, Boston, 1990, 219–248.
[27] E. Freitag and R. Kiehl, *Étale Cohomology and the Weil Conjectures* (translated from the German by B.S. Waterhouse and W.C. Waterhouse), Ergebnisse der Math. 13, Springer-Verlag, Berlin, 1988.
[28] R. Gerkmann, Relative rigid cohomology and deformation of hypersurfaces, *Int. Math. Res. Papers* **2007**, article ID rpm003 (67 pages).
[29] P.A. Griffiths, On the periods of certain rational integrals I, II, *Ann. of Math.* **90** (1969), 460–495; *ibid.* **90**, 496–541.
[30] P.A. Griffiths, Periods of integrals on algebraic manifolds: Summary of main results and discussion of open problems, *Bull. Amer. Math. Soc.* **76** (1970), 228–296.
[31] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, John Wiley & Sons, 1978.

[32] A. Grothendieck, On the De Rham cohomology of algebraic varieties, *Publ. Math. IHÉS* **29** (1966), 95–103.
[33] G.-M. Greuel and Gerhard Pfister, A `Singular` Introduction to Commutative Algebra, Springer-Verlag, Berlin, 2002.
[34] R. Hartshorne, On the De Rham cohomology of algebraic varieties, *Publ. Math. IHÉS* **45** (1975), 5–99.
[35] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. 52, Springer, New York, 1977.
[36] D. Harvey, Kedlaya's algorithm in larger characteristic, *Int. Math. Res. Notices* **2007**, article ID rnm095 (29 pages).
[37] D. Harvey, Counting points on projective hypersurfaces, lecture notes available at `http://www.cims.nyu.edu/~harvey/`.
[38] H. Hubrechts, Quasi-quadratic elliptic curve point counting using rigid cohomology, conference *MEGA 2007* (2007).
[39] H. Hubrechts, Point counting in families of hyperelliptic curves in characteristic 2, *LMS J. Comput. Math.* **10** (2007), 207–234.
[40] H. Hubrechts, Point counting in families of hyperelliptic curves, *Found. Comput. Math.* **8** (2008), 137–169.
[41] L. Illusie, Crystalline cohomology, in *Motives*, Proc. Sympos. Pure Math., vol. 55, part 1, Amer. Math. Soc. Providence, RI, 1994, 43–70.
[42] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second edition, Graduate Texts in Math. 84, Springer-Verlag, 1990.
[43] K. Kato, Logarithmic structures of Fontaine-Illusie, in *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, Johns Hopkins Univ. Press, Baltimore, 1989, 191–224.
[44] N.M. Katz, Slope filtration of F-crystals, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, *Astérisque* **63** (1979), 113–163.
[45] N.M. Katz and W. Messing, Some consequences of the Riemann hypothesis for varieties over finite fields. *Invent. Math.* **23** (1974), 73–77.
[46] N.M. Katz and T. Oda, On the differentiation of de Rham cohomology classes with respect to parameters. *J. Math. Kyoto Univ.* **8** (1968), 199–213.
[47] K.S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* **16** (2001), 323–338; errata, *ibid.* **18** (2003), 417–418.
[48] K.S. Kedlaya, Computing zeta functions via p-adic cohomology, in D.A. Buell (ed.), *Algorithmic Number Theory (ANTS 2004)*, Lecture Notes in Comp. Sci. 3076, 2004, 1–17.
[49] K.S. Kedlaya, Fourier transforms and p-adic "Weil II", *Compos. Math.* **142** (2006), 1426–1450.
[50] K.S. Kedlaya, Search techniques for root-unitary polynomials, in K.E. Lauter and K. Ribet (eds.), *Computational Arithmetic Geometry*, Contemp. Math. 463, Amer. Math. Soc., 2008, 71–82. Associated `Sage` package available at `http://math.mit.edu/~kedlaya/papers/`.
[51] K.S. Kedlaya, p-adic cohomology: from theory to practice, in D. Savitt and D.S. Thakur (eds.), *p-adic Geometry*, University Lecture Series 45, Amer. Math. Soc., 2008, 175–203.
[52] K.S. Kedlaya, p-adic cohomology, in D. Abramovich et al. (eds.), *Algebraic Geometry: Seattle 2005*, Proc. Symp. Pure Math. 80, Amer. Math. Soc., 2009, 667–684.
[53] K.S. Kedlaya, *p-adic Differential Equations*, Cambridge Studies in Advanced Math. 125, Cambridge Univ. Press, 2010.
[54] K.S. Kedlaya, Effective p-adic cohomology for cyclic cubic threefolds, supporting `Sage` worksheet available at `http://math.mit.edu/~kedlaya/papers/`.
[55] K.S. Kedlaya and A.V. Sutherland, Computing L-series of hyperelliptic curves, in *Algorithmic Number Theory (ANTS VIII)*, Lecture Notes in Computer Science 5011, Springer, New York, 2008, 312–326.
[56] K.S. Kedlaya and J. Tuitman, Effective convergence bounds for Frobenius structures, arXiv:1111.0136v1 (2011).
[57] S. Kleiman, Algebraic cycles and the Weil conjectures, in *Dix exposés sur la cohomologie des schémas*, North-Holland, 1968, 359–386.
[58] R. Kloosterman, Point counting on singular varieties, in *Algorithmic Number Theory (ANTS VIII)*, Lecture Notes in Computer Science 5011, Springer, New York, 2008, 327–341; updated version at `http://www.iag.uni-hannover.de/~kloosterman/publ.php`.

[59] A.G.B. Lauder, Counting solutions to equations in many variables over finite fields, *Found. Comput. Math.* **4** (2004), 221–267.
[60] A.G.B. Lauder, Rigid cohomology and p-adic point counting, *J. Théor. Nombres Bordeaux* **17** (2005), 169–180.
[61] A.G.B. Lauder, A recursive method for computing zeta functions of varieties. *LMS J. Comput. Math.* **9** (2006), 222–269.
[62] A.G.B. Lauder, Ranks of elliptic curves over function fields, *LMS J. Comput. Math.* **11** (2008), 172–212.
[63] A.G.B. Lauder, Degenerations and limit Frobenius structures in rigid cohomology, *London Math. Soc. J. Comp. Math.* **14** (2011), 1–33.
[64] A.G.B. Lauder and D. Wan, Counting rational points on varieties over finite fields of small characteristic, in J.P. Buhler and P. Stevenhagen (eds.), *Algorithmic Number Theory: lattices, number fields, curves and cryptography*, MSRI Publications 44, Cambridge Univ. Press, Cambridge, 2008.
[65] R. Lercier and D. Lubicz, A quasi quadratic time algorithm for hyperelliptic curve point counting, *Ramanujan J.* **12** (2006), 399–423.
[66] B. le Stum, *Rigid Cohomology*, Cambridge Univ. Press, 2007.
[67] `Magma` version 2.17-5(2011), information available at `http://magma.maths.usyd.edu.au/`.
[68] Yu. Manin, Rational points of algebraic curves over function fields (Russian), *Izv. Akad. Nauk. SSSR Ser. Math.* **27** (1963), 1395–1440; English translation, *AMS Transl.* **50** (1966), 189–234.
[69] B. Mazur, Frobenius and the Hodge filtration, *Bull. Amer. Math. Soc.* **78** (1972), 653–667.
[70] B. Mazur, Frobenius and the Hodge filtration (estimates), *Ann. of Math.* **98** (1973), 58–95.
[71] B. Mazur, W. Stein, and J. Tate, Computation of p-adic heights and log convergence, *Doc. Math.* Extra Vol. (2006), 577–614.
[72] J.-F. Mestre, Algorithmes pour compter des points en petite caractéristique en genre 1 et 2, unpublished preprint. available at `http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps`.
[73] J.S. Milne, *Étale Cohomology*, Princeton Math. Series 33, Princeton Univ. Press, Princeton, 1980.
[74] J.S. Milne, Étale cohomology, course notes available at `http://www.jmilne.org/math/`.
[75] P. Monsky, Formal cohomology. II: The cohomology sequence of a pair, *Annals of Math.* **88** (1968), 218–238.
[76] P. Monsky, Formal cohomology. III: Fixed point theorems, *Annals of Math.* **93** (1971), 315–343.
[77] P. Monsky and G. Washnitzer, Formal cohomology. I, *Annals of Math.* **88** (1968), 181–217.
[78] B. Osserman, The Weil conjectures, in W.T. Gowers (ed.), *The Princeton Companion to Mathematics*, Princeton Univ. Press, 2008, 729–732; also available online at `http://www.math.ucdavis.edu/~osserman`.
[79] D. Petrequin, Classes de Chern et classes de cycles en cohomologie rigide, *Bull. Soc. Math. France* **131** (2003), 59–121.
[80] J. Pila, Frobenius maps of abelian varieties and finding roots of unity in finite fields, *Math. Comp.* **55** (1990), 745–763.
[81] `Sage` version 4.6.1 (2011), available at `http://sagemath.org/`.
[82] T. Satoh, The canonical lift of an ordinary elliptic curve over a finite field and its point counting, *J. Ramanujan Math. Soc.* **15** (2000), 247–270.
[83] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), 483–494.
[84] A. Shiho, Crystalline fundamental groups, I: Isocrystals on log crystalline site and log convergent site, *J. Math. Sci. Univ. Tokyo* **7** (2000), 509–656.
[85] A. Shiho, Crystalline fundamental groups, II: Log convergent cohomology and rigid cohomology, *J. Math. Sci. Univ. Tokyo* **9** (2002), 1–163.
[86] A. Shiho, Relative log convergent cohomology and relative rigid cohomology, I, arXiv:0707.1742v2 (2008).
[87] A. Shiho, Relative log convergent cohomology and relative rigid cohomology, II, arXiv:0707.1743v2 (2008).
[88] A. Shiho, Relative log convergent cohomology and relative rigid cohomology, III, arXiv:0805.3229v1 (2008).

[89] `Singular` version 3.1.1 (2010), available at `http://www.singular.uni-kl.de/`.
[90] G. Tamme, *Introduction to Étale Cohomology* (translated from the German by M. Kolster), Springer-Verlag, Berlin, 1994.
[91] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math.* **141** (1995), 553–572.
[92] N. Tsuzuki, Slope filtration of quasi-unipotent overconvergent F-isocrystals, *Ann. Inst. Fourier (Grenoble)* **48** (1998), 379–412.
[93] N. Tsuzuki, On base change theorem and coherence in rigid cohomology, *Doc. Math.* Extra Vol. (2003), 891–918.
[94] M. van der Put, The cohomology of Monsky and Washnitzer, Introductions aux cohomologies p-adiques (Luminy, 1984), *Mém. Soc. Math. France* **23** (1986), 33–59.
[95] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* **141** (1995), 443–551.

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139
E-mail address: `kedlaya@mit.edu`
URL: `http://math.mit.edu/~kedlaya`