Ralf Gerkmann, Universität Mainz

Relative rigid cohomology and point counting on hypersurfaces

talk given at the

Department of Mathematics, University of Sydney

March 23, 2006

http://www.mathematik.uni-mainz.de/∼gerkmann

Review on Lauder's algorithm

given: hypersurface $X \subseteq \mathbb{P}^n$ of degree d

define by $f \in \mathbb{F}_q[X_0, ..., X_n]$, $q = p^a$, a large, $p \nmid d$

aim: compute the zeta function

$$\mathscr{Z}(V,t) = \exp\left(\sum_{r=0}^{\infty} \frac{\sharp V(\mathbb{F}_{q^r})t^r}{r}\right) = \frac{p(t)}{(1-t)(1-qt)\cdots(1-q^n t)}$$

where $p(t) \in \mathbb{Z}[t], \deg(p) = d^{-1}((d-1)^{n+1} + (-1)^{n+1}(d-1))$

Dwork homology of a hypersurface

$K = \mathbb{Q}_p(\zeta, \pi)$, $\pi^{p-1} = -p$, ζ primitive $(q-1)$-st root of unity

define index sets

$$\begin{aligned} \mathcal{I} &= \{(u_{-1}, u_0, ..., u_n) \in \mathbb{N}_0^{n+2} \mid du_{-1} = \textstyle\sum_{k=0}^n u_k\} \\ \mathcal{I}^{(i)} &= \{u \in \mathcal{I} \mid u_j > 0 \text{ for } j \neq i\} \;\; 0 \leq i \leq n \\ \mathcal{I}_0 &= \mathcal{I} \cap \mathbb{N}^{n+2} \end{aligned}$$

define subspaces of $K[[Z, X_0, ..., X_n]]$ by

$$\begin{aligned} \mathcal{L} &= \langle X^u \mid u \in \mathcal{I}_0 \rangle_K \\ \mathcal{L}^{(i)} &= \langle X^u \mid u \in \mathcal{I}^{(i)} \rangle_K \end{aligned}$$

define differential operators on $\mathcal{L}$ by

$$D_i := X_i \frac{\partial}{\partial X_i} + \pi X_0 X_i \frac{\partial F}{\partial X_i} \qquad 0 \leq i \leq n$$

where $F \in K[X_0, ..., X_n]$ is obtained from f by Teichmüller lifting the coefficients

define Dwork homology of the hypersurface X by

$$H_0(X) := \mathcal{L} / \sum_{i=0}^{n} D_i(\mathcal{L}^{(i)})$$

is a finite-dimensional K-vector space with basis $\{X^u \mid u \in \mathcal{B}\}$ where

$$\mathcal{B} = \{u \in \mathcal{I}_0 \mid u_0, ..., u_n < d\}$$

construction of a linear operator α on $H_0(X)$

define

$$\Psi : \mathcal{L} \to \mathcal{L} \ , \qquad \sum_{u \in \mathcal{I}_0} c_u X^u \mapsto \sum_{u \in \mathcal{I}_0} c_{qu} X^u$$

put $G := ZF \ , \ \ H := \exp \ \pi(G - G(X^q)) \ , \ \ \alpha := \Psi \circ H$

then the characteristic polynomial of α satisfies

$$p(qt) = \det(1 - \alpha t)$$

where $p(t) \in \mathbb{Z}[t]$ appears in the zeta function $\mathscr{Z}(X, t)$

Ideas behind the construction of Dwork homology

★ number of rational points on $X^* := X \cap (\mathbb{G}_m)^{n+1}$ can be expressed by character sums , where character := homomorphism $\psi : (\mathbb{F}_q, +) \to K^\times$

key property: $$\sum_{a \in \mathbb{F}_q} \psi(a) = \begin{cases} q & \text{if } \psi \text{ trivial} \\ 0 & \text{if } \psi \text{ non-trivial} \end{cases}$$

★ values of characters can be expressed by p-adic exponential, more precisely $\psi(a) = \exp(\pi \hat{a}), \pi = \pi(\psi)$

$\Rightarrow$ formula for $\mathbb{F}_{q^r}$-rational points in terms of the "trace" of $\Psi \circ H$ acting on the infinite-dimensional space $K[[Z, X_0, ..., X_n]]$

★ restriction to a space of overconvergent power series

$\Rightarrow$ nuclear operator on p-adic Banach space (well-defined trace and "char. polynomial")

★ forming appropriate alternating sum

(intersections with all lower-dimensional subspaces of $\mathbb{P}^n$)

$\Rightarrow$ trace formula for $\sharp X(\mathbb{F}_{q^r})$ rather than $\sharp X^*(\mathbb{F}_{q^r})$

★ Given a chain complex of Banach spaces and a nuclear chain map, the alternating sum of the traces coincides with the alternating sum of its cohomology.

here: chain maps constructed from the differential operators

$\Rightarrow$ formula for $\sharp X(\mathbb{F}_{q^r})$ as a trace on a finite-dimensional space

Relative version of Dwork homology

consider now an algebraic family of hypersurfaces of the form

$$f := \sum_{i=0}^{n} a_i X_i^d + zh = 0 \qquad a_i \in \mathbb{F}_p\,, \;\; h \in \mathbb{F}_p[X_0, ..., X_n] \text{ of degree } d$$

define $F \in K[z][X_0, ..., X_n]$:= Teichmüller lift of f

R := subring of $K(z)$, function without pole in $z = 0$

$\mathcal{L}_z := \langle X^u \;\mid\; u \in \mathcal{I}_0 \rangle_R$

$\mathcal{L}_z^{(i)} := \langle X^u \;\mid\; u \in \mathcal{I}^{(i)} \rangle_R$

differential operators $D_{i,z}$, $H_0(X)_z$ accordingly

Terminology:

element $g \in \mathcal{L}_z$ reduced :⇔ contained in the subspace generated by X^u, $u \in \mathcal{B}$

Procedure of Lauder's algorithm

- ★ compute a matrix B over R ("connection matrix")
  $B_{uv}(z) :=$ coefficient of $\pi^{u-1}X^u$ in the reduction of $\pi^{u-1}X^u$
- ★ solve the linear differential equation $\partial C/\partial z = C(z)B(z)$
- ★ compute the representation matrix of α at $z = 0$ by the explicit formula

$$M_{uv} = \pi^{v-1-u-1} \prod_{i=0}^{n} \sum_{m,r} \lambda_m (u_i/d)_r (-1)^r \pi^{-r} \hat{a}_i^{pm-r}$$

  (sum over all $(m, r$ with $pu_i - v_i = d(m - pr))$
- ★ analytic continuation of $M(z) := C(z^p)^{-1}MC(z)$
- ★ for $b \in \mathbb{F}_q$, compute the product $M(\hat{b})M(\hat{b}^p) \cdots M(\hat{b}^{p^{b-1}})$
  $\Rightarrow$ obtain zeta function of the hypersurface $\sum_{i=0}^{n} a_i X_i^d + bh = 0$

Previous work in a simliar direction

(a) Candelas, de la Ossa, Villegas (1990)

- ★ found a relation between periods of certain families of Calabi-Yaus and and the number $\mathbb{F}_q$-rational points on the reduction modulo p
- ★ determined the period function and its Fourier expansion by a heuristic based on physical considerations
- ★ combinatorial expression for the number of $\mathbb{F}_p$-rational points modulo p and p^2
- ★ relation mod p and p^2 suggests general formula for all p-adic digits, which is established by a Gauss sum computation

(b) D. Morrison (1998)

- ★ worked exclusively over $\mathbb{C}$ (neither finite nor p-adic fields)
- ★ Yukawa coupling := rational expression in the period functions associated to a certain family of Calabi-Yaus
- ★ Conjecture: Fourier coefficients of the Yukawa coupling are related to the number of rational curves on another CY-family obtained by mirror symmetry
- ★ Morrision used this relation to predict the number of rational curves on CYs using computer algebra
- ★ makes systematic use of Griffiths' reduction theory in order to compute Fourier expansion of the periods

Dwork's homology, as presented here, is restricted to smooth projective hypersurfaces. There are variants, but in general the relation to classical (i.e. singular) cohomology of varieties is not fully understood.

Meanwhile, there exists a satisfactory p-adic cohomology theory for general varieties over a finite field $\mathbb{F}_q$, closely related to the classical de Rham cohomology based on differential forms:

rigid cohomology due to P. Berthelot ($\sim$ 1990)

Some properties of rigid cohomology:

★ contravariant functors $X \mapsto \mathrm{H}^i_{\mathrm{rig}}(X)$ ($0 \leq i \leq 2\dim(X)$) from $\mathbb{F}_q$-schemes of finite type to K-vector spaces, where $K \supseteq \mathbb{Q}_p(\zeta_{q-1})$ (finite-dimensional if X smooth)

★ cohomology groups with compact support, Poincaré duality

$$\mathrm{H}^i_{\mathrm{rig,c}}(X) \times \mathrm{H}^{2d-i}_{\mathrm{rig}}(X) \mapsto K(-d)$$

★ Lefschetz-type trace formula $\sharp X(\mathbb{F}_{q^r}) = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(\mathrm{Fr}^s | \mathrm{H}^i_{\mathrm{rig,c}}(X))$

★ excision sequence: $Z \subseteq Y$ closed, $Y := X \setminus Z$

$$\cdots \to \mathrm{H}^i_{\mathrm{rig,c}}(X) \to \mathrm{H}^i_{\mathrm{rig,c}}(Y) \to \mathrm{H}^i_{\mathrm{rig,c}}(Z) \to \mathrm{H}^{i+1}_{\mathrm{rig,c}}(X) \to \cdots$$

Comparision with other cohomology theories

★ X smooth projective $\Rightarrow$ rigid cohomology $=$ crystalline cohomology (modulo torsion)

★ X smooth affine $\Rightarrow$ rigid cohomology $=$ Monsky-Washnitzer cohomlogy

$$X = \mathrm{Spec}(\bar{A}),\ \bar{A} \text{ finitely generated } \mathbb{F}_q\text{-algebra}$$

$$A = \text{smooth lift of } \bar{A} \text{ to } \mathcal{O}_K\text{-algebra generated by } x_1, ..., x_r$$

$$A^\dagger = \text{weak completion}$$

$$\left\{\sum a_{i_1\ldots i_r} x_1^{i_1} \cdots x_r^{i_r} \mid \exists\gamma > 0 : v_p(a_{i_1\ldots i_r}) \geq \gamma(i_1 + ... + i_r)\right\}$$

$$\mathrm{H}^i_{MW}(X) = \mathrm{H}^i_{\mathrm{dR}}(A^\dagger_K) = \mathrm{H}^i(\Omega^\cdot_{A^\dagger_K})$$

★ comparision between rigid cohomology and algebraic de Rham cohomology:
$X \subseteq Y$ open immersion of $\mathbb{F}_q$-varieties, lifts to open immersion $\mathcal{X} \subseteq \mathcal{Y}$ of smooth $\mathcal{O}_K$-schems, $\mathcal{Z} := \mathcal{Y} \setminus \mathcal{X}$ is smooth relative divisor with normal crossings, $\mathcal{X}_K$ generic fibre of $\mathcal{X} \Rightarrow \mathrm{H}^i_{\mathrm{rig}}(X) \cong \mathrm{H}^i_{\mathrm{dR}}(\mathcal{X}_K)$

In 2001 K. Kedlaya introduced an algorithm which uses the trace formula in Monsky-Washnitzer cohomology in order to compute the zeta function of hyperelliptic curves. Since then, many other types of varieties have been considered (superelliptic curves, Artin-Schreier covers of $\mathbb{P}^1$, C_{ab}-curves, certain complete intersections in $\mathbb{A}^n$ ...).

Outline of Kedlaya's algorithm: $X = \mathrm{Spec}(\bar{A})$ smooth curve over $\mathbb{F}_q$

★ compute an analytic lift of the q-power Frobenius on $\bar{A}$ to a $\mathcal{O}_K$-algebra homomorphism $\hat{F} : A^\dagger \to A^\dagger$

★ choose a basis $\omega_1, ..., \omega_b$ of $\mathrm{H}^1_{\mathrm{dR}}(A^\dagger_K)$ and compute the images $\hat{F}(\omega_i)$ (up to some precision)

★ use relations in the algebraic de Rham cohomology in order to find exact differentials $d\psi_i$ such that $\hat{F}(\omega_i) + d\psi_i \in \langle \omega_1, ..., \omega_b \rangle_K$
$\Rightarrow$ yields approximate representation matrix of the Frobenius

★ compute and output the characteristic polynomial

Question: Is it possible to formulate Lauder's deformation method within this framework?

- ★ G. 2005: carried this out for elliptic curves (any characteristic)
- ★ Hubrechts 2006: same for hyperelliptic curves in odd characteristic established a subcubic time complexity in $\log(\text{field size})$ (Kedlaya's algorithm needs cubic time)
- ★ **here:** What can be said about general smooth hypersurfaces ?

given smooth hypersurface $X/\mathbb{F}_q$ of degree d in $\mathbb{P}^n$ with defining equation $f \in \mathbb{F}_q[X_0, ..., X_n]$; let $U := \mathbb{P}^n \setminus X$

excision sequence in rigid cohomology shows that

$$\mathscr{Z}(X,t) = \frac{p(t)}{(1-t)(1-qt)\cdots(1-q^n t)}$$

where $p = \det(1 - t\mathrm{q}^{\mathrm{n}}\mathrm{Fr}^{-1}|\mathrm{H}^n_{\mathrm{rig}}(U))$, $U := \mathbb{P}^n \setminus X$

complement U is affine, furthermore: lift X, U to schemes $\mathcal{U}, \mathcal{X}$ over $\mathcal{O}_K$
$\Rightarrow \mathcal{X}$ is a smooth relative divisor with normal crossings, so that

$$\mathrm{H}^n_{\mathrm{rig}}(U) \cong \mathrm{H}^n_{\mathrm{dR}}(\mathcal{U}_K)$$

Griffiths' theory on complements of projective hypersurfaces

differentials on projective space:

A meromorphic k-form ω on $\mathbb{A}^{n+1}$ represents a differential on $\mathbb{P}^n$ if and only if $\mathfrak{X}(\omega) = 0$, where $\mathfrak{X} = \sum_{i=0}^{n} X_i \partial/\partial X_i$ (Euler vector field).

$\Rightarrow$ Every n-form on $\mathbb{P}^n$ with poles along a hypersurface $F = 0$ can be written as $\omega = H\Omega/F^\ell$, where $\deg(H) + (n+1) = \ell \deg(F)$ and where $\Omega = \sum_{i=0}^{n} (-1)^i X_i dX_0 \wedge \cdots \wedge \widehat{dX_i} \wedge \cdots \wedge dX_n$

Every $(n-1)$-form is a linear combination of the form $\sum_{i=0}^{n} A_i K_{X_i} \Omega$, $0 \leq i \leq n$, where K_{X_i} = contraction with $\partial/\partial X_i$ and $\deg(A_i) + n = \ell \deg(F)$.

Griffths' reduction of differentials

★ An n-differential $\omega = H\Omega/F^{\ell}$ is equivalent to a form of lower pole order if and only if H is contained in the Jacobian ideal.

more precisely: If $H = \sum_{j=0}^{n} A_j \frac{\partial F}{\partial X_j}$, define

$$\varphi = 1/F^{\ell-1}(\sum_{j=0}^{n} A_j K_{X_j}\Omega)$$

Then $\omega + d\varphi = P\Omega/F^{\ell-1}$ where $P = \frac{1}{F^{\ell-1}} \sum_{j=0}^{n} \frac{\partial A_j}{\partial X_j}$.

★ The latter is always the case if $\ell > n$.

Applications of Griffiths' reduction

★ basis computation for $\mathrm{H}^n_{\mathrm{dR}}(\mathcal{U}_K)$:

for $1 \leq \ell \leq n$, compute basis of the quotient space $K[X_0, ..., X_n]_{\ell d-(n+1)}/\mathcal{J}_{\ell d-(n+1)}$, where $\mathcal{J} = \langle \frac{\partial F}{\partial X_0}, ..., \frac{\partial F}{\partial X_n} \rangle$

★ reduction algorithm for differential forms

(a) for $1 \leq \ell \leq n$, compute coordinates of $H\Omega/F^\ell$ with respect to basis of $\mathrm{H}^n_{\mathrm{dR}}(\mathcal{U}_K)$ for every monomial of degree $\ell d - (n+1)$

(b) write every monomial H of degree $(n+1)(d-1)$ as $\sum_{j=0}^n A_{H,j}\partial F/\partial X_j$

(c) given $\omega = H\Omega/F^\ell$ with $\ell > n$, $\deg(H) = \ell d - (n+1)$, $H = \sum_{i=0}^r \lambda_i P_i$ lin. comb. of monomials, $P_i = Q_i R_i$ with $\deg(Q_i) = (n+1)(d-1)$

$\Rightarrow H = \sum_{j=0}^n (\sum_{i=0}^r \lambda_i R_i A_{Q_i,j})\partial F/\partial X_j$

apply Griffiths' reduction formula

The dagger ring of hypersurface complements

$$A^\dagger = \left\{ \sum_{k=0}^{\infty} \frac{G_k}{F^k} \;\middle|\; \deg(G_k) = dk, \exists\gamma : v_p(G_k) \geq \gamma k \right\}$$

Frobenius action on meromorphic functions

$$\frac{H}{F^\ell} \mapsto H(X^q)F^{-q\ell}(1 - \frac{qG}{F^q})(1 - qG)^{-\ell} = \sum_{k=0}^{\infty} \frac{q^k \alpha_k H(X^q) G^k}{F^{q(k+\ell)}}$$

where $qG = F^q - F(X^q)$, $(1-t)^{-\ell} = \sum_{i=0}^{\infty} \alpha_i t^i$

Frobenius action on differential forms given by

$$\omega = \frac{H\Omega}{F^\ell} \mapsto \frac{H(X^q)(\prod_{i=0}^{n} X_i^{q-1})\Omega}{F^{q\ell}} \left(\sum_{k=0}^{\infty} \frac{q^k \alpha_k G^k}{F^{qk}} \right)$$

Kedlaya's algorithm for complements of hypersurfaces

(due to Abbott, Kedlaya, Roe)

Procedure :

★ determine a basis $\omega_1, ..., \omega_b$ of $\mathrm{H}^n_{\mathrm{rig}}(U) = \mathrm{H}^n_{\mathrm{dR}}(\mathcal{U}_K)$

★ compute an approximation of $\hat{F}(\omega_i)$ for $1 \leq i \leq b$

★ use the reduction algorithm to obtain the representation matrix

Problem: What is the correct p-adic precision?

(Reduction of differentials introduces p-adic denominators.)

Estimating the required p-adic precision

It is known that there exists a Frobenius-invariant sublattice Γ in $\mathrm{H}^n_{\mathrm{rig}}(U)$ (comes from crystalline cohomology in the case of curves). Using the theory of log schemes, Kedlaya showed that if $\omega \in \Omega^n_A$ has pole order ℓ, then $p^{\lfloor \log_p \ell \rfloor}[\omega] \in \Gamma$.

Problem: Γ cannot be computed directly. Instead, we consider the following lattices.

$$\Lambda \quad := \quad \text{lattice spanned by basis elements}$$

$$\tilde{\Lambda} \quad := \quad \text{lattice spanned by } H\Omega/F^{\ell},\ H \text{ monomial and } 1 \leq \ell \leq n$$

Considering the $\log$-complex over $\mathcal{O}_K$, one can show that $\tilde{\Lambda}$ contains Γ. By elementary methods one can compute constants which determine the relative position of $\Gamma, \tilde{\Lambda}$ and Λ.

Some basic facts on relative rigid cohomology

★ For general (non-affine) varieties X, rigid cohomology is defined by

$$\mathrm{H}^i_{\mathrm{rig}}(X) = \mathbb{H}^i(\, j^\dagger \Omega^{\cdot}_{]X[}\,)$$

★ Now let $f : X \to S$ be a smooth $\mathbb{F}_q$-morphism. It induces a map $\hat{f}_K :]X[\to]S[$ between the associated rigid-analytic spaces. Now relative rigid cohomology is the sheaf on $]S[$ defined by

$$\mathscr{H}^i_{\mathrm{rig}}(X/S) := \mathbb{R}^i \hat{f}_{K*}\left(j^\dagger \Omega^{\cdot}_{]\bar{X}[/]\bar{S}[}\right)$$

It is equipped with a canonical connection (Gauß-Manin connection).

★ If S is affine with dagger ring $A_K^\dagger$, write $\mathrm{H}^i_{\mathrm{rig}}(X/S)$ for the global sections of $\mathscr{H}^i_{\mathrm{rig}}(X/S)$. Then the GM-connection is a map

$$\nabla : \mathrm{H}^i_{\mathrm{rig}}(X/S) \to \Omega^1_{A_K^\dagger} \otimes_{A_K^\dagger} \mathrm{H}^i_{\mathrm{rig}}(X/S)$$

Relative rigid and relative de Rham cohomology

★ Let $\hat{f} : \mathcal{X} \to \mathcal{S}$ denote a smooth lift of $f : X \to S$. If the "normal crossings property" is defined generically (i.e. in every fibre), then there is a natural isomorphism $\mathrm{H}^i_{\mathrm{rig}}(X/S) \cong \mathrm{H}^i_{\mathrm{dR}}(\mathcal{X}_K/\mathcal{S}_K) \otimes_{A_K} A_K^\dagger$.

★ This isomorphism is compatible with the Gauss-Manin connection, i.e. we have $\Omega^1_{A_K^\dagger} \cong \Omega^1_{A_K} \otimes_{A_K} A_K^\dagger$ and ∇ is induced by the algebraic connection

$$\nabla : \mathrm{H}^i_{\mathrm{dR}}(\mathcal{X}_K/\mathcal{S}_K) \longrightarrow \Omega^1_{A_K} \otimes_{A_K} \mathrm{H}^i_{\mathrm{dR}}(\mathcal{X}_K/\mathcal{S}_K).$$

$\Rightarrow$ can use the classical GM-connection, for varieties over fields of characteristic zero

Frobenius structure

★ The Frobenius action on X and S induces an endomorphism $\mathrm{Fr}: \mathrm{H}^i_{\mathrm{rig}}(X/S) \to \mathrm{H}^i_{\mathrm{rig}}(X/S)$ of $A^\dagger_K$-modules. It is compatible with the Gauss-Manin-connection, i.e.

$$\begin{array}{ccc} \mathrm{H}^i_{\mathrm{rig}}(X/S) & \stackrel{\nabla}{\longrightarrow} & \Omega^1_{A^\dagger_K} \otimes_{A^\dagger_K} \mathrm{H}^i_{\mathrm{rig}}(X/S) \\ \mathrm{Fr} \downarrow & & \downarrow \mathrm{Fr} \\ \mathrm{H}^i_{\mathrm{rig}}(X/S) & \stackrel{\nabla}{\longrightarrow} & \Omega^1_{A^\dagger_K} \otimes_{A^\dagger_K} \mathrm{H}^i_{\mathrm{rig}}(X/S) \end{array} \quad \text{commutes}$$

★ Let $\iota_P : \bar{A} \to \mathbb{F}_q$ denote a rational point on S with fibre X_P and $\hat{\iota}_P : A^\dagger \to \mathcal{O}$ a Frobenius-compatible lift. Then $\mathrm{H}^i_{\mathrm{rig}}(X_P) \cong \mathrm{H}^i_{\mathrm{rig}}(X) \otimes_{A^\dagger_K, \hat{\iota}_P} K$ and

$$\begin{array}{ccc} \mathrm{H}^i_{\mathrm{rig}}(X/S) & \stackrel{\hat{\iota}_P}{\longrightarrow} & \mathrm{H}^i_{\mathrm{rig}}(X) \\ \mathrm{Fr} \downarrow & & \downarrow \mathrm{Fr} \\ \mathrm{H}^i_{\mathrm{rig}}(X/S) & \stackrel{\hat{\iota}_P}{\longrightarrow} & \mathrm{H}^i_{\mathrm{rig}}(X) \end{array} \quad \text{commutes}$$

Computing the Gauß-Manin connection

Katz (1968) gave the following explicit description of the GM-connection:

Let $f : X \to S$ be a smooth algebraic family, locally given by a homomorphism $A \to B$ of K-algebras. Pick $s_1, ..., s_r \in A$ such that the ds_i form a free system of generators of Ω^1_A and $x_1, ..., x_n$ such that the dx_i freely generate $\Omega^1_{B|A}$. Then

$$\nabla^{GM} : \mathrm{H}^k_{\mathrm{dR}}(X/S) \to \Omega^1_S \otimes \mathrm{H}^k_{\mathrm{dR}}(X/S)$$

is induced by

$$h\omega \mapsto \sum_{i=1}^{r} \frac{\partial h}{\partial s_i} ds_i \wedge d\omega$$

if $\omega = dx_{i_1} \wedge \cdots \wedge dx_{i_k}$ and $h \in B$.

here:

S open subset of $\mathbb{P}^1$, U family of complements of hypersurfaces defined by $F \in K[z][X_0, ..., X_n]$

Let $\omega_1, ..., \omega_b$ denote a basis of $\mathrm{H}^n_{\mathrm{dR}}(U/S)$.

aim: find $c_{ij} \in A_K$ such that $\nabla(\omega_j) = \sum_{i=1}^b c_{ij} dz \otimes \omega_i$ (connection matrix)

Procedure:

★ compute $\nabla(\omega_i)$ for $i = 1, .., b$ on the level of differential forms according to

$$\nabla : \frac{H\Omega}{F^\ell} \mapsto \frac{\partial}{\partial z}(\frac{H}{F^\ell})\Omega = \frac{G\Omega}{F^{\ell+1}} \quad , \quad G := -\ell H(\partial F/\partial z)$$

★ use Griffiths reduction in order to determine $c_{ij} \in A_K$ such that $\nabla(\omega_j) \equiv \sum_{i=1}^b c_{ij}\omega_i$

Gauß-Manin connection and Frobenius; the p-adic differential equation

$S = \mathbb{P}^1 \setminus \{P_1, ..., P_r, \infty\} \;\Rightarrow\;]S[= \mathbb{P}^1 \setminus$ finitely many open p-adic discs of radius 1

aim: compute the representation matrix $M(z)$ for Frob with respect to $\omega_1, ..., \omega_b$ over $A_K^\dagger :=$ overconvergent functions on $]S[$

The commutative diagram relating ∇ and Frob gives rise to the matrix equation

$$\frac{\partial}{\partial z}(M) + C(z)M = pz^{p-1}MC(z^p)$$

choose $z_0 \in]S[$, define $N(z) := M(z+z_0) = \sum_{n=0}^{\infty} N_n z^n$

define $d(z) :=$ least common multiple of denominators in C, write $f(z)C(z) = D(z)$

$\Rightarrow$ modified differential equation

$$f(z)\frac{\partial}{\partial z}N(z) + g(z)D(z)N(z) = h(z)N(z)G(z)$$

solution formula

$$(n+1)f_0 N_{n+1} = -\sum_{i=0}^{\alpha_n}(n-i+1)f_i N_{n-i+1} - \sum_{i=0}^{\beta_n} R_i N_{n-i} + T_n$$

where $R_n = \sum g_i D_{n-i}$, $S_n = \sum h_i N_{n-i}$, $T_n = \sum S_i G_{n-i}$

Estimating the size of p-adic denominators

For practical purposes it is useful to have a bound on the p-adic denominators that occur in the matrices N_n of the local expansion.

There is a theorem of Christol-Dwork which gives a logarithmic upper bound for solutions of linear p-adic differential equations around a regular singular point, i.e. for deq's of the form

$$z\frac{\partial}{\partial z}(M) = G(z)M(z) \qquad G(0) \text{ nilpotent }, \|G\| \leq 1$$

period matrix of a connection ∇ := solution of $\partial/\partial z P = -CP$

Any solution of the differential equation for Frob is of the form $P(z)M_0P(z^p)^{-1}$, where M_0 := constant matrix and P := period matrix associated to C.
$\Rightarrow$ can derive bounds on $M(z)$ from those of $P(z)$

Analytic continuation of the local solution

Problem:

The local solution $\sum_{n=0}^{\infty} N_n(z-z_0)^n$ only converges on an open disc of radius 1.

$\Rightarrow$ cannot evaluate it on $z_1 \in]S[$ with $z_1 \not\equiv z_0 \mod p$

On the other hand, we know that the matrix coefficients are contained in $A_K^\dagger$, and every $f \in A_K^\dagger$ has a Laurent series expansion

$$f(z) = \sum_{n=0}^{\infty} \beta_n(f) z^n + \sum_{n=1}^{\infty} \sum_{\ell=0}^{s-1} \frac{\gamma_{n\ell}(f)}{d(z)^n}$$

where the zeroes of $d(z)$ are p-adic integers which reduce to the finitely many geometric points on $\mathbb{P}^1 \setminus S$, and $s = \deg(d)$.

Let $z_0, z_1 \in K$, $d(z_0), d(z_1) \not\equiv 0 \mod p$, and assume that a local expansion $\sum_{n=0}^{\infty} \alpha_n (z - z_0)^n$ around z_0 is given.

Aim: compute $f(z_1)$ up to p-adic precision N

If $v_p(\beta_n(f)) \geq N$ for $n \geq m_1$ and $v_p(\gamma_{n\ell}) \geq N$ for $n \geq m_2$, then it suffices to evaluate the rational function

$$\tilde{f}(z) = \sum_{n=0}^{m_1-1} \beta_n(f) z^n + \sum_{n=1}^{m_2-1} \sum_{\ell=0}^{s-1} \frac{\gamma_{n\ell}(f)}{d(z)^n}$$

Multiplication by principal denominator and using the local expansion shows

$$f(z_1) \equiv \tilde{f}(z_1) \equiv d(z_1)^{1-m_2} \sum_{n=0}^{\gamma} \tilde{\alpha}_n (z_1 - z_0)^n \mod p^N \ , \ \gamma := m_1 - 1 + s(m_2 - 1)$$

where $\sum \tilde{\alpha}_n (z - z_0)^n = d(z)^{m_2-1} (\sum_{n=0}^{\infty} \alpha_n (z - z_0)^n)$

Problem: given some precision N, how to obtain m_1, m_2

Notation: let $\mathbb{P}^1 \setminus \mathcal{S}_K = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s, \infty\}$, $f \in K(z) \cap A_K^\dagger$

$$\begin{aligned} \mathrm{ord}_0(f) \quad &:= \quad \text{maximal pole order of } f \text{ at one of the } \mathfrak{p}_i \\ \mathrm{ord}_\infty(f) \quad &:= \quad \text{maximal pole order of } f \text{ at } \infty \end{aligned}$$

$G \in K(z)[X_0, ..., X_n] \Rightarrow \mathrm{ord}_0(G), \mathrm{ord}_\infty(G) =$ maximal pole order at one of the coefficients

Let $\omega_1, ..., \omega_b$ denote a basis of $\mathrm{H}^n_{\mathrm{rig}}(U)$. The Frobenius action is given by

$$q^{-n}\mathrm{Fr}(\omega_j) = \sum_{k=0}^{\infty} p^k \omega_{jk} \ , \ \omega_{jk} = \frac{\tilde{H}_{jk}\Omega}{F^{p(\ell_j+k)}} \ , \ \tilde{H}_{jk} = \alpha_k G^k H_j(X^p) \prod_{i=0}^{n} X_i^{p-1}$$

Reducing each summand ω_{jk} separately, we obtain relations in de Rham cohomology

$$\omega_{jk} \equiv \sum_{i=1}^{b} m_{ijk}\omega_i \qquad \text{where } m_{ijk} \in K(z) \cap A_K^{\dagger}$$

By a simple induction proof, we can estimate the pole orders in the coefficients of the reduction of any $\omega = H\Omega/F^{\ell}$, depending on ℓ. This yields

$$\begin{aligned} \mathrm{ord}_0(m_{ijk}) &\leq w_0' + (pn + pk - n)w_0'' \\ \mathrm{ord}_\infty(m_{ijk}) &\leq w_\infty' + (pn + pk - n)w_\infty'' + k\,\mathrm{ord}_\infty(G) \end{aligned}$$

where $w_0', w_0'', w_\infty', w_\infty''$ are constants depending on the family.

Now consider the Laurent expansion of a coefficient of the Frobenius matrix.

$$m_{ij}(z) = \sum_{n=0}^{\infty} \beta_n(m_{ij}) z^n + \sum_{n=1}^{\infty} \sum_{\ell=0}^{s-1} \frac{\gamma_{n\ell}(m_{ij})}{d(z)^n}$$

The above linear bound shows:

If n is large, then the term $\beta_n(m_{ij})z^n$ is “caused” by reducing a summand in $\mathrm{Fr}(\omega_j)$ with pole of high order along the hypersurface.

$\Rightarrow$ p-adic valuation of $\beta_n(m_{ij})$ must be high

Result:

$v_p(\beta_\ell(m_{ij})) \geq \zeta_\infty(\ell) - r_1 - (n+1) - \lfloor \log_p(n + \zeta_\infty(\ell) - 1) \rfloor$

where $\zeta_\infty(\ell)$ linear function, r_1 constant (same for the $\gamma_{n\ell}(m_{ij})$)

Summary: The complete algorithm

given $f \in \mathbb{F}_p[z][X_0, ..., X_n]$ homogeneous of degree d, $q = p^a$, a large, $\bar{z}_1 \in \mathbb{F}_q$
$F \in \mathbb{Q}_p[z][X_0, ..., X_n]$ lift to characteristic zero

aim: compute the zeta function of the hypersurface corresponding to
$f(\bar{z}_1) \in \mathbb{F}_q[X_0, ..., X_n]$

★ compute the connection matrix which belongs to F

★ choose $z_0 \in \mathbb{Z}_p$ such that the hypersurface corresponding to $f(\bar{z}_0)$ is smooth, compute the Frobenius matrix M_0 (see below!)

★ solve the p-adic differential equation with M_0 as constant term $\Rightarrow$ solution $M(z)$

★ evaluate $M(z)$ at $M(z_1), M(z_1^p), ..., M(z_1^{p^a-1})$, compute the product and its characteristic polynomial

It remains to compute the Frobenius matrix M_0 which serves as constant term for the local expansion. Here we can use one of the following methods:

(a) for characteristic $p \nmid d =$ degree of the hypersurface

★ use Dwork's explicit formula for diagonal hypersurfaces and Katz's comparision theorem

(b) for general p

★ use the general hypersurface algorithm of Abbott/Kedlaya/Roe (inefficient for curves)

★ find other hypersurfaces with many automorphisms

★ use more efficient (e.g. Vercauteren's) version of Kedlaya's algorithm for curves

Remember that Dwork gave an explicit formula for the representation matrix M_0' of his operator α in the case of diagonal hypersurfaces of the form $\sum_{i=0}^{n} a_i X_i^d = 0$. These are non-singular if and only if $p \nmid d$.

In 1968 Katz constructed an isomorphism ϕ between Dwork homology $H_0(X)$ and $\mathrm{H}^n_{\mathrm{rig}}(U) \otimes_K K(\pi)$ of the complement. Furthermore, he showed that there is a commutative diagram

$$\begin{array}{ccc} H_0(X) & \xrightarrow{\phi} & \mathrm{H}^n_{\mathrm{rig}}(U) \\ \alpha \downarrow & & \downarrow q^{n+1}\mathrm{Fr}^{-1} \\ H_0(X) & \xrightarrow{\phi} & \mathrm{H}^n_{\mathrm{rig}}(U) \end{array}$$

Since in the case of diagonal hypersurfaces M_0' is a diagonal times a permutation matrix, it is easy to defer an explicit expression for Fr on $\mathrm{H}^n_{\mathrm{rig}}(U)$.

$\Rightarrow M_0'$ defined over K rather than $K(\pi)$

Hypersurfaces with many automorphisms

Let X be a hypersurface over $\mathbb{F}_q$, and G its automorphism group. We say that X has **sufficiently many automorphisms** if and only if there is a decomposition into one-dimensional χ-isotypical components

$$\mathrm{H}^n_{\mathrm{rig}}(U) = \bigoplus_{\chi} \mathrm{H}^n_{\mathrm{rig}}(U)_\chi$$

where χ runs through the characters of G.

Key fact: The Frobenius commutes with every automorphism in G.

$\Rightarrow$ eigenvalues of Frobenius and corresponding χ-eigenspaces completely determine the Frobenius matrix

For example, this condition is satisfied by the diagonal hypersurfaces.

Example: curve $C/\mathbb{F}_2$ given by $X^4 + XY^3 + XZ^3 = 0$

de Rham cohomology of the complement U is spanned by

$$\begin{array}{lll} \omega_1 = X\Omega/F & \omega_2 = Y\Omega/F & \omega_3 = Z\Omega/F \\ \omega_4 = X^3Y^2\Omega/F^2 & \omega_5 = X^3YZ\Omega/F^2 & \omega_6 = X^2Y^2Z\Omega/F^2 \end{array}$$

A non-trivial automorphism on C is given by $\sigma : X \mapsto X, Y \mapsto \zeta^3 Y, Z \mapsto \zeta^2 Z$.
(where ζ = primitive 9-th root of unity)

eigenvalues of σ on $\omega_1, \ldots, \omega_6$: $\zeta, \zeta^4, \zeta^2, \zeta^5, \zeta^6, \zeta^3$ (all distinct)

number of rational points: $\sharp C(\mathbb{F}_2) = 3$, $\sharp C(\mathbb{F}_4) = 5$, $\sharp C(\mathbb{F}_8) = 9$

$$\Rightarrow \mathscr{Z}(C,t) = \frac{1 + 8t^6}{(1-t)(1-2t)}$$

$\Rightarrow$ characteristic polynomial of 2^6-Frobenius is $(1+8t)^6$
representation matrix is -8 times identity matrix

Problems with this approach:

★ In general, varieties with many automorphisms are hard to find.
(here: only considered curves of degree $d = 3, 4, 5, 6$)

★ For high Betti numbers, the zeta function cannot be obtained by elementary point counting.
$\Rightarrow$ need combinatorial expression for $\sharp X(\mathbb{F}_q)$, as in the diagonal case

Alternative method for curves:

Use Kedlaya's original algorithm. (This is more efficient than the general one, since it involves differential form on a one-dimensional variety instead of a two-dimensional one.)

Problem here:

Algorithm computes Frobenius on $\mathrm{H}^1_{\mathrm{rig}}(C)$ rather than $\mathrm{H}^2_{\mathrm{rig}}(U)$.
$\Rightarrow$ need an explicit isomorphism for given bases of the two spaces

Residue map

$X/\mathbb{F}_q$ projective curve in $\mathbb{P}^2$, U := complement

The exicision sequence relating X, U and $\mathbb{P}^2$ contains a map $\mathrm{H}^1_{\mathrm{rig,c}}(X) \to \mathrm{H}^2_{\mathrm{rig,c}}(U)$.

By Poincaré duality one obtains

$$\mathrm{res} : \mathrm{H}^2_{\mathrm{rig}}(U) \to \mathrm{H}^1_{\mathrm{rig}}(X) \qquad \text{(residue map)}$$

By comparision with de Rham cohomology, we can as well consider the map $\mathrm{res} : \mathrm{H}^2_{\mathrm{dR}}(\mathcal{U}_K) \to \mathrm{H}^1_{\mathrm{dR}}(\mathcal{X}_K)$ in characteristic zero.

Let $x = X/Z$, $y = Y/Z$ define local coordinates for $\mathbb{A}^2 \subseteq \mathbb{P}^2$ and put $\mathcal{X}'_K := \mathcal{X} \cap \mathbb{A}^2$.

Our aim is to compute the composite map

$$\mathrm{H}^2_{\mathrm{rig}}(\mathcal{U}_K) \to \mathrm{H}^1_{\mathrm{rig}}(\mathcal{X}_K) \to \mathrm{H}^1_{\mathrm{rig}}(\mathcal{X}'_K)$$

in explicit terms.

Theorem:

$F \in K[X,Y,Z]$, $f \in K[x,y]$ defining equations of projective/affine curve

F_X, F_Y, F_Z partial derivatives, $f_X, \ldots$ dehomogenization

$\omega = H\Omega/F^\ell$, $\ell = 1,2$, $h \in K[x,y]$ dehom.

write $h = g_0 f_X + g_1 f_Y + g_2 f$ (possible since $\mathcal{X}'$ non-singular)

(a) For $\ell = 1$, put $\omega' := -g_1\, dx + g_0\, dy$.

(b) For $\ell = 2$, define $\omega' := \frac{f_X h_X - f_{XX} h}{f_X^3}\, dy - df_0$ where $f_0 = -g_1/f_X$.

Then $\mathrm{res}([\omega]) = [\omega']$.

Idea of proof:

There is an explicit local description of the residue map for differentials ω with logarithmic poles: If $f = 0$ is a local equation for the hypersurface, then

$$\mathrm{res} : \omega = \frac{df}{f} \wedge \eta + \eta' \mapsto \eta \qquad \eta, \eta' \text{ locally holomorphic forms}$$

If $\ell = 1$, then ω has globally only logarithmic poles along $\mathcal{X}$. This immediately gives (a).

If $\ell = 2$, one has to consider both $\mathrm{H}^2_{\mathrm{dR}}(\mathcal{U}_K)$ and $\mathrm{H}^1_{\mathrm{dR}}(\mathcal{X}'_K)$ as hypercohomology with respect to the Čech coverings

$$\mathfrak{U} = \{\mathcal{U}_X = \{F_X \neq 0\}, \mathcal{U}_Y = \{F_Y \neq 0\}, \mathcal{U}_Z = \{F_Z \neq 0\}\} \quad \text{and } \mathfrak{U}' := \{U \cap \mathcal{X}'_K \mid U \in \mathfrak{U}\}$$

Then $\mathrm{H}^2_{\mathrm{dR}}(\mathcal{U}_K)$ is a subspace of a quotient of

$$\Gamma(\mathcal{U}_X, \Omega^2_{\mathcal{U}_K}) \oplus \Gamma(\mathcal{U}_Y, \Omega^2_{\mathcal{U}_K}) \oplus \Gamma(\mathcal{U}_Z, \Omega^2_{\mathcal{U}_K}) \oplus \Gamma(\mathcal{U}_X \cap \mathcal{U}_Y, \Omega^1_{\mathcal{U}_K}) \oplus \Gamma(\mathcal{U}_X \cap \mathcal{U}_Z, \Omega^1_{\mathcal{U}_K}) \oplus \Gamma(\mathcal{U}_Y \cap \mathcal{U}_Z, \Omega^1_{\mathcal{U}_K})$$

Similiarly, $\mathrm{H}^1_{\mathrm{dR}}(\mathcal{X}'_K)$ is expressed locally be 0-forms and 1-forms.

Procedure:

★ write ω as a Čech-2-cocycle on $\mathcal{U}_K$

★ modify it by an exact one so that every component has at most logarithmic poles

★ apply the local residue map to each component

★ add an exact 1-cocycle in order to remove the 0-form components

★ recover the image as global 1-form on $\mathcal{X}'_K$

Example:

projective genus 3 curve $Y^3Z = X^4 + XZ^3$ (in affine coordinates: $y^3 = x^4 + x$)

cohomology $\mathrm{H}^2_{\mathrm{dR}}(\mathcal{U}_{\mathbb{Q}_p})$ of the complement is spanned by

$$X\Omega/F\ ,\ Y\Omega/F\ ,\ Z\Omega/F\ ,\ X^3YZ\Omega/F^2\ ,\ X^3Z^2\Omega/F^2\ ,\ X^2YZ^2\Omega/F^2$$

cohomology $\mathrm{H}^1_{\mathrm{dR}}(\mathcal{X}'_{\mathbb{Q}_p})$ of the curve itself is spanned by

$$y\,dx\ ,\ xy\,dx\ ,\ x^2y\,dx\ ,\ xy\,dy\ ,\ x^2y\,dy\ ,\ x^3y\,dy$$

explicit residue map

$$X\Omega/F \mapsto -\tfrac{16}{9}x^3y\,dy\ \ ,\ \ Y\Omega/F \mapsto \tfrac{2}{3}y\,dy\ \ ,\ \ Z\Omega/F \mapsto -\tfrac{16}{9}x^2y\,dy\ \ ,$$
$$X^3YZ\Omega/F^2 \mapsto \tfrac{2339}{3069}x^2y\,dx\ \ ,\ \ X^3Z^2\Omega/F^2 \mapsto -\tfrac{15284528}{2097657}xy\,dy\ \ ,$$
$$X^2Y^2\Omega/F^2 \mapsto \tfrac{175406}{145521}xy\,dx$$