Computing zeta functions of nondegenerate toric hypersurfaces

Edgar Costa (Dartmouth College)

December 4th, 2017

Presented at Boston University Number Theory Seminar
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 $\mathbb{Q}$

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

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

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 $\mathbb{Q}$

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

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

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

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

$\zeta(s)$ 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, we are often interested in $\#X(\mathbb{F}_q)$

Real life applications

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

Real life applications

- Cryptography/Coding Theory, we are often interested in $\#X(\mathbb{F}_q)$
- Isomorphism/Isogeny testing
- Determining endomorphisms of an abelian variety

Real life applications

- Cryptography/Coding Theory, we are often interested in $\#X(\mathbb{F}_q)$
- Isomorphism/Isogeny testing
- Determining endomorphisms of an abelian variety
- rank of the Picard lattice (and the order of the Brauer group)

Real life applications

- Cryptography/Coding Theory, we are often interested in $\#X(\mathbb{F}_q)$
- Isomorphism/Isogeny testing
- Determining endomorphisms of an abelian variety
- rank of the Picard lattice (and the order of the Brauer group)
- Computing L-functions and their special values, e.g.:
  - Birch–Swinnerton-Dyer
  - searching for Langlands correspondences

Real life applications

- Cryptography/Coding Theory, we are often interested in $\#X(\mathbb{F}_q)$
- Isomorphism/Isogeny testing
- Determining endomorphisms of an abelian variety
- rank of the Picard lattice (and the order of the Brauer group)
- Computing L-functions and their special values, e.g.:
  - Birch–Swinnerton-Dyer
  - 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

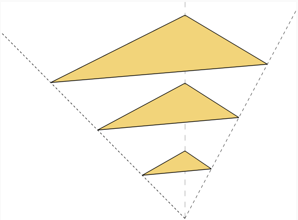
  $$P_d := \text{homogeneous polynomials in } n+1 \text{ variables of degree } d$$

  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 $\mathbb{T}^n := \operatorname{Spec}(R[x_1^{\pm}, \ldots, x_n^{\pm}])$
- $\Delta :=$ 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.

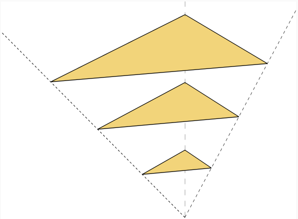
Toric hypersurfaces

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

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

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

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



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

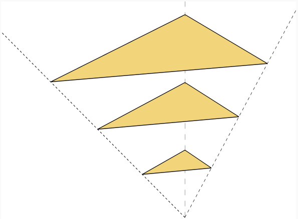
Toric hypersurfaces

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

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

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

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



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

Examples

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

Toric hypersurfaces are everywhere

Some familiar examples:

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

Some familiar examples:

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

Some familiar examples:

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

Some familiar examples:

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

Some familiar examples:

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

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

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

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?

Given

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

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, 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

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

Goal

Compute

$$\begin{aligned}
\zeta_X(t) &:= exp\left(\sum_{i \geq 1} \#X(\mathbb{F}_{q^i}) t^i / i\right) \in \mathbb{Q}(t) \\
&= \prod_i \det\left(1 - t \operatorname{Frob} | H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}} \\
&= Q(t)^{(-1)^n} \prod_{i=0}^{n-1} \left(\frac{1}{1 - q^i t}\right)^{b_i},
\end{aligned}$$

where $Q(t) \in 1 + \mathbb{Z}[t]$ and the b_i are determined by Δ.

How can we do this?

Naively computing $\#X(\mathbb{F}_{q^a})$ to deduce $Q(t)$ is not practical!

How can we do this?

Naively computing $\#X(\mathbb{F}_{q^a})$ to deduce $Q(t)$ is not practical!

In general, to recover $Q(t)$ we need $\#X(\mathbb{F}_{q^a})$ for $a = 1, \ldots, \lceil \deg Q/2 \rceil$.

Some data points:

- Elliptic curve, $Q(t) = 1 - a_p t + p t^2$
- Smooth plane curve, $Q(t) = 1 + a_{p,1} t + a_{p,2} t^2 + p a_{p,1} t^3 + p^2 t^4$
- K3 surface, $\deg Q \leq 21$
- Calabi-Yau 3fold, $\deg Q \leq 204$

How can we do this?

Naively computing $\#X(\mathbb{F}_{q^a})$ to deduce $Q(t)$ is not practical!

In general, to recover $Q(t)$ we need $\#X(\mathbb{F}_{q^a})$ for $a = 1, \ldots, \lceil \deg Q/2 \rceil$.

Some data points:

- Elliptic curve, $Q(t) = 1 - a_p t + pt^2$
- Smooth plane curve, $Q(t) = 1 + a_{p,1} t + a_{p,2} t^2 + p a_{p,1} t^3 + p^2 t^4$
- K3 surface, $\deg Q \leq 21$
- Calabi-Yau 3fold, $\deg Q \leq 204$

Can we rewrite $\#X(\mathbb{F}_q) = \{x \in \mathbb{F}_q : f(x) = 0\}$?

How can we do this?

Naively computing $\#X(\mathbb{F}_{q^a})$ to deduce $Q(t)$ is not practical!

In general, to recover $Q(t)$ we need $\#X(\mathbb{F}_{q^a})$ for $a = 1, \ldots, \lceil \deg Q/2 \rceil$.

Some data points:

- Elliptic curve, $Q(t) = 1 - a_p t + pt^2$
- Smooth plane curve, $Q(t) = 1 + a_{p,1}t + a_{p,2}t^2 + pa_{p,1}t^3 + p^2t^4$
- K3 surface, $\deg Q \leq 21$
- Calabi-Yau 3fold, $\deg Q \leq 204$

Can we rewrite $\#X(\mathbb{F}_q) = \{x \in \mathbb{F}_q : f(x) = 0\}$?

$$\cdots = \{x \in X\left(\overline{\mathbb{F}_q}\right) : \mathrm{Frob}_{\mathbb{F}_q}(x) = x\}$$

Lefschetz fixed point theorem

Given

- Z be a nice space;
- H^* be a nice cohomology theory;
- $F : X \to X$ be a nice map.
- $L(F^n) = \#\{x \in X : F^n(x) = x\}$

we have

$$exp\left(\sum_{n=1}^{\infty} L(F^n)t^n/n\right) = \prod_i \det(1 - tF^*|H^i(X))^{(-1)^{i+1}}$$

Lefschetz fixed point theorem

Given

- Z be a nice space;
- H^* be a nice cohomology theory;
- $F : X \to X$ be a nice map.
- $L(F^n) = \#\{x \in X : F^n(x) = x\}$

we have

$$exp\left(\sum_{n=1}^{\infty} L(F^n)t^n/n\right) = \prod_i \det(1 - tF^*|H^i(X))^{(-1)^{i+1}}$$

Applying this to the Frobenius endomorphism, we get

$$\zeta_{X_{\mathbb{F}_q}}(t) = \prod_i \det(1 - t\,\mathrm{Frob}\,|H^i(X_{\overline{\mathbb{F}_q}}))^{(-1)^{i+1}}$$

Lefschetz fixed point theorem

Given

- Z be a nice space;
- H^* be a nice cohomology theory;
- $F : X \to X$ be a nice map.
- $L(F^n) = \#\{x \in X : F^n(x) = x\}$

we have

$$exp\left(\sum_{n=1}^{\infty} L(F^n) t^n/n\right) = \prod_i \det(1 - tF^* | H^i(X))^{(-1)^{i+1}}$$

Applying this to the Frobenius endomorphism, we get

$$\zeta_{X_{\mathbb{F}_q}}(t) = \prod_i \det(1 - t\,\mathrm{Frob}\,|H^i(X_{\overline{\mathbb{F}_q}}))^{(-1)^{i+1}}$$

$$= \det(1 - q^{-1}t\,\mathrm{Frob}\,|H^n(U_{\overline{\mathbb{F}_q}}))^{(-1)^n} \prod_{i=0}^{n-1}\left(\frac{1}{1-q^i t}\right)^{b_i},$$

where $U := \mathbb{P}_\Delta \backslash X$

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
- $U := \mathbb{P}_\Delta \backslash X$ the complement of X
- σ := p-th power Frobenius

Goal

Compute the matrix representing the action of σ in $H^n(U)$ with enough of p-adic precision to deduce

$$Q(t) := \det(1 - q^{-1} t \operatorname{Frob} | H^n(U)) \in 1 + \mathbb{Z}[t].$$

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
- $U := \mathbb{P}_\Delta \backslash X$ the complement of X
- σ := p-th power Frobenius

Goal

Compute the matrix representing the action of σ in $H^n(U)$ with enough of p-adic precision to deduce

$$Q(t) := \det(1 - q^{-1} t \operatorname{Frob} | H^n(U)) \in 1 + \mathbb{Z}[t].$$

We will work with $H^n = H^{\dagger, n}$, the Monsky–Washnitzer cohomology.

Overall picture

Goal

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

Overall picture

Goal

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

$$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U) \circlearrowright \sigma$$

Overall picture

Goal

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

$$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p}) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U) \circlearrowright \sigma$$

$$\Big\downarrow$$

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

Overall picture

Goal

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

$$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p}) \xrightarrow[\text{id}]{\sim} H^{\dagger,n}(U) \circlearrowright \sigma$$

$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p}) \dashrightarrow$ explicit description over $\mathbb{C}$ [Dwork–Griffiths, Batyrev–Cox]

$H^{\dagger,n}(U) \dashrightarrow$ de Rham cohomology with overconvergent power series

Overall picture

Goal

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

$$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p}) \xrightarrow[\text{id}]{\sim} H^{\dagger,n}(U) \circlearrowright \sigma$$

$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p})$ ⇢ explicit description over $\mathbb{C}$ [Dwork–Griffiths, Batyrev–Cox]

$H^{\dagger,n}(U)$ ⇢ de Rham cohomology with overconvergent power series

cohomology relations + commutative algebra $\Longrightarrow$ basis for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q}) = \left\{x^\beta \omega / f^i\right\}_\beta$ + reduction algorithm

Generic algorithm – Abbott–Kedlaya–Roe type

$$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q}) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U) \circlearrowright \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m} \omega \right\}_\beta$ a monomial basis for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$ with $\omega := \frac{\mathrm{d}x_1}{x_1} \wedge \cdots \wedge \frac{\mathrm{d}x_n}{x_n} \in \Omega^n$
2. In $H^{\dagger,n}$ 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

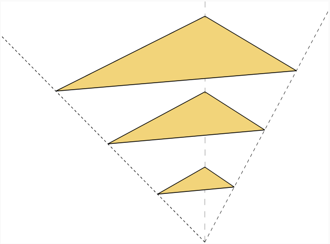
Note: Originally for smooth hypersurfaces in the projective space.

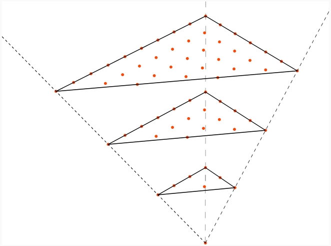
Schematically

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

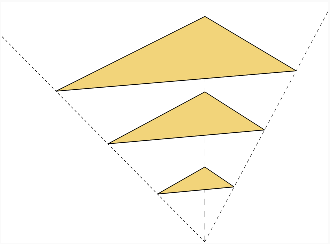
Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$
$(pdK)^{n+O(1)}$ terms		$(dK)^{n+O(1)}$ terms

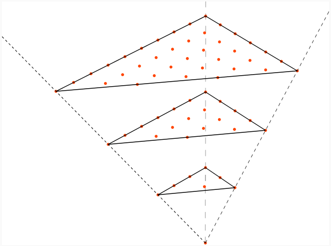




Schematically

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



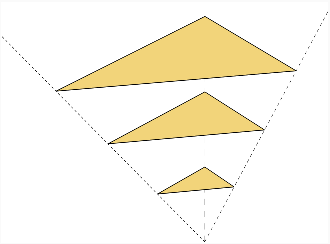


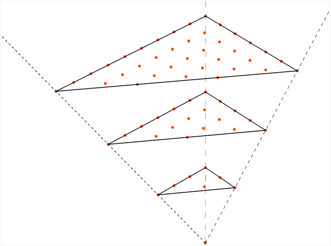
$$\rho : P_{\ell+1} \longmapsto P_\ell$$

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

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





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

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

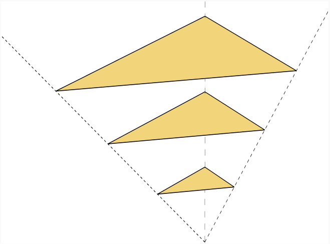
$\pi : P_n \longmapsto P_n$

$$\ell x^{\alpha+\beta} \frac{g\omega}{f^{\ell+1}} \equiv x^\beta \frac{\pi(g)\omega}{f^\ell}, \; x^\alpha \in P_1$$

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

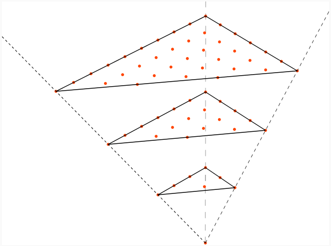


$$\rho : P_{\ell+1} \longmapsto P_\ell$$

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

“slice” $\mapsto$ “slice”

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



$$\pi : P_n \longmapsto P_n$$

$$\ell x^{\alpha+\beta} \frac{g\omega}{f^{\ell+1}} \equiv x^\beta \frac{\pi(g)\omega}{f^\ell}, \; x^\alpha \in P_1$$

“dot” $\mapsto$ “dot”

Generic algorithm – C.–Harvey–Kedlaya

$$H^n_{\mathrm{dR}}(U) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U_{\mathbb{F}_p}) \circlearrowright \sigma$$

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

$$H^n_{\mathrm{dR}}(U) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U_{\mathbb{F}_p}) \circlearrowright \sigma$$

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

$$H^n_{\mathrm{dR}}(U) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U_{\mathbb{F}_p}) \circlearrowright \sigma$$

1. Compute $\left\{ \frac{x^\beta}{f^m}\omega \right\}_\beta$ a monomial basis for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$
2. In $H^{\dagger,n}$ 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 (∼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: random dense K3 surface

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

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

For $p = 49999$, in `1h5m5s`, we obtain

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

where

$$\begin{aligned}
pQ(t/p) =&(1-t)(p + 63115t + 14796t^2 + 42361t^3 + 49443t^4 \\
&+ 11718t^5 + 42046t^6 + 51501t^7 + 20534t^8 + 27146t^9 \\
&+ 38370t^{10} + 27146t^{11} + 20534t^{12} + \cdots + pt^{20})
\end{aligned}$$

Example: a quartic surface in the Dwork pencil

Consider the surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ for $p = \texttt{4999999} = 5 \cdot 10^6 - 1$ given by

$$x_0^4 + x_1^4 + x_2^4 + x_3^4 + x_0 x_1 x_2 x_3 = 0.$$

Using the old projective code in `100h30m` we compute that

$$\zeta_X(t) = \frac{1}{(1-t)(1-pt)(1-p^2t)R_1(pt)^3 R_2(pt)^6 S(t)}$$

where the “interesting” factor

$$S(t) = (1+pt)(1+5301514t+p^2t^2).$$

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 surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ for $p = \texttt{4999999} = 5 \cdot 10^6 - 1$ given by

$$x_0^4 + x_1^4 + x_2^4 + x_3^4 + x_0x_1x_2x_3 = 0.$$

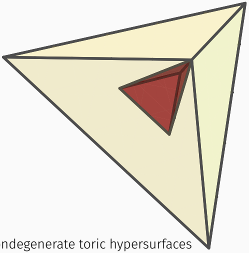
Using the toric ~~old projective~~ code in `6m32s` ~~`100h30m`~~ we compute

$$\zeta_X(t) = \frac{1}{(1-t)(1-pt)(1-p^2t)R_1(pt)^3R_2(pt)^6S(t)}$$

where the "interesting" factor

$$S(t) = (1+pt)(1+5301514t+p^2t^2).$$

The polytope
of X is much smaller than the full simplex
($32/3 \approx 10.6$ vs $2/3 \approx 0.6$), as the monomials
defining X generate a sublattice of index 4^2 in $\mathbb{Z}^3$.



Example: a quintic threefold in the Dwork pencil

Consider the threefold X in $\mathbb{P}^4_{\mathbb{F}_p}$ for $p = 1000003$ given by

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

In 667s, 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, it would have taken around 37h.

Example: another family of K3 surfaces

Consider now the surface X in the weighted projective space $\mathbb{P}(8,5,4,3)_{\mathbb{F}_p}$ given by taking the closure of the affine surface

$$yz^5 + xz^4 + y^4 + z^4 + x^2 + 1 = 0.$$

For $p = 49999$, in **120s** we compute that

$$\zeta_X(t) = \frac{1}{(1-t)(1-pt)(1-p^2t)R(pt)S(t)}$$

where

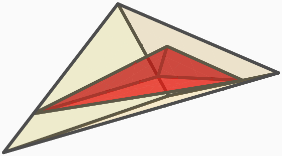
$$pS(p^{-1}t) = p - 14662t - 31559t^2 - 5620t^3 - 31559t^4 - 14662t^5 + pt^6.$$

This example is from Miles Reid's list of 95 families of nondegenerate toric surfaces which are K3 surfaces.

There is no other method that can handle dense surfaces in $\mathbb{P}(8,5,4,3)$ in this p range.

Consider the appropriate completion of the toric surface over $\mathbb{F}_p$ with $p = 49999$ given by

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



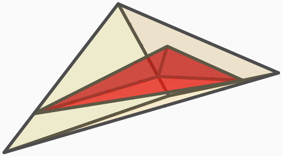
In 61s, we compute that the "interesting" factor of $\zeta_X(t)$ is

$$1 - 9786t - 42243pt^2 + 35036p^2t^3 - 42243p^3t^4 - 9786p^4t^5 + p^6t^6.$$

In $\mathbb{P}^3$ this surface is degenerate, and would have taken us one hour 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 $p = 49999$ given by



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

In 61s, we compute that the "interesting" factor of $\zeta_X(t)$ is

$$1 - 9786t - 42243pt^2 + 35036p^2t^3 - 42243p^3t^4 - 9786p^4t^5 + p^6t^6.$$

In $\mathbb{P}^3$ this surface is degenerate, and would have taken us one hour 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, 49999: Degree:=1);
1 - 9786*$.1 + O($.1^2)
```

Example: another Calabi–Yau threefold

Let X be the closure in the weighted projective space $\mathbb{P}(10, 11, 16, 19, 21)_{\mathbb{F}_p}$ for $p = 49999$ of the affine threefold

$$y^7 + x^2zw + zyzw + y^2zw + z^3w + w^3 + xz + yz = 0.$$

In 401s, we we compute that the "interesting" factor of ζ_X is

$$1 + 6423186t + 2211095838pt^2 - 127485903944p^2t^3$$
$$+2211095838p^4t^4 + 6423186p^6T^5 + p^9T^6$$

By analogy with the Reid list, one can classify Calabi–Yau threefolds arising as hypersurfaces in weighted projective spaces; there are 7555 such families. See `http://hep.itp.tuwien.ac.at/~kreuzer/CY/`.

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...