Computing zeta functions of nondegenerate toric hypersurfaces

Edgar Costa (Dartmouth College)

October 14th, 2017

Presented at 2017 Maine/Québec Number Theory Conference
Joint work with David Harvey (UNSW) and Kiran Kedlaya (UCSD)

Slides available at `edgarcosta.org` under Research

The zeta function problem

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

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

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

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

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

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

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

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
- Arithmetic statistics
  - Sato–Tate
  - Lang–Trotter
  - searching for Langlands correspondences

Approaches

- ℓ-adic approaches, by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.

Approaches

- ℓ-adic approaches, by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.
  - We need to have an effective *description* of the cohomology.

Approaches

- ℓ-adic approaches, by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.
  - We need to have an effective *description* of the cohomology.
- Very generic algorithms derived from Dwork's p-adic analytic proof that $\zeta_X(t) \in \mathbb{Q}(t)$

Approaches

- ℓ-adic approaches, by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.
  - We need to have an effective *description* of the cohomology.
- Very generic algorithms derived from Dwork's p-adic analytic proof that $\zeta_X(t) \in \mathbb{Q}(t)$
- p-adic methods 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

Nondegenerate toric hypersurfaces

p-adic Cohomology

Some examples

Nondegenerate toric hypersurfaces

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

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
- $\Delta :=$ Newton polytope of f = convex hull in $\mathbb{R}^n$ of the support of f
- To Δ we can associate to it a graded ring (and a projective variety).

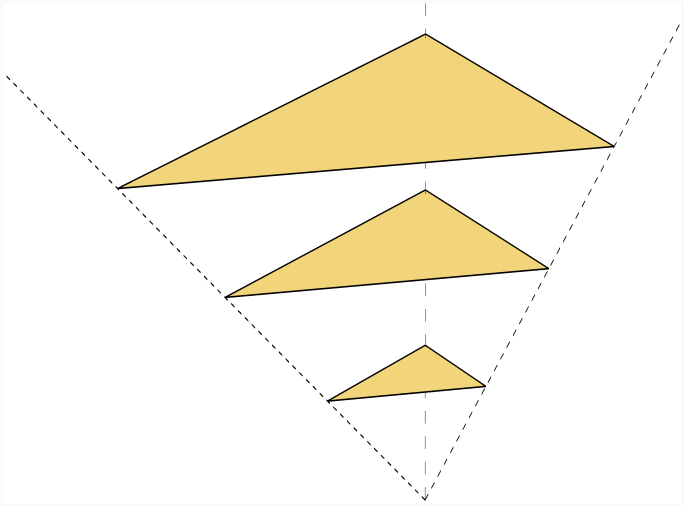
Toric hypersurfaces

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

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

$$X_\Delta := \operatorname{Proj} P_\Delta$$

and $V(f)$ is an hypersurface in the toric variety X_Δ.



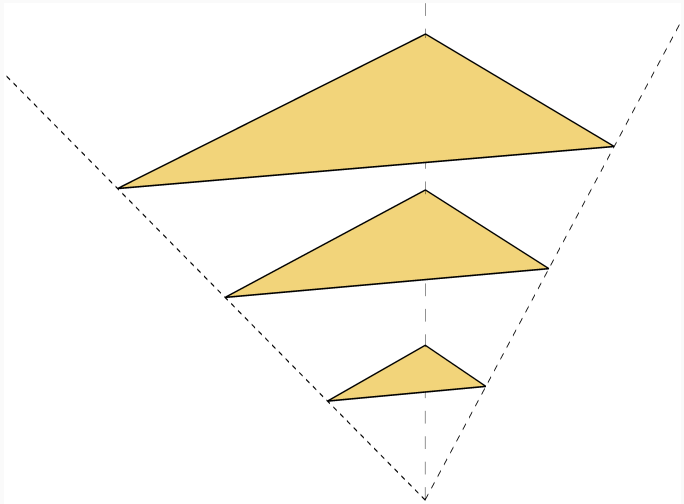
Toric hypersurfaces

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

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

$$X_\Delta := \operatorname{Proj} P_\Delta$$

and $V(f)$ is an hypersurface in the toric variety X_Δ.



Examples

Δ	X_Δ
$\operatorname{Conv}(0, e_1, \ldots, e_n)$	$\mathbb{P}^n$
$\operatorname{Conv}(0, e_1, \ell e_2, \ldots, \ell e_n)$	$\mathbb{P}^n(\ell, 1, \ldots, 1)$
$\operatorname{Conv}(0, e_1, e_2, e_1 + e_2)$	$\mathbb{P}^1 \times \mathbb{P}^1$

Nondegenerate toric hypersurfaces

Geometric definition

The hypersurface defined by f is nondegenerate if for every face $\sigma \subset \Delta$ (including Δ itself) 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.

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
$0, 5e_1, \ldots, 5e_5$	Quintic Calabi-Yau threefold

There are 4319 reflexive polyhedra that give rise to K3 surfaces as toric hypersurfaces.

p-adic Cohomology

Goal

Setup

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^{\pm}, \ldots, x_n^{\pm}]$ a Laurent polynomial
- $Z := V(f) = \{x \in X_\Delta : f(x) = 0\}$ a nondegenerate hypersurface

Goal

Compute

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

where $Q(t) = \det\left(1 - q^{-1} t \,\mathrm{Frob} \,|H^n_{\mathrm{et}}(\overline{X_\Delta \backslash Z}, \mathbb{Q}_\ell)\right) \in 1 + \mathbb{Z}[t]$.

Goal

Setup

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^{\pm}, \ldots, x_n^{\pm}]$ a Laurent polynomial
- $Z := V(f) = \{x \in X_\Delta : f(x) = 0\}$ a nondegenerate hypersurface

Goal

Compute

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

where $Q(t) = \det\left(1 - q^{-1} t \,\mathrm{Frob} \,|H^{\dagger,n}(X_\Delta \backslash Z)\right) \in 1 + \mathbb{Z}[t]$.

Master plan

Setup

- $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in \mathbb{F}_q[x_1^{\pm}, \ldots, x_n^{\pm}]$ a Laurent polynomial
- $Z := V(f) = \{x \in X_\Delta : f(x) = 0\}$ a nondegenerate hypersurface
- $U := X_\Delta \backslash Z$
- $\sigma :=$ p-th power Frobenius

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.

Overall picture

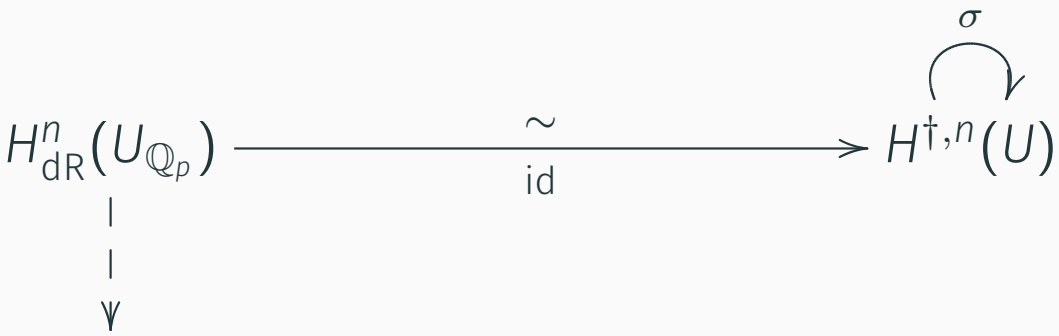
Goal

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

Overall picture

Goal

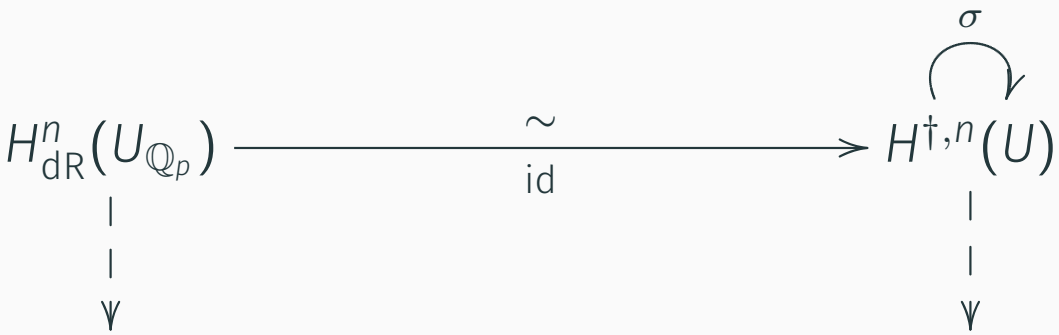
Compute the matrix representing the action of σ in $H^{\dagger,n}(U)$ with enough p-adic precision.



Overall picture

Goal

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



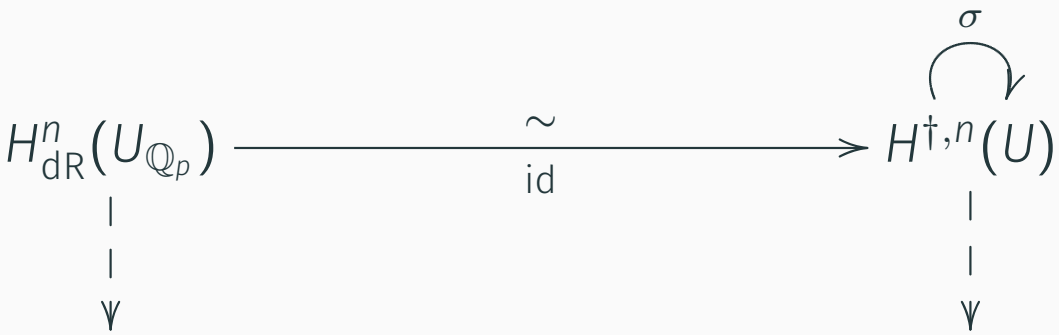
explicit description over $\mathbb{C}$
[Dwork–Griffiths, Batyrev–Cox]

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.



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

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

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

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

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

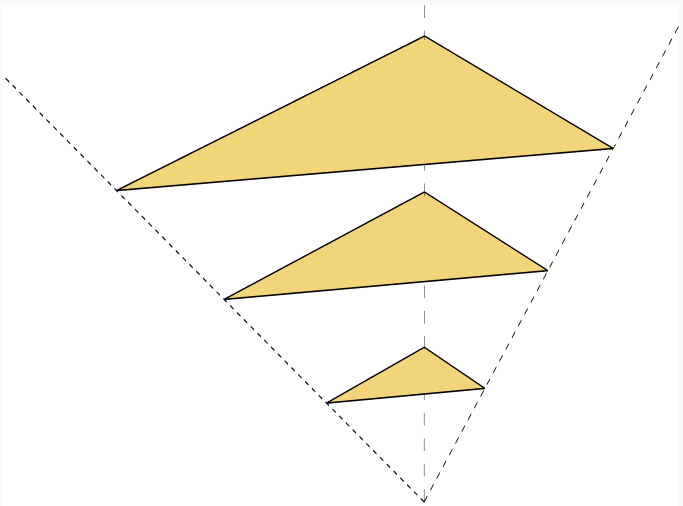
3. Write the approximation in terms of basis elements, i.e., apply the de Rham relations

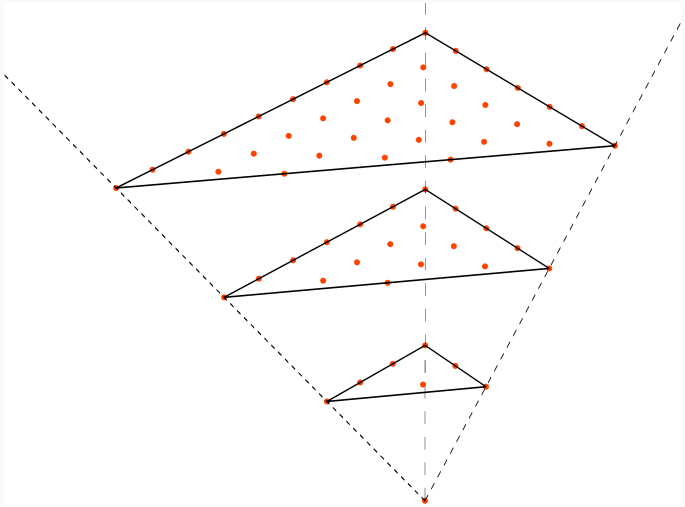
Schematically

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

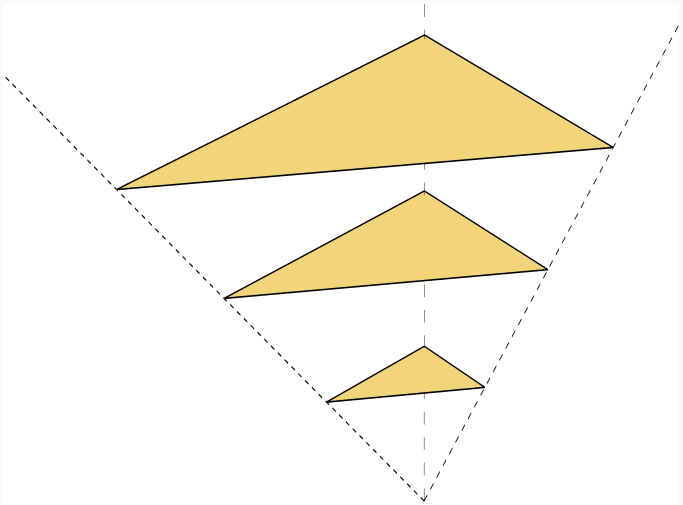
Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$
$(pdK)^{n+O(1)}$ terms		$(dK)^{n+O(1)}$ terms

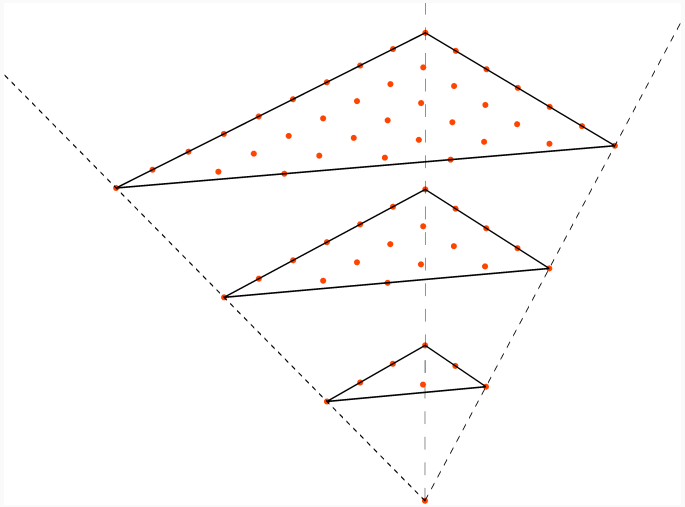




Schematically

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



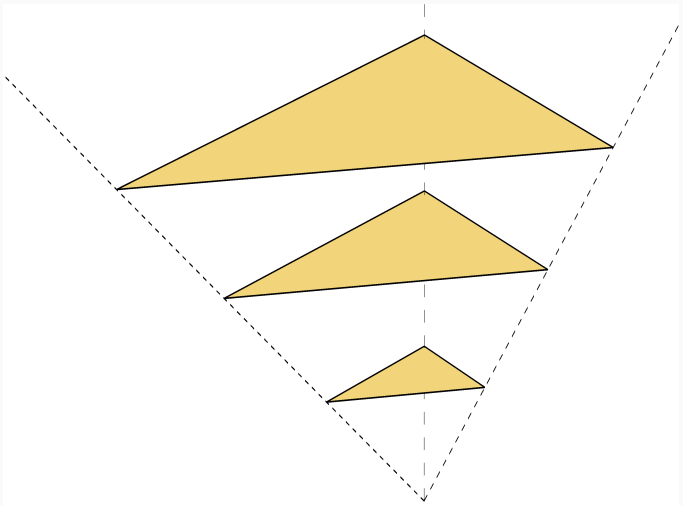


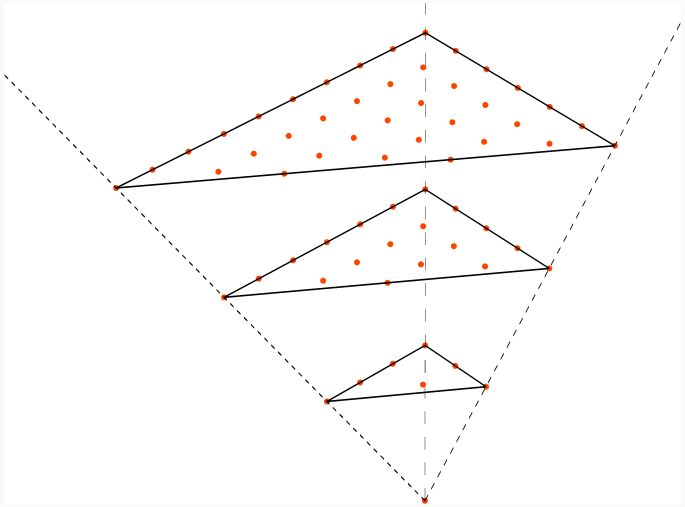
$$\rho : P_{\ell+1} \longmapsto P_\ell$$

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

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



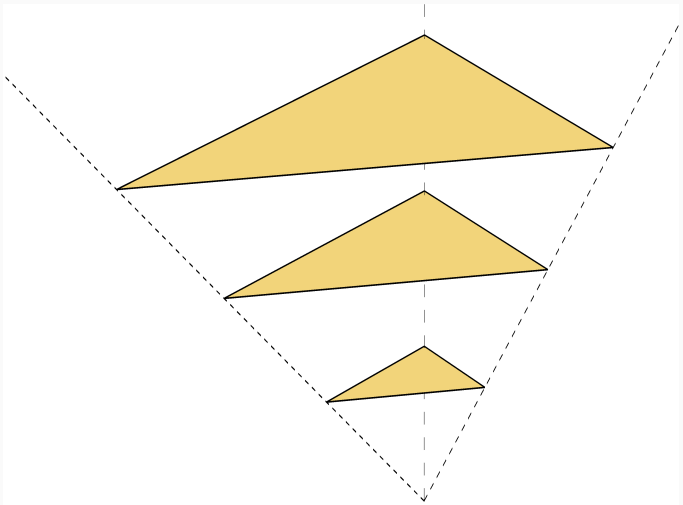


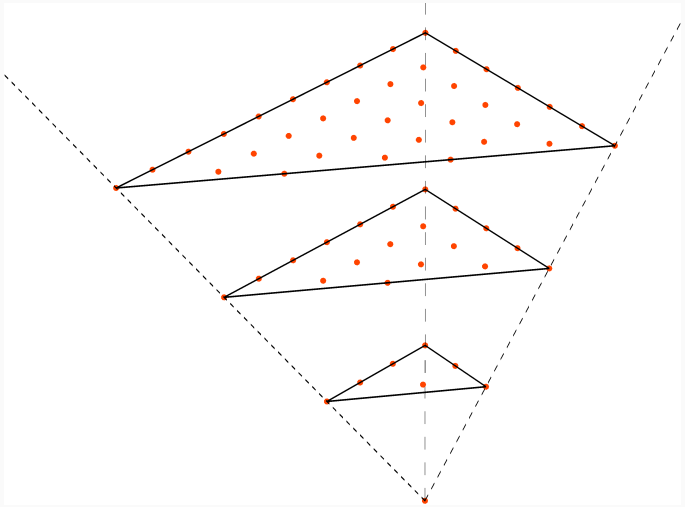
$$\rho : P_{\ell+1} \longmapsto P_\ell \qquad \pi : P_n \longmapsto P_n$$

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

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





$\rho : P_{\ell+1} \longmapsto P_\ell$		$\pi : P_n \longmapsto P_n$
$\ell \frac{g\omega}{f^{\ell+1}} \equiv \frac{\rho(g)\omega}{f^\ell}$		$\ell x^{\alpha+\beta} \frac{g\omega}{f^{\ell+1}} \equiv x^\beta \frac{\pi(g)\omega}{f^\ell}, \; x^\alpha \in P_1$
"slice" $\mapsto$ "slice"		"dot" $\mapsto$ "dot"

Generic algorithm – C.–Harvey–Kedlaya

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

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

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

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 convolved 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

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

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 convolved 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

$X \subset \mathbb{P}^3_{\mathbb{F}_p}$ for $p = 49999$ given by

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

In 1h5m5s, we obtain

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

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 $p = 4999999 = 5 \cdot 10^6 - 1$ given by

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

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

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

where the "interesting" factor

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

The 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 $p = 4999999 = 5 \cdot 10^6 - 1$ given by

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

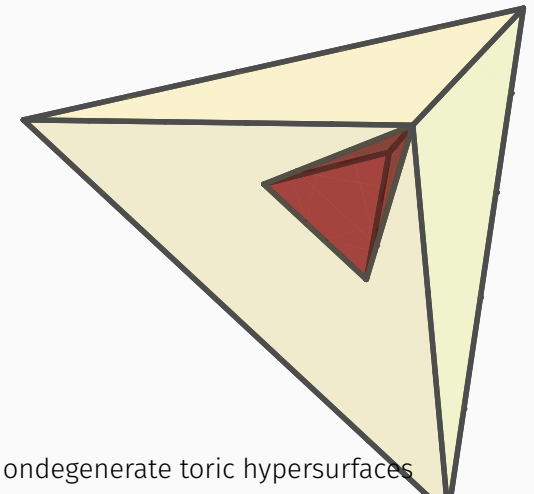
Using the toric ~~old projective~~ code in `6m32s` ~~`100h30m`~~ we compute

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

where the "interesting" factor

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

The polytope of X is much smaller than the full symplex $32/3$ `vs` $2/3$, as the 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

$$x_0^5 + \cdots + x_4^5 + x_0x_1x_2x_3x_5 = 0.$$

In **667s**, we compute that

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

where the "interesting" factor

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

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, would have taken us at around **37h**.

Example: another family of K3 surfaces

Consider now the surface X in the weighted projective space $\mathbb{P}(8,5,4,3)_{\mathbb{F}_p}$ for $p = 49999$ given by taking the closure of the affine surface

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

In 120s, we compute that

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

where

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

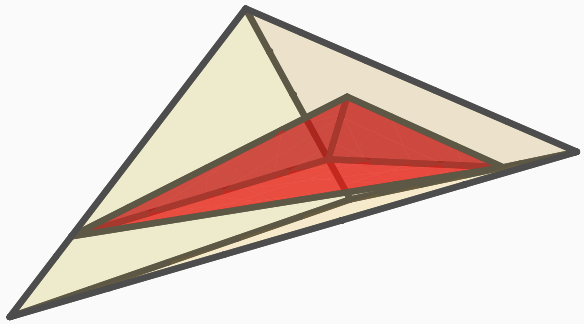
This example is from Miles Reid's list of 95 families of nondegenerate toric surfaces which are K3 surfaces.

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

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

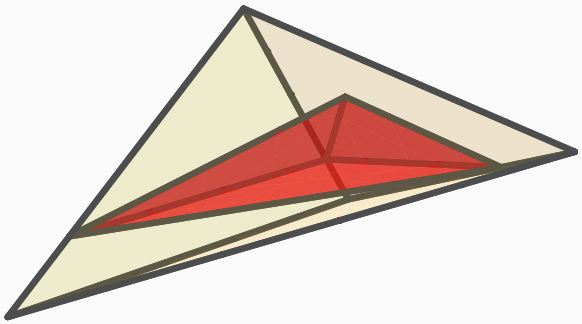
$$1 - 9786t - 42243pt^2 + 35036p^2t^3 - 42243p^3t^4 - 9786p^4t^5 + p^6t^6.$$

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

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

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

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.