Computing zeta functions of nondegenerate hypersurfaces in toric varieties

Edgar Costa (Dartmouth College)

May 16th, 2018

Presented at ICERM, Birational Geometry and Arithmetic
Joint work with David Harvey (UNSW) and Kiran Kedlaya (UCSD)

Slides available at `edgarcosta.org` under Research

Motivation

Riemann zeta function

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} \cdots$$
$$= \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdots$$

- One of the most famous examples of a global zeta function
- Together with the functional equation

$$\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \xi(1-s)$$

  encodes a lot of the arithmetic information of $\mathbb{Z}$.
  e.g.: Zeros of $\zeta(s) \rightsquigarrow$ precise prime distribution
- $\zeta(s)$ still keeps secret many of its properties

Hasse–Weil zeta functions

Hasse and Weil generalized an analog of $\zeta(s)$ for algebraic varieties

$$\zeta_X(s) := \prod_p \zeta_{X_p}(p^{-s})$$

Hasse–Weil zeta functions

Hasse and Weil generalized an analog of $\zeta(s)$ for algebraic varieties

$$\zeta_X(s) := \prod_p \zeta_{X_p}(p^{-s})$$

If $X_p := X \bmod p$ is smooth, then

$$\zeta_{X_p}(t) := exp\left(\sum_{i \geq 0} \#X_p(\mathbb{F}_{p^i})\frac{t^i}{i}\right) \in \mathbb{Q}(t)$$

Hasse–Weil zeta functions

Hasse and Weil generalized an analog of $\zeta(s)$ for algebraic varieties

$$\zeta_X(s) := \prod_p \zeta_{X_p}(p^{-s})$$

If $X_p := X \bmod p$ is smooth, then

$$\zeta_{X_p}(t) := exp\left(\sum_{i\geq 0} \#X_p(\mathbb{F}_{p^i})\frac{t^i}{i}\right) \in \mathbb{Q}(t)$$

Example: $X = \{\bullet\}$, a point, then $\zeta_{\{\bullet\}}(s) = \zeta(s)$

Hasse–Weil zeta functions

Hasse and Weil generalized an analog of $\zeta(s)$ for algebraic varieties

$$\zeta_X(s) := \prod_p \zeta_{X_p}(p^{-s})$$

If $X_p := X \bmod p$ is smooth, then

$$\zeta_{X_p}(t) := exp\left(\sum_{i \geq 0} \#X_p(\mathbb{F}_{p^i})\frac{t^i}{i}\right) \in \mathbb{Q}(t)$$

Example: $X = \{\bullet\}$, a point, then $\zeta_{\{\bullet\}}(s) = \zeta(s)$

- What arithmetic properties of X can we read from $\zeta_{X_p}(s)$?
- $\zeta_{X_p}(t)$ obeys a functional equation and satisfies the Riemann hypothesis!
- What about $\zeta_X(s)$?

Elliptic curves

E an elliptic curve over $\mathbb{Q}$

$$\zeta_E(s) := \prod_p \zeta_{E_p}(p^{-s}) \quad \text{and} \quad \zeta_{E_p}(t) = \frac{L_p(t)}{(1-t)(1-pt)}$$

$$L_p(t) = \begin{cases} 1 - a_p t + pt^2, & \text{good reduction}, a_p = p + 1 - \#E_p(\mathbb{F}_p) \\ 1 \pm t, & \text{non-split/split multiplicative reduction;} \\ 1 & \text{additive reduction;} \end{cases}$$

Elliptic curves

E an elliptic curve over $\mathbb{Q}$

$$\zeta_E(s) := \prod_p \zeta_{E_p}(p^{-s}) \quad \text{and} \quad \zeta_{E_p}(t) = \frac{L_p(t)}{(1-t)(1-pt)}$$

$$L_p(t) = \begin{cases} 1 - a_p t + p t^2, & \text{good reduction}, a_p = p + 1 - \#E_p(\mathbb{F}_p) \\ 1 \pm t, & \text{non-split/split multiplicative reduction;} \\ 1 & \text{additive reduction;} \end{cases}$$

$$\zeta_E(s) = \prod_p \frac{L_p(p^{-s})}{(1-p^{-s})(1-p^{-s+1})} = \frac{\zeta(s)\zeta(s-1)}{L_E(s)}$$

Elliptic curves

E an elliptic curve over $\mathbb{Q}$

$$\zeta_E(s) := \prod_p \zeta_{E_p}(p^{-s}) \quad \text{and} \quad \zeta_{E_p}(t) = \frac{L_p(t)}{(1-t)(1-pt)}$$

$$L_p(t) = \begin{cases} 1 - a_p t + p t^2, & \text{good reduction}, a_p = p + 1 - \#E_p(\mathbb{F}_p) \\ 1 \pm t, & \text{non-split/split multiplicative reduction;} \\ 1 & \text{additive reduction;} \end{cases}$$

$$\zeta_E(s) = \prod_p \frac{L_p(p^{-s})}{(1-p^{-s})(1-p^{-s+1})} = \frac{\zeta(s)\zeta(s-1)}{L_E(s)}$$

- $a_p \rightsquigarrow$ arithmetic information about $E_p \rightsquigarrow E$.

Elliptic curves

E an elliptic curve over $\mathbb{Q}$

$$\zeta_E(s) := \prod_p \zeta_{E_p}(p^{-s}) \quad \text{and} \quad \zeta_{E_p}(t) = \frac{L_p(t)}{(1-t)(1-pt)}$$

$$L_p(t) = \begin{cases} 1 - a_p t + pt^2, & \text{good reduction}, a_p = p + 1 - \#E_p(\mathbb{F}_p) \\ 1 \pm t, & \text{non-split/split multiplicative reduction;} \\ 1 & \text{additive reduction;} \end{cases}$$

$$\zeta_E(s) = \prod_p \frac{L_p(p^{-s})}{(1-p^{-s})(1-p^{-s+1})} = \frac{\zeta(s)\zeta(s-1)}{L_E(s)}$$

- $a_p \rightsquigarrow$ arithmetic information about $E_p \rightsquigarrow E$.
- Modularity theorem $\implies$ L_E satisfies a functional equation
- Birch–Swinnerton-Dyer conjecture predicts $\operatorname{ord}_{s=1} L_E(s) = \operatorname{rk}(E)$.

$\zeta(s)$ vs $\zeta_X(s)$

We always expect $\zeta_X(s)$ to satisfy a functional equation.

- zero-dimensional varieties (number fields) ✓
- elliptic curves over $\mathbb{Q}$ ✓
- genus 2 curves ?

$\zeta(s)$ vs $\zeta_X(s)$

We always expect $\zeta_X(s)$ to satisfy a functional equation.

- zero-dimensional varieties (number fields) ✓
- elliptic curves over $\mathbb{Q}$ ✓
- genus 2 curves ? numerically ✓

$\zeta(s)$ vs $\zeta_X(s)$

We always expect $\zeta_X(s)$ to satisfy a functional equation.

- zero-dimensional varieties (number fields) ✓
- elliptic curves over $\mathbb{Q}$ ✓
- genus 2 curves ? numerically ✓
- surfaces ?

$\zeta(s)$ vs $\zeta_X(s)$

We always expect $\zeta_X(s)$ to satisfy a functional equation.

- zero-dimensional varieties (number fields) ✓
- elliptic curves over $\mathbb{Q}$ ✓
- genus 2 curves ? numerically ✓
- surfaces ?

Major difference

- easy to explicitly write down $\zeta(s)$
- extremely difficult to calculate $\zeta_{X_p}(t)$ for an arbitrary X

$\zeta(s)$ vs $\zeta_X(s)$

We always expect $\zeta_X(s)$ to satisfy a functional equation.

- zero-dimensional varieties (number fields) ✓
- elliptic curves over $\mathbb{Q}$ ✓
- genus 2 curves ? numerically ✓
- surfaces ?

Major difference

- easy to explicitly write down $\zeta(s)$
- extremely difficult to calculate $\zeta_{X_p}(t)$ for an arbitrary X

Problem

Given an *explicit* description of X, compute

$$\zeta_{X_p}(t) := exp\left(\sum_{i\geq 0} \#X_p(\mathbb{F}_{p^i})\frac{t^i}{i}\right) \in \mathbb{Q}(t)$$

The zeta function problem

Let X be a smooth variety over a finite field $\mathbb{F}_q$ of characteristic p, consider

$$\zeta_X(t) := exp\left(\sum_{i\geq 1} \#X(\mathbb{F}_{q^i})\frac{t^i}{i}\right)$$

Problem

Compute ζ_X from an *explicit* description of X.

The zeta function problem

Let X be a smooth variety over a finite field $\mathbb{F}_q$ of characteristic p, consider

$$\zeta_X(t) := exp\left(\sum_{i\geq 1} \#X(\mathbb{F}_{q^i})\frac{t^i}{i}\right)$$

Problem

Compute ζ_X from an *explicit* description of X.

Theoretically this is "trivial".
The degree of ζ_X is bounded by the geometry of X, and we can then enumerate $X(\mathbb{F}_{q^i})$ for enough i to pinpoint ζ_X.

The zeta function problem

Let X be a smooth variety over a finite field $\mathbb{F}_q$ of characteristic p, consider

$$\zeta_X(t) := exp\left(\sum_{i\geq 1} \#X(\mathbb{F}_{q^i})\frac{t^i}{i}\right)$$

Problem

Compute ζ_X from an *explicit* description of X.

Theoretically this is "trivial".
The degree of ζ_X is bounded by the geometry of X, and we can then enumerate $X(\mathbb{F}_{q^i})$ for enough i to pinpoint ζ_X.

This approach is only practical for very few classes of varieties, e.g., low genus curves and p small.

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing Isomorphism/Isogeny

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing Isomorphism/Isogeny
- Computing $\mathrm{End}(A)$ for A an abelian variety.

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing Isomorphism/Isogeny
- Computing $\mathrm{End}(A)$ for A an abelian variety.
  $\rightsquigarrow$ A couple of $\zeta_{A_p}(t)$ usually give away the shape of $\mathrm{End}(A)$.
- Computing Picard number of a K3 surface

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing Isomorphism/Isogeny
- Computing $\mathrm{End}(A)$ for A an abelian variety.
  $\rightsquigarrow$ A couple of $\zeta_{A_p}(t)$ usually give away the shape of $\mathrm{End}(A)$.
- Computing Picard number of a K3 surface
  $\rightsquigarrow$ sufficient criterion for infinitely many rational curves on a K3

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing Isomorphism/Isogeny
- Computing $\mathrm{End}(A)$ for A an abelian variety.
  $\rightsquigarrow$ A couple of $\zeta_{A_p}(t)$ usually give away the shape of $\mathrm{End}(A)$.
- Computing Picard number of a K3 surface
  $\rightsquigarrow$ sufficient criterion for infinitely many rational curves on a K3
- Testing the speciality of a cubic fourfold
- Computing L-functions and their special values, e.g.:
  - Birch–Swinnerton-Dyer conjecture $\rightsquigarrow \mathrm{rk}(A)$
  - searching for Langlands correspondences

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing Isomorphism/Isogeny
- Computing $\mathrm{End}(A)$ for A an abelian variety.
  $\rightsquigarrow$ A couple of $\zeta_{A_p}(t)$ usually give away the shape of $\mathrm{End}(A)$.
- Computing Picard number of a K3 surface
  $\rightsquigarrow$ sufficient criterion for infinitely many rational curves on a K3
- Testing the speciality of a cubic fourfold
- Computing L-functions and their special values, e.g.:
  - Birch–Swinnerton-Dyer conjecture $\rightsquigarrow \mathrm{rk}(A)$
  - searching for Langlands correspondences
- Arithmetic statistics
  - Sato–Tate
  - Lang–Trotter

Common Approaches

- Very generic algorithms derived from Dwork's p-adic analytic proof that $\zeta_X(t) \in \mathbb{Q}(t)$

Common Approaches

- Very generic algorithms derived from Dwork's p-adic analytic proof that $\zeta_X(t) \in \mathbb{Q}(t)$
- ℓ-adic: by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.

Common Approaches

- Very generic algorithms derived from Dwork's p-adic analytic proof that $\zeta_X(t) \in \mathbb{Q}(t)$
- ℓ-adic: by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.
    - We need to have an effective *description* of the cohomology.
    - E.g.: for abelian varieties we have Schoof-Pila's method However, only practical if $g \leq 2$ or some extra structure is available.

Common Approaches

- Very generic algorithms derived from Dwork's p-adic analytic proof that $\zeta_X(t) \in \mathbb{Q}(t)$
- ℓ-adic: by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.
    - We need to have an effective *description* of the cohomology.
    - E.g.: for abelian varieties we have Schoof-Pila's method However, only practical if $g \leq 2$ or some extra structure is available.
- p-adic: based on Monsky–Washnitzer cohomology

Today

New p-adic method to compute $\zeta_X(t)$ that achieves a striking balance between **practicality** and **generality**.

Outline

Toric hypersurfaces

p-adic Cohomology

Some examples

Toric hypersurfaces

Toy example, the Projective space

- There are many ways to define the $\mathbb{P}^n$

Toy example, the Projective space

- There are many ways to define the $\mathbb{P}^n$
- For example, let

  $$P_d := \text{homogeneous polynomials in } n+1 \text{ variables of degree } d$$

  and consider the graded ring

  $$P := \bigoplus_{d \geq 0} P_d.$$

  Then we have $\mathbb{P}^n := \operatorname{Proj} P$

Toy example, the Projective space

- There are many ways to define the $\mathbb{P}^n$
- For example, let

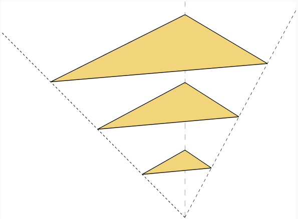
$$P_d := \text{homogeneous polynomials in } n+1 \text{ variables of degree } d$$

and consider the graded ring

$$P := \bigoplus_{d \geq 0} P_d.$$

Then we have $\mathbb{P}^n := \operatorname{Proj} P$

- We can think of $P_d := R[d\Delta \cap \mathbb{Z}^n]$, where Δ is the standard simplex.
- Idea: generalize Δ to be any polytope.



Toric hypersurfaces

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in R[x_1^\pm, \ldots, x_n^\pm]$ a Laurent polynomial
- f defines an hypersurface in the torus $\mathbb{T}^n := \mathrm{Spec}(R[x_1^\pm, \ldots, x_n^\pm])$

Toric hypersurfaces

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in R[x_1^\pm, \ldots, x_n^\pm]$ a Laurent polynomial
- f defines an hypersurface in the torus $\mathbb{T}^n := \mathrm{Spec}(R[x_1^\pm, \ldots, x_n^\pm])$
- $\Delta :=$ Newton polytope of f = convex hull of the support of f in $\mathbb{R}^n$

Toric hypersurfaces

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in R[x_1^\pm, \ldots, x_n^\pm]$ a Laurent polynomial
- f defines an hypersurface in the torus $\mathbb{T}^n := \mathrm{Spec}(R[x_1^\pm, \ldots, x_n^\pm])$
- $\Delta :=$ Newton polytope of f = convex hull of the support of f in $\mathbb{R}^n$
- To Δ we can associate a graded ring and a projective variety.

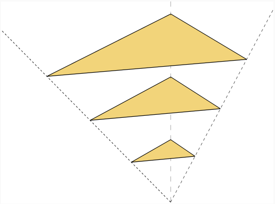
Toric hypersurfaces

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in R[x_1^\pm, \ldots, x_n^\pm]$ a Laurent polynomial
- f defines an hypersurface in the torus $\mathbb{T}^n := \mathrm{Spec}(R[x_1^\pm, \ldots, x_n^\pm])$
- $\Delta :=$ Newton polytope of f = convex hull of the support of f in $\mathbb{R}^n$
- To Δ we can associate a graded ring and a projective variety.

$$P_\Delta := \bigoplus_{d \geq 0} P_d, \quad P_d := R[x^\alpha : \alpha \in d\Delta \cap \mathbb{Z}^n]$$

$$\mathbb{P}_\Delta := \mathrm{Proj}\, P_\Delta$$

$$X_f := \mathrm{Proj}\, P_\Delta/(f) \subset \mathbb{P}_\Delta$$



X_f is an hypersurface in the toric variety $\mathbb{P}_\Delta$

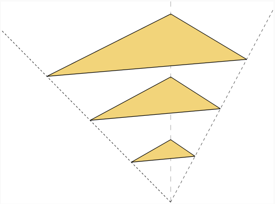
Toric hypersurfaces

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in R[x_1^\pm, \ldots, x_n^\pm]$ a Laurent polynomial
- f defines an hypersurface in the torus $\mathbb{T}^n := \mathrm{Spec}(R[x_1^\pm, \ldots, x_n^\pm])$
- $\Delta :=$ Newton polytope of f = convex hull of the support of f in $\mathbb{R}^n$
- To Δ we can associate a graded ring and a projective variety.

$$P_\Delta := \bigoplus_{d \geq 0} P_d, \quad P_d := R[x^\alpha : \alpha \in d\Delta \cap \mathbb{Z}^n]$$

$$\mathbb{P}_\Delta := \mathrm{Proj}\, P_\Delta$$

$$X_f := \mathrm{Proj}\, P_\Delta/(f) \subset \mathbb{P}_\Delta$$



X_f is an hypersurface in the toric variety $\mathbb{P}_\Delta$

Examples

Δ	X_Δ
$\mathrm{Conv}(0, e_1, \ldots, e_n)$	$\mathbb{P}^n$
$\mathrm{Conv}(0, e_1, \ell e_2, \ldots, \ell e_n)$	$\mathbb{P}^n(\ell, 1, \ldots, 1)$
$\mathrm{Conv}(0, e_1, e_2, e_1 + e_2) = [0, 1]^2$	$\mathbb{P}^1 \times \mathbb{P}^1$

Toric hypersurfaces are everywhere

Vertices of Δ	Resulting hypersurface
$0, de_1, de_2$	Smooth plane curve of genus $\binom{d-1}{2}$
$0, (2g+1)e_1, 2e_2$	Odd hyperelliptic curve of genus g
$0, ae_1, be_2$	$C_{a,b}$-curve
$0, 4e_1, 4e_2, 4e_3$	Quartic K3 surface
$0, 2e_1, 6e_2, 6e_3$	Degree 2 K3 surface

Toric hypersurfaces are everywhere

Vertices of Δ	Resulting hypersurface
$0, de_1, de_2$	Smooth plane curve of genus $\binom{d-1}{2}$
$0, (2g+1)e_1, 2e_2$	Odd hyperelliptic curve of genus g
$0, ae_1, be_2$	$C_{a,b}$-curve
$0, 4e_1, 4e_2, 4e_3$	Quartic K3 surface
$0, 2e_1, 6e_2, 6e_3$	Degree 2 K3 surface

(All the examples above are hypersurfaces in a weighted projective spaces.)

Toric hypersurfaces are everywhere

Vertices of Δ	Resulting hypersurface
$0, de_1, de_2$	Smooth plane curve of genus $\binom{d-1}{2}$
$0, (2g+1)e_1, 2e_2$	Odd hyperelliptic curve of genus g
$0, ae_1, be_2$	$C_{a,b}$-curve
$0, 4e_1, 4e_2, 4e_3$	Quartic K3 surface
$0, 2e_1, 6e_2, 6e_3$	Degree 2 K3 surface

(All the examples above are hypersurfaces in a weighted projective spaces.)

K3 surfaces can arise as hypersurfaces:

- in $\mathbb{P}^3$, as a quartic surface;

Toric hypersurfaces are everywhere

Vertices of Δ	Resulting hypersurface
$0, de_1, de_2$	Smooth plane curve of genus $\binom{d-1}{2}$
$0, (2g+1)e_1, 2e_2$	Odd hyperelliptic curve of genus g
$0, ae_1, be_2$	$C_{a,b}$-curve
$0, 4e_1, 4e_2, 4e_3$	Quartic K3 surface
$0, 2e_1, 6e_2, 6e_3$	Degree 2 K3 surface

(All the examples above are hypersurfaces in a weighted projective spaces.)

K3 surfaces can arise as hypersurfaces:

- in $\mathbb{P}^3$, as a quartic surface;
- in 95 weighed projective spaces;

Toric hypersurfaces are everywhere

Vertices of Δ	Resulting hypersurface
$0, de_1, de_2$	Smooth plane curve of genus $\binom{d-1}{2}$
$0, (2g+1)e_1, 2e_2$	Odd hyperelliptic curve of genus g
$0, ae_1, be_2$	$C_{a,b}$-curve
$0, 4e_1, 4e_2, 4e_3$	Quartic K3 surface
$0, 2e_1, 6e_2, 6e_3$	Degree 2 K3 surface

(All the examples above are hypersurfaces in a weighted projective spaces.)

K3 surfaces can arise as hypersurfaces:

- in $\mathbb{P}^3$, as a quartic surface;
- in 95 weighed projective spaces;
- in **4319** toric varieties.

Keeping our eyes on the prize

Given

$$f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^{\pm}, \ldots, x_n^{\pm}]$$

efficiently compute

$$\begin{aligned}\zeta_X(t) &:= exp\left(\sum_{i \geq 1} \#X(\mathbb{F}_{q^i}) \frac{t^i}{i}\right) \\ &= \prod_i \det\bigl(1 - t\,\mathrm{Frob}\,|H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)\bigr)^{(-1)^{i+1}} \in \mathbb{Q}(t),\end{aligned}$$

where $X := \mathrm{Proj}\, P_\Delta/(f) \subset \mathbb{P}_\Delta$

Keeping our eyes on the prize

Given

$$f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^{\pm}, \ldots, x_n^{\pm}]$$

efficiently compute

$$\zeta_X(t) := exp\left(\sum_{i \geq 1} \#X(\mathbb{F}_{q^i}) \frac{t^i}{i}\right)$$
$$= \prod_i \det\left(1 - t\,\mathrm{Frob}\,|H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}} \in \mathbb{Q}(t),$$

where $X := \mathrm{Proj}\, P_\Delta/(f) \subset \mathbb{P}_\Delta$

But under what assumptions on X? Is smoothness enough?

Keeping our eyes on the prize

Given

$$f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^{\pm}, \ldots, x_n^{\pm}]$$

efficiently compute

$$\zeta_X(t) := exp\left(\sum_{i \geq 1} \#X(\mathbb{F}_{q^i}) \frac{t^i}{i}\right)$$
$$= \prod_i \det\left(1 - t\,\mathrm{Frob}\,|H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}} \in \mathbb{Q}(t),$$

where $X := \mathrm{Proj}\, P_\Delta/(f) \subset \mathbb{P}_\Delta$

But under what assumptions on X? Is smoothness enough?

We will need a bit more, we will **nondegeneracy**.

Nondegenerate toric hypersurfaces

Geometric definition

An hypersurface is **nondegenerate** if the cross-section by any bounding hyperplane (in any dimension) are all smooth in their respective tori.

Equivalently, if for every face $\sigma \subseteq \Delta$, f restricted to the torus associated to σ is nonsingular of codimension 1.

Nondegenerate toric hypersurfaces

Geometric definition

An hypersurface is **nondegenerate** if the cross-section by any bounding hyperplane (in any dimension) are all smooth in their respective tori.

Equivalently, if for every face $\sigma \subseteq \Delta$, f restricted to the torus associated to σ is nonsingular of codimension 1.

Example

Let C be a plane curve in $\mathbb{P}^2$, then C is nondegenerate if:

- C does not pass through the points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$;
- C intersects the coordinate axes $x = 0$, $y = 0$, $z = 0$ transversally;
- C is smooth on the complement of the coordinate axes.

Nondegenerate toric hypersurfaces

Geometric definition

An hypersurface is **nondegenerate** if the cross-section by any bounding hyperplane (in any dimension) are all smooth in their respective tori.

Equivalently, if for every face $\sigma \subseteq \Delta$, f restricted to the torus associated to σ is nonsingular of codimension 1.

Example

Let C be a plane curve in $\mathbb{P}^2$, then C is nondegenerate if:

- C does not pass through the points $(1, 0, 0), (0, 1, 0), (0, 0, 1)$;
- C intersects the coordinate axes $x = 0$, $y = 0$, $z = 0$ transversally;
- C is smooth on the complement of the coordinate axes.

In terms of ideals, $\operatorname{rad} \left\langle x\frac{\partial}{\partial x}f, y\frac{\partial}{\partial y}f, z\frac{\partial}{\partial z}f, f \right\rangle = \langle x, y, z \rangle$

p-adic Cohomology

Goal

Setup

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^\pm, \ldots, x_n^\pm]$
- $X := \operatorname{Proj} P_\Delta/(f) \subset \mathbb{P}_\Delta$ a nondegenerate hypersurface

Goal

Compute

$$\begin{aligned}\zeta_X(t) &:= exp\left(\sum_{i\geq 1} \#X(\mathbb{F}_{q^i}) t^i / i\right) \\ &= \prod_i \det\left(1 - t \operatorname{Frob} | H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}} \\ &= Q(t)^{(-1)^n} \zeta_{\mathbb{P}_\Delta}(t),\end{aligned}$$

where $\quad Q(t) := \det(1 - t \operatorname{Frob} | PH^{n-1}_{\mathrm{et}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)) \in 1 + \mathbb{Z}[t]$

Master plan

Setup

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^\pm, \ldots, x_n^\pm]$
- $X := \operatorname{Proj} P_\Delta/(f) \subset \mathbb{P}_\Delta$ a nondegenerate hypersurface
- $\sigma :=$ p-th power Frobenius map

Goal

Compute the matrix representing the action of σ in $PH^{n-1}_{\mathrm{rig}}(X)$ with enough of p-adic precision to deduce

$$Q(t) = \det(1 - q^{-1} t \operatorname{Frob} | PH^{n-1}_{\mathrm{rig}}(X)) \in 1 + \mathbb{Z}[t].$$

Master plan

Setup

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^\pm, \ldots, x_n^\pm]$
- $X := \operatorname{Proj} P_\Delta/(f) \subset \mathbb{P}_\Delta$ a nondegenerate hypersurface
- $\sigma :=$ p-th power Frobenius map

Goal

Compute the matrix representing the action of σ in $PH^{n-1}_{\text{rig}}(X)$ with enough of p-adic precision to deduce

$$Q(t) = \det(1 - q^{-1} t \operatorname{Frob} | PH^{n-1}_{\text{rig}}(X)) \in 1 + \mathbb{Z}[t].$$

Instead, of working with rigid cohomology, we will work with the Monsky–Washnitzer cohomology $PH^{\dagger, n-1}(X)$

Master plan

Setup

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^\pm, \dots, x_n^\pm]$
- $X := \operatorname{Proj} P_\Delta / (f) \subset \mathbb{P}_\Delta$ a nondegenerate hypersurface
- $\sigma :=$ p-th power Frobenius map

Goal

Compute the matrix representing the action of σ in $PH^{n-1}_{\mathrm{rig}}(X)$ with enough of p-adic precision to deduce

$$Q(t) = \det(1 - q^{-1} t \operatorname{Frob} | PH^{n-1}_{\mathrm{rig}}(X)) \in 1 + \mathbb{Z}[t].$$

Instead, of working with rigid cohomology, we will work with the Monsky–Washnitzer cohomology $PH^{\dagger, n-1}(X)$ $(\subset PH^{\dagger, n-1}(\mathbb{T} \backslash X))$.

Overall picture

Goal

Compute the matrix representing the action of σ in $PH^{\dagger,n-1}(X)$ with enough p-adic precision.

Overall picture

Goal

Compute the matrix representing the action of σ in $PH^{\dagger,n-1}(X)$ with enough p-adic precision.

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger,n-1}(X) \circlearrowright \sigma$$

Overall picture

Goal

Compute the matrix representing the action of σ in $PH^{\dagger,n-1}(X)$ with enough p-adic precision.

$$\begin{array}{ccc} & & \overset{\sigma}{\curvearrowright} \\ PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) & \xrightarrow[\mathrm{id}]{\sim} & PH^{\dagger,n-1}(X) \\ \Big\downarrow & & \\ \text{explicit description over } \mathbb{C} & & \\ \text{[Dwork–Griffiths, Batyrev–Cox]} & & \end{array}$$

Overall picture

Goal

Compute the matrix representing the action of σ in $PH^{\dagger,n-1}(X)$ with enough p-adic precision.

$$
\begin{array}{ccc}
PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) & \xrightarrow[\mathrm{id}]{\sim} & PH^{\dagger,n-1}(X) \circlearrowright \sigma \\
\downarrow & & \downarrow \\
\text{explicit description over } \mathbb{C} & & \text{de Rham cohomology} \\
\text{[Dwork–Griffiths, Batyrev–Cox]} & & \text{with overconvergent power series}
\end{array}
$$

Overall picture

Goal

Compute the matrix representing the action of σ in $PH^{\dagger,n-1}(X)$ with enough p-adic precision.

$$\begin{array}{ccc} & & \circlearrowright \sigma \\ PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) & \xrightarrow[\mathrm{id}]{\sim} & PH^{\dagger,n-1}(X) \\ \downarrow & & \downarrow \end{array}$$

explicit description over $\mathbb{C}$
[Dwork–Griffiths, Batyrev–Cox]

de Rham cohomology
with overconvergent power series

cohomology relations
+
commutative algebra

$\Longrightarrow$

basis for $PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) = \left\{ x^{\beta}\omega/f^{i} \right\}_{\beta}$
+
reduction algorithm

Generic algorithm – Abbott–Kedlaya–Roe type

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger,n-1}(X) \circlearrowright \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m} \omega \right\}_\beta$ a monomial basis for $PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q})$ where $\omega := \frac{\mathrm{d}x_1}{x_1} \wedge \cdots \wedge \frac{\mathrm{d}x_n}{x_n}$

Generic algorithm – Abbott–Kedlaya–Roe type

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger,n-1}(X) \circlearrowright \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m}\omega \right\}_\beta$ a monomial basis for $PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q})$ where $\omega := \frac{\mathrm{d}x_1}{x_1} \wedge \cdots \wedge \frac{\mathrm{d}x_n}{x_n}$
2. In $PH^{\dagger,n}$ compute a series approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) = p^n \frac{x^{p\beta}}{f^{pm}}\omega \sum_{i\geq 0} \binom{-m}{i} \left(\frac{\sigma(f) - f^p}{f^p}\right)^i$$

Generic algorithm – Abbott–Kedlaya–Roe type

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger, n-1}(X) \circlearrowright \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m} \omega \right\}_\beta$ a monomial basis for $PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q})$ where $\omega := \frac{\mathrm{d}x_1}{x_1} \wedge \cdots \wedge \frac{\mathrm{d}x_n}{x_n}$
2. In $PH^{\dagger,n}$ compute a series approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) = p^n \frac{x^{p\beta}}{f^{pm}} \omega \sum_{i \geq 0} \binom{-m}{i} \left(\frac{\sigma(f) - f^p}{f^p}\right)^i$$

3. Write the approximation in terms of basis elements, i.e., apply the de Rham relations

Generic algorithm – Abbott–Kedlaya–Roe type

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger,n-1}(X) \circlearrowleft \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m} \omega \right\}_\beta$ a monomial basis for $PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q})$ where $\omega := \frac{\mathrm{d}x_1}{x_1} \wedge \cdots \wedge \frac{\mathrm{d}x_n}{x_n}$
2. In $PH^{\dagger,n}$ compute a series approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) = p^n \frac{x^{p\beta}}{f^{pm}} \omega \sum_{i \geq 0} \binom{-m}{i} \left(\frac{\sigma(f) - f^p}{f^p}\right)^i$$

3. Write the approximation in terms of basis elements, i.e., apply the de Rham relations

Note: Originally for smooth hypersurfaces in the projective space.

A sparse representation of Frobenius

Unfortunately, the truncation of the series expansion to K terms

$$\sigma\left(\frac{x^{\beta}}{f^{m}}\omega\right) \approx p^{n}\frac{x^{p\beta}\omega}{f^{pm}}\sum_{i=0}^{K-1}\binom{-m}{i}\left(\frac{\sigma(f)-f^{p}}{f^{p}}\right)^{i}$$

involves dense polynomials of degree $p(K-1)$ in n variables, and thus an unavoidable factor of p^{n} in the runtime.

A sparse representation of Frobenius

Unfortunately, the truncation of the series expansion to K terms

$$\sigma\left(\frac{x^{\beta}}{f^{m}}\omega\right) \approx p^{n}\frac{x^{p\beta}\omega}{f^{pm}}\sum_{i=0}^{K-1}\binom{-m}{i}\left(\frac{\sigma(f)-f^{p}}{f^{p}}\right)^{i}$$

involves dense polynomials of degree $p(K-1)$ in n variables, and thus an unavoidable factor of p^n in the runtime.

But there is another way...

By expanding $\left(\frac{\sigma(f)-f^{p}}{f^{p}}\right)^{i}$ with the binomial theorem, swapping the summation order, we are able to rewrite in a sparse way.

A sparse representation of Frobenius

Unfortunately, the truncation of the series expansion to K terms

$$\sigma\left(\frac{x^{\beta}}{f^{m}}\omega\right) \approx p^{n}\frac{x^{p\beta}\omega}{f^{pm}}\sum_{i=0}^{K-1}\binom{-m}{i}\left(\frac{\sigma(f)-f^{p}}{f^{p}}\right)^{i}$$

involves dense polynomials of degree $p(K-1)$ in n variables, and thus an unavoidable factor of p^n in the runtime.

But there is another way...

By expanding $\left(\frac{\sigma(f)-f^{p}}{f^{p}}\right)^{i}$ with the binomial theorem, swapping the summation order, we are able to rewrite in a sparse way.

$$\sum_{i=0}^{K-1}\binom{-m}{i}\left(\frac{\sigma(f)-f^{p}}{f^{p}}\right)^{i} = \cdots = \sum_{i=0}^{K-1}\binom{-m}{i}\binom{m+K-1}{K-i-1}\sigma(f)^{i}f^{-p(m+i)}$$

Schematically

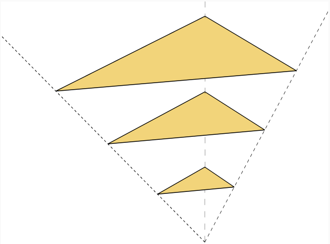
Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$
$(pdK)^{n+O(1)}$ terms		

Schematically

Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f) - f^p}{f^p} \right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$
$(pdK)^{n+O(1)}$ terms		$(dK)^{n+O(1)}$ terms

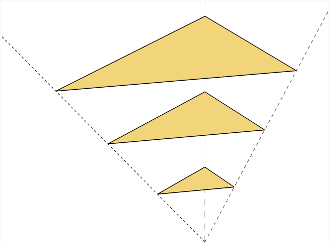
Schematically

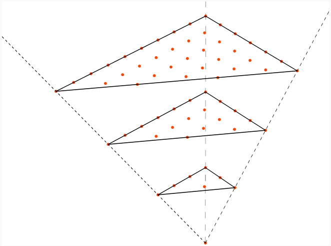
Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$
$(pdK)^{n+O(1)}$ terms		$(dK)^{n+O(1)}$ terms



Schematically

Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$
$(pdK)^{n+O(1)}$ terms		$(dK)^{n+O(1)}$ terms

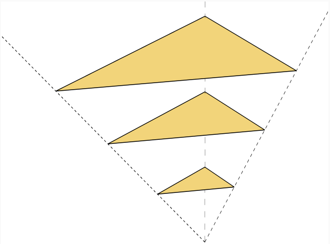




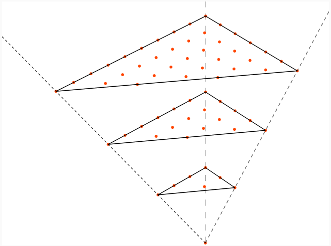
Schematically

Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f) - f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$

$(pdK)^{n+O(1)}$ terms



$(dK)^{n+O(1)}$ terms



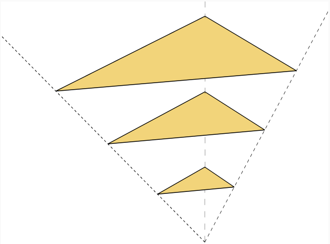
$$\rho : P_{\ell+1} \longmapsto P_\ell$$

$$g \frac{\omega}{f^{\ell+1}} \equiv \rho(g) \frac{\omega}{f^\ell}$$

Schematically

Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$

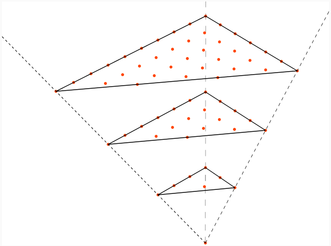
$(pdK)^{n+O(1)}$ terms



$$\rho : P_{\ell+1} \longmapsto P_\ell$$

$$g\frac{\omega}{f^{\ell+1}} \equiv \rho(g)\frac{\omega}{f^\ell}$$

$(dK)^{n+O(1)}$ terms



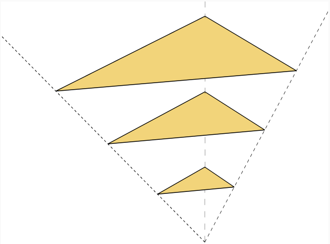
$$\pi : P_n \longmapsto P_n$$

$$x^{\alpha+\beta} g\frac{\omega}{f^{\ell+1}} \equiv x^\beta \pi(g)\frac{\omega}{f^\ell},$$

Schematically

Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$

$(pdK)^{n+O(1)}$ terms

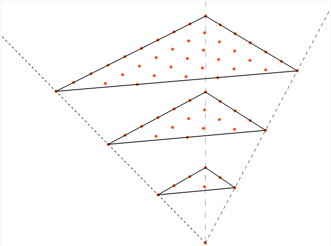


$\rho : P_{\ell+1} \longmapsto P_\ell$

$$g\frac{\omega}{f^{\ell+1}} \equiv \rho(g)\frac{\omega}{f^\ell}$$

“slice” $\mapsto$ “slice”

$(dK)^{n+O(1)}$ terms



$\pi : P_n \longmapsto P_n$

$$x^{\alpha+\beta} g\frac{\omega}{f^{\ell+1}} \equiv x^\beta \pi(g)\frac{\omega}{f^\ell},$$

“dot” $\mapsto$ “dot”

Generic algorithm – C.–Harvey–Kedlaya

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger,n-1}(X) \circlearrowright \sigma$$

1. Compute $\left\{\frac{x^\beta}{f^m}\omega\right\}_\beta$ a monomial basis for $PH^n_{\mathrm{dR}}(X_{\mathbb{Q}_q})$
2. In $PH^{\dagger,n}$ compute a **sparse** approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) \approx p^n \frac{x^{p\beta}}{f^{pm}} \sum_{i=0}^{N-1} \binom{-m}{i} \binom{m+N-1}{N-i-1} \sigma(f)^i f^{-p(m+i)}$$

3. Apply **sparse** reduction algorithm to reduce expansion to basis elements.
   - Involves multiplying together $O(p)$ matrices of size $\#(n\Delta \cap L) \sim n^n \operatorname{vol} \Delta$

Generic algorithm – C.–Harvey–Kedlaya

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger,n-1}(X) \circlearrowright \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m}\omega \right\}_\beta$ a monomial basis for $PH^n_{\mathrm{dR}}(X_{\mathbb{Q}_q})$
2. In $PH^{\dagger,n}$ compute a **sparse** approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) \approx p^n \frac{x^{p\beta}}{f^{pm}} \sum_{i=0}^{N-1} \binom{-m}{i} \binom{m+N-1}{N-i-1} \sigma(f)^i f^{-p(m+i)}$$

3. Apply **sparse** reduction algorithm to reduce expansion to basis elements.
   - Involves multiplying together $O(p)$ matrices of size $\#(n\Delta \cap L) \sim n^n \operatorname{vol} \Delta$
   - In a more convoluted process, we can reduce the matrix size to $n! \operatorname{vol} \Delta$, saving a factor of $e^n \approx n^n/n!$ (e.g. $220 \rightsquigarrow 64$)

Generic algorithm – C.–Harvey–Kedlaya

$$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger, n-1}(X) \circlearrowright \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m} \omega \right\}_\beta$ a monomial basis for $PH^n_{\mathrm{dR}}(X_{\mathbb{Q}_q})$
2. In $PH^{\dagger, n}$ compute a **sparse** approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) \approx p^n \frac{x^{p\beta}}{f^{pm}} \sum_{i=0}^{N-1} \binom{-m}{i} \binom{m+N-1}{N-i-1} \sigma(f)^i f^{-p(m+i)}$$

3. Apply **sparse** reduction algorithm to reduce expansion to basis elements.
    - Involves multiplying together $O(p)$ matrices of size $\#(n\Delta \cap L) \sim n^n \operatorname{vol} \Delta$
    - In a more convoluted process, we can reduce the matrix size to $n! \operatorname{vol} \Delta$, saving a factor of $e^n \approx n^n / n!$ (e.g. $220 \rightsquigarrow 64$)

For large p, all the work is in step 3

Some Remarks

- **Complexity**
  First version of our new algorithm has complexity roughly

$$p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

Some Remarks

- **Complexity**
  First version of our new algorithm has complexity roughly

$$p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

  and space complexity is only

$$\log p \operatorname{vol}(\Delta)^{O(n)}.$$

Some Remarks

- Complexity
  First version of our new algorithm has complexity roughly

$$p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

  and space complexity is only

$$\log p \operatorname{vol}(\Delta)^{O(n)}.$$

  This allows us to handle examples with much larger p than any found in the literature.

Some Remarks

- Complexity

  First version of our new algorithm has complexity roughly

  $$p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

  and space complexity is only

  $$\log p \operatorname{vol}(\Delta)^{O(n)}.$$

  This allows us to handle examples with much larger p than any found in the literature.

- Implementation
  - Projective hypersurfaces ($\sim$2014): C++ with NTL and Flint
    Soon available in Sage

Some Remarks

- **Complexity**
  First version of our new algorithm has complexity roughly

$$p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

  and space complexity is only

$$\log p \operatorname{vol}(\Delta)^{O(n)}.$$

  This allows us to handle examples with much larger p than any found in the literature.
- **Implementation**
  - Projective hypersurfaces (∼2014): C++ with NTL and Flint
    Soon available in Sage
  - Toric hypersurfaces: beta version in C++ with NTL

Some examples

Example: K3 surface in the Dwork pencil

Consider the projective quartic surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ given by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0.$$

For $\lambda = 1$ and $p = 2^{20} - 3$, using the old projective code in `22h7m` we compute that

$$\zeta_X(t)^{-1} = (1 - t)(1 - pt)^{16}(1 + pt)^3(1 - p^2 t)Q(t),$$

where the "interesting" factor is

$$Q(t) = (1 + pt)(1 - 1688538t + p^2 t^2).$$

The polynomials R_1 and R_2 arise from the action of Frobenius on the Picard lattice; by a p-adic formula of de la Ossa–Kadir.

Example: a quartic surface in the Dwork pencil

Consider the projective quartic surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ given by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0.$$

For $\lambda = 1$ and $p = 2^{20} - 3$, using the toric ~~old projective~~ code in `1m33s` ~~`22h7m`~~ we compute

$$\zeta_X(t)^{-1} = (1-t)(1-pt)^{16}(1+pt)^3(1-p^2t)(1+pt)(1-1688538t+p^2t^2).$$

Example: a quartic surface in the Dwork pencil

Consider the projective quartic surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ given by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0.$$

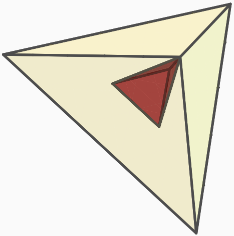
For $\lambda = 1$ and $p = 2^{20} - 3$, using the toric ~~old projective~~ code in `1m33s` ~~`22h7m`~~ we compute

$$\zeta_X(t)^{-1} = (1-t)(1-pt)^{16}(1+pt)^3(1-p^2t)(1+pt)(1-1688538t+p^2t^2).$$

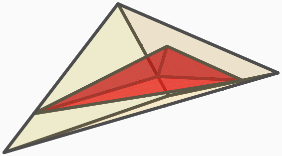
The defining monomials of X generate a sublattice of index 4^2 in $\mathbb{Z}^3$, and we can work "in" that sublattice, by using

$$x^4y^{-1}z^{-1} + \lambda x + y + z + 1 = 0$$

which has a polytope much smaller than the full simplex ($32/3 \approx 10.6$ vs $2/3 \approx 0.6$).



Example: a hypergeometric motive (also a K3 surface)



Consider the appropriate completion of the toric surface over $\mathbb{F}_p$ with $p = 2^{15} - 19$ given by

$$x^3 y + y^4 + z^4 - 12xyz + 1 = 0.$$

In `4s`, we compute that the "interesting" factor of $\zeta_X(t)$ is (up to rescaling)

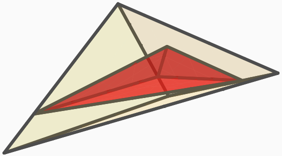
$$pQ(t/p) = p + 20508t^1 - 18468t^2 - 26378t^3 - 18468t^4 + 20508t^5 + pt^6.$$

In $\mathbb{P}^3$ this surface is degenerate, and would have taken us `27m12s` to do the same computation with a dense model.

Example: a hypergeometric motive (also a K3 surface)

Consider the appropriate completion of the toric surface over $\mathbb{F}_p$ with $p = 2^{15} - 19$ given by

$$x^3y + y^4 + z^4 - 12xyz + 1 = 0.$$



In `4s`, we compute that the “interesting” factor of $\zeta_X(t)$ is (up to rescaling)

$$pQ(t/p) = p + 20508t^1 - 18468t^2 - 26378t^3 - 18468t^4 + 20508t^5 + pt^6.$$

In $\mathbb{P}^3$ this surface is degenerate, and would have taken us `27m12s` to do the same computation with a dense model.

We can confirm the linear term with Magma:

```
C2F2 := HypergeometricData([6,12], [1,1,1,2,3]);
EulerFactor(C2F2, 2^10 * 3^6, 2^15-19: Degree:=1);
1 + 20508*$.1 + O($.1^2)
```

Example: a K3 surface in a non weighted projective space

Consider the surface X defined as the closure (in $\mathbb{P}_\Delta$) of the affine surface defined by the Laurent polynomial

$$3x + y + z + x^{-2}y^2z + x^3y^{-6}z^{-2} + 3x^{-2}y^{-1}z^{-2} - 2 - x^{-1}y - y^{-1}z^{-1} - x^2y^{-4}z^{-1} - xy^{-3}z^{-1}.$$

The Hodge numbers of $PH^2(X)$ are $(1, 14, 1)$. For $p = 2^{15} - 19$, in `6m20s` we obtain the "interesting" factor of $\zeta_X(t)$:

$$pQ(t/p) = (1-t)\cdot(1+t)\cdot(p + 33305t^1 + 1564t^2 - 14296t^3 - 11865t^4 + 5107t^5 + 27955t^6 + 25963t^7 + 27955t^8 + 5107t^9 - 11865t^{10} - 14296t^{11} + 1564t^{12} + 33305t^{13} + pt^{14}).$$

We know of no previous algorithm that can compute $\zeta_X(t)$ for p in this range!

Example: random dense K3 surface

$X \subset \mathbb{P}^3_{\mathbb{F}_p}$ given by

$$-9x^4 - 10x^3y - 9x^2y^2 + 2xy^3 - 7y^4 + 6x^3z + 9x^2yz - 2xy^2z + 3y^3z$$
$$+ 8x^2z^2 + 6y^2z^2 + 2xz^3 + 7yz^3 + 9z^4 + 8x^3w + x^2yw - 8xy^2w - 7y^3w$$
$$+ 9x^2zw - 9xyzw + 3y^2zw - xz^2w - 3yz^2w + z^3w - x^2w^2 - 4xyw^2$$
$$- 3xzw^2 + 8yzw^2 - 6z^2w^2 + 4xw^3 + 3yw^3 + 4zw^3 - 5w^4 = 0$$

For $p = 2^{15} - 19$, in `38m27s`, we obtain

$$\zeta_X(t) = ((1-t)(1-pt)(1-p^2t)Q(t))^{-1}$$

where

$$pQ(t/p) = (t+1)\big(p - 53159t^1 + 10023t^2 - 3204t^3 + 49736t^4 - 56338t^5$$
$$+ 43086t^6 - 48180t^7 + 44512t^8 - 42681t^9 + 47794t^{10}$$
$$- 42681t^{11} + 44512t^{12} - 48180t^{13} + 43086t^{14} - 56338t^{15}$$
$$+ 49736t^{16} - 3204t^{17} + 10023t^{18} - 53159t^{19} + pt^{20}\big)$$

Old implementation takes roughly the same time.

Example: a quintic threefold in the Dwork pencil

Consider the threefold X in $\mathbb{P}^4_{\mathbb{F}_p}$ for $p = 2^{20} - 3$ given by

$$x_0^5 + \cdots + x_4^5 + x_0 x_1 x_2 x_3 x_5 = 0.$$

In `11m18s`, we compute that

$$\zeta_X(t) = \frac{R_1(pt)^{20} R_2(pt)^{30} S(t)}{(1-t)(1-pt)(1-p^2 t)(1-p^3 t)}$$

where the "interesting" factor is

$$S(t) = 1 + 74132440T + 748796652370pT^2 + 74132440p^3T^3 + p^6T^4.$$

and R_1 and R_2 are the numerators of the zeta functions of certain curves (given by a formula of Candelas–de la Ossa–Rodriguez Villegas).

Using the old projective code, we extrapolate it would have taken us at least 120 days.

Example: a Calabi–Yau 3fold in a non weighted projective space

Let X be the closure (in $\mathbb{P}_\Delta$) of the affine threefold

$$xyz^2w^3 + x + y + z - 1 + y^{-1}z^{-1} + x^{-2}y^{-1}z^{-2}w^{-3} = 0.$$

For $p = 2^{20} - 3$, in `1h15m`, we computed the "interesting" factor of $\zeta_X(t)$

$$(1+718pt+p^3t^2)(1+1188466826t+1915150034310pt^2+1188466826p^3t^3+p^6t^4).$$

Example: a Calabi–Yau 3fold in a non weighted projective space

Let X be the closure (in $\mathbb{P}_\Delta$) of the affine threefold

$$xyz^2w^3 + x + y + z - 1 + y^{-1}z^{-1} + x^{-2}y^{-1}z^{-2}w^{-3} = 0.$$

For $p = 2^{20} - 3$, in `1h15m`, we computed the "interesting" factor of $\zeta_X(t)$

$$(1+718pt+p^3t^2)(1+1188466826t+1915150034310pt^2+1188466826p^3t^3+p^6t^4).$$

By analogy with the Reid's list, Calabi–Yau threefolds can arise as hypersurfaces in:

- 7555 weighted projective spaces;
- 473,800,776 toric varieties.

See `http://hep.itp.tuwien.ac.at/~kreuzer/CY/`.

Example: a dense Cubic fourfold

$$\begin{aligned} x_0^2x_1 + x_0x_1^2 + x_1^2x_2 + x_0x_2^2 + 4x_0^2x_3 + x_1^2x_3 \\ + 8x_0x_2x_3 + 2x_1x_2x_3 + 2x_2^2x_3 + 4x_0x_3^2 + x_1x_3^2 + x_3^3 + 8x_0x_1x_4 \\ + x_1^2x_4 + 4x_1x_2x_4 + x_2^2x_4 + 8x_0x_3x_4 + 2x_2x_3x_4 + 8x_0x_4^2 \\ + x_1x_4^2 + 2x_3x_4^2 + x_4^3 + 2x_0^2x_5 + x_1^2x_5 + x_1x_2x_5 + x_2^2x_5 \\ + 8x_0x_3x_5 + x_1x_3x_5 + x_3^2x_5 + 4x_0x_4x_5 + 3x_3x_4x_5 + 2x_0x_5^2 + x_4x_5^2. \end{aligned}$$

For $p = 23$, in `22h52m`, we computed $\zeta_X(t)$ using a a **fully dense** nondegenerate model, obtained by random change of variables in $\mathbb{P}^5$. And we concluded that $\rho(X) = 3$ (one extra class over $\mathbb{F}_p$ and another one over $\mathbb{F}_{p^2}$).

Example: a dense Cubic fourfold

$$\begin{aligned} x_0^2x_1 + x_0x_1^2 + x_1^2x_2 + x_0x_2^2 + 4x_0^2x_3 + x_1^2x_3 \\ + 8x_0x_2x_3 + 2x_1x_2x_3 + 2x_2^2x_3 + 4x_0x_3^2 + x_1x_3^2 + x_3^3 + 8x_0x_1x_4 \\ + x_1^2x_4 + 4x_1x_2x_4 + x_2^2x_4 + 8x_0x_3x_4 + 2x_2x_3x_4 + 8x_0x_4^2 \\ + x_1x_4^2 + 2x_3x_4^2 + x_4^3 + 2x_0^2x_5 + x_1^2x_5 + x_1x_2x_5 + x_2^2x_5 \\ + 8x_0x_3x_5 + x_1x_3x_5 + x_3^2x_5 + 4x_0x_4x_5 + 3x_3x_4x_5 + 2x_0x_5^2 + x_4x_5^2. \end{aligned}$$

For $p = 23$, in `22h52m`, we computed $\zeta_X(t)$ using a a **fully dense** nondegenerate model, obtained by random change of variables in $\mathbb{P}^5$. And we concluded that $\rho(X) = 3$ (one extra class over $\mathbb{F}_p$ and another one over $\mathbb{F}_{p^2}$).

For $p = 113$ the running time was `26h34m` and for $p = 499$ it was `33h47m`.

Most of the time is spent setting up and solving the initial linear algebra problems.

Other possible versions

- **Space-time tradeoff**
  We can reduce the time dependence on p to

$$p^{0.5+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

Other possible versions

- **Space-time tradeoff**
  We can reduce the time dependence on p to

$$p^{0.5+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

- **Average polynomial time**
  Given an hypersurface defined over $\mathbb{Q}$, we may compute the zeta functions of its reductions modulo various primes at once. The average time complexity for each prime p < N is

$$\log(N)^{4+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

Other possible versions

- **Space-time tradeoff**
  We can reduce the time dependence on p to

$$p^{0.5+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

- **Average polynomial time**
  Given an hypersurface defined over $\mathbb{Q}$, we may compute the zeta functions of its reductions modulo various primes at once. The average time complexity for each prime $p < N$ is

$$\log(N)^{4+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

These have not yet been implemented and we still need to write the paper...