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 \( \zeta(s) \) \( \sim \) 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

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

Example: $X = fg$, a point, then $fg(s) = (s)$.

What arithmetic properties of $X$ can we read from $X_p(s)$?

$X_p(t)$ obeys a functional equation and satisfies the Riemann hypothesis!

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

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

If $X_p := X \mod p$ 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 and Weil generalized an analog of $\zeta(s)$ for algebraic varieties

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

If $X_p := X \mod p$ 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 and Weil generalized an analog of $\zeta(s)$ for algebraic varieties

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

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

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

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 $\mathbb{Q}$

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

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

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

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

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

$$\zeta_E(s) = \prod_p \frac{L_p(p^{-s})}{(1 - p^{-s})(1 - p^{-s+1})} = \frac{\zeta(s)\zeta(s - 1)}{L_E(s)}$$
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 $E_p \rightsquigarrow E.$
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 $\text{ord}_{s=1} L_E(s) = \text{rk}(E)$. 
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 ✓
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?
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 $X$
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

$$
\zeta_{X_p}(t) := \exp \left( \sum_{i \geq 0} \# X_p(\mathbb{F}_{p^i}) \frac{t^i}{i} \right) \in \mathbb{Q}(t)
$$
Let $X$ be a smooth variety over a finite field $\mathbb{F}_q$ of characteristic $p$, consider

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

**Problem**

Compute $\zeta_X$ from an *explicit* description of $X$. 
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 $\zeta_X$ from an *explicit* description of $X$.

Theoretically this is “trivial”. The degree of $\zeta_X$ is bounded by the geometry of $X$, and we can then enumerate $X(\mathbb{F}_{q^i})$ for enough $i$ to pinpoint $\zeta_X$. 
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 $\zeta_X$ from an *explicit* description of $X$.

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

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
- Computing $\text{End}(A)$ for $A$ an abelian variety.
  $\Rightarrow$ A couple of $A_p(t)$ usually give away the shape of $\text{End}(A)$
- Computing Picard number of a K3 surface $\Rightarrow$ 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 $\Rightarrow \text{rk}(A)$
  - searching for Langlands correspondences
- Arithmetic statistics
- Sato–Tate
- Lang–Trotter
“Real life” applications

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

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

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing Isomorphism/Isogeny
- Computing $\text{End}(A)$ for $A$ an abelian variety.
  $\leadsto$ A couple of $\zeta_{A_p}(t)$ usually give away the shape of $\text{End}(A)$.
- Computing Picard number of a K3 surface
  $\leadsto$ 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 $\text{End}(A)$ for $A$ an abelian variety.
  $\leadsto$ A couple of $\zeta_{A_p}(t)$ usually give away the shape of $\text{End}(A)$.
• Computing Picard number of a K3 surface
  $\leadsto$ 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 $\leadsto \text{rk}(A)$
  • searching for Langlands correspondences
"Real life" applications

- Cryptography/Coding Theory, often interested in \( \#X(\mathbb{F}_q) \)
- Testing Isomorphism/Isogeny
- Computing \( \text{End}(A) \) for \( A \) an abelian variety.
  \( \rightsquigarrow \) A couple of \( \zeta_{A_p}(t) \) usually give away the shape of \( \text{End}(A) \).
- 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 \( \rightsquigarrow \text{rk}(A) \)
  - 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 $\zeta_X(t) \in \mathbb{Q}(t)$
- $\ell$-adic: by computing the action of Frobenius on mod-$\ell$ étale cohomology for many $\ell$.
Common Approaches

• Very generic algorithms derived from Dwork’s p-adic analytic proof that \( \zeta_X(t) \in \mathbb{Q}(t) \)
• \( \ell \)-adic: by computing the action of Frobenius on mod-\( \ell \) étale cohomology for many \( \ell \).
  • We need to have an effective \textit{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 $\zeta_X(t) \in \mathbb{Q}(t)$
- $\ell$-adic: by computing the action of Frobenius on mod-$\ell$ étale cohomology for many $\ell$.
  - 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 $\mathbb{P}^n$

For example, let $\mathbb{P}^d := \text{homogeneous polynomials in } n + 1 \text{ variables of degree } d$ and consider the graded ring $\mathbb{P}^d := \bigoplus_{d=0}^{\infty} \mathbb{P}^d$.

Then we have $\mathbb{P}^n := \text{Proj} \mathbb{P}^d$.

We can think of $\mathbb{P}^d := \mathbb{R}[\Delta_{\mathbb{Z}^n}]$, where $\Delta$ is the standard simplex.

Idea: generalize $\Delta$ to be any polytope.
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 $\mathbb{P}^n := \text{Proj } P$
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 $\mathbb{P}^n := \text{Proj } P$

• We can think of $P_d := R[d\Delta \cap \mathbb{Z}^n]$, where $\Delta$ is the standard simplex.
• Idea: generalize $\Delta$ to be any polytope.
• $f = \sum_{\alpha \in \mathbb{Z}^n} c_{\alpha} x^\alpha \in R[x_1^\pm, \ldots, x_n^\pm]$ a Laurent polynomial

• $f$ defines an hypersurface in the torus $\mathbb{T}^n := \text{Spec}(R[x_1^\pm, \ldots, x_n^\pm])$
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 \( \mathbb{T}^n := \text{Spec}(R[x_1^\pm, \ldots, x_n^\pm]) \)

• \( \Delta := \) 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 \( \mathbb{T}^n := \text{Spec}(R[x_1^\pm, \ldots, x_n^\pm]) \)
- \( \Delta := \text{Newton polytope of } f = \text{convex hull of the support of } f \) in \( \mathbb{R}^n \)
- To \( \Delta \) 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 \( \mathbb{T}^n := \text{Spec}(R[x_1^\pm, \ldots, x_n^\pm]) \)
- \( \Delta := \text{Newton polytope of } f = \text{convex hull of the support of } f \text{ in } \mathbb{R}^n \)
- To \( \Delta \) we can associate a graded ring and a projective variety.

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

\[
\mathbb{P}_\Delta := \text{Proj } P_\Delta
\]

\[
X_f := \text{Proj } P_\Delta/(f) \subset \mathbb{P}_\Delta
\]

\( X_f \) 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 $\mathbb{T}^n := \text{Spec}(R[x_1^\pm, \ldots, x_n^\pm])$
- $\Delta :=$ Newton polytope of $f = \text{convex hull of the support of } f$ in $\mathbb{R}^n$
- To $\Delta$ we can associate a graded ring and a projective variety.

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

\[
\mathbb{P}_\Delta := \text{Proj } P_\Delta
\]

\[
X_f := \text{Proj } P_\Delta/(f) \subset \mathbb{P}_\Delta
\]

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

<table>
<thead>
<tr>
<th>$\Delta$</th>
<th>$X_\Delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Conv}(0, e_1, \ldots, e_n)$</td>
<td>$\mathbb{P}^n$</td>
</tr>
<tr>
<td>$\text{Conv}(0, e_1, \ell e_2, \ldots, \ell e_n)$</td>
<td>$\mathbb{P}^n(\ell, 1, \ldots, 1)$</td>
</tr>
<tr>
<td>$\text{Conv}(0, e_1, e_2, e_1 + e_2) = [0, 1]^2$</td>
<td>$\mathbb{P}^1 \times \mathbb{P}^1$</td>
</tr>
</tbody>
</table>
Toric hypersurfaces are everywhere

<table>
<thead>
<tr>
<th>Vertices of $\Delta$</th>
<th>Resulting hypersurface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, $de_1, de_2$</td>
<td>Smooth plane curve of genus $\binom{d-1}{2}$</td>
</tr>
<tr>
<td>0, $(2g + 1)e_1, 2e_2$</td>
<td>Odd hyperelliptic curve of genus $g$</td>
</tr>
<tr>
<td>0, $ae_1, be_2$</td>
<td>$C_{a,b}$-curve</td>
</tr>
<tr>
<td>0, $4e_1, 4e_2, 4e_3$</td>
<td>Quartic K3 surface</td>
</tr>
<tr>
<td>0, $2e_1, 6e_2, 6e_3$</td>
<td>Degree 2 K3 surface</td>
</tr>
</tbody>
</table>
Toric hypersurfaces are everywhere

<table>
<thead>
<tr>
<th>Vertices of $\Delta$</th>
<th>Resulting hypersurface</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0, de_1, de_2$</td>
<td>Smooth plane curve of genus $\binom{d-1}{2}$</td>
</tr>
<tr>
<td>$0, (2g+1)e_1, 2e_2$</td>
<td>Odd hyperelliptic curve of genus $g$</td>
</tr>
<tr>
<td>$0, ae_1, be_2$</td>
<td>$C_{a,b}$-curve</td>
</tr>
<tr>
<td>$0, 4e_1, 4e_2, 4e_3$</td>
<td>Quartic K3 surface</td>
</tr>
<tr>
<td>$0, 2e_1, 6e_2, 6e_3$</td>
<td>Degree 2 K3 surface</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Vertices of $\Delta$</th>
<th>Resulting hypersurface</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0, de_1, de_2$</td>
<td>Smooth plane curve of genus $\binom{d-1}{2}$</td>
</tr>
<tr>
<td>$0, (2g+1)e_1, 2e_2$</td>
<td>Odd hyperelliptic curve of genus $g$</td>
</tr>
<tr>
<td>$0, ae_1, be_2$</td>
<td>$C_{a,b}$-curve</td>
</tr>
<tr>
<td>$0, 4e_1, 4e_2, 4e_3$</td>
<td>Quartic K3 surface</td>
</tr>
<tr>
<td>$0, 2e_1, 6e_2, 6e_3$</td>
<td>Degree 2 K3 surface</td>
</tr>
</tbody>
</table>

(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

<table>
<thead>
<tr>
<th>Vertices of $\Delta$</th>
<th>Resulting hypersurface</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0, de_1, de_2$</td>
<td>Smooth plane curve of genus $\binom{d-1}{2}$</td>
</tr>
<tr>
<td>$0, (2g + 1)e_1, 2e_2$</td>
<td>Odd hyperelliptic curve of genus $g$</td>
</tr>
<tr>
<td>$0, ae_1, be_2$</td>
<td>$C_{a,b}$-curve</td>
</tr>
<tr>
<td>$0, 4e_1, 4e_2, 4e_3$</td>
<td>Quartic K3 surface</td>
</tr>
<tr>
<td>$0, 2e_1, 6e_2, 6e_3$</td>
<td>Degree 2 K3 surface</td>
</tr>
</tbody>
</table>

(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

<table>
<thead>
<tr>
<th>Vertices of $\Delta$</th>
<th>Resulting hypersurface</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0, de_1, de_2$</td>
<td>Smooth plane curve of genus $\binom{d-1}{2}$</td>
</tr>
<tr>
<td>$0, (2g+1)e_1, 2e_2$</td>
<td>Odd hyperelliptic curve of genus $g$</td>
</tr>
<tr>
<td>$0, ae_1, be_2$</td>
<td>$C_{a,b}$-curve</td>
</tr>
<tr>
<td>$0, 4e_1, 4e_2, 4e_3$</td>
<td>Quartic K3 surface</td>
</tr>
<tr>
<td>$0, 2e_1, 6e_2, 6e_3$</td>
<td>Degree 2 K3 surface</td>
</tr>
</tbody>
</table>

(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.
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
\[ \zeta_X(t) := \exp \left( \sum_{i \geq 1} \#X(\mathbb{F}_q^i) \frac{t^i}{i} \right) \]
\[ = \prod_i \det(1 - t \text{Frob} \vert H_{et}^i(X_{\mathbb{F}_q^i}, \mathbb{Q}_\ell)) (-1)^{i+1} \in \mathbb{Q}(t), \]
where \( X := \text{Proj} P_\Delta/(f) \subset \mathbb{P}_\Delta \)
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

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

\[ = \prod_i \det(1 - t \text{Frob}_i | H^{i}_{\text{et}}(X_{\mathbb{F}_{q^i}}, \mathbb{Q}_\ell)) (-1)^{i+1} \in \mathbb{Q}(t), \]

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

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

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

\[ = \prod_i \det(1 - t \text{Frob} | H^i_{et}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)) (-1)^{i+1} \in \mathbb{Q}(t), \]

where \( X := \text{Proj} \mathbb{P}_\Delta/(f) \subset \mathbb{P}_\Delta \)

But under what assumptions on \( X \)? Is smoothness enough?

We will need a bit more, we will **nondegeneracy**.
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 $\sigma$ is nonsingular of codimension 1.
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 $\sigma$ 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 $\sigma$ 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, $\text{rad} \left( x \frac{\partial}{\partial x} f, y \frac{\partial}{\partial y} f, z \frac{\partial}{\partial z} f, f \right) = \langle x, y, z \rangle$.
$p$-adic Cohomology
Goal

Setup

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

Goal

Compute

\[
\zeta_X(t) := \exp \left( \sum_{i \geq 1} \frac{\#X(\mathbb{F}_q^i) t^i}{i} \right) = \prod_{i \geq 1} \det (1 - t \text{Frob} | H^i_{et}(\mathbb{X}_{\mathcal{F}_q}, \mathbb{Q}_\ell)) (-1)^{i+1} = Q(t)^{(1)^n} \zeta_{\mathbb{P}_\Delta}(t),
\]

where \( Q(t) := \det (1 - t \text{Frob} | PH^{n-1}_{et}(\mathbb{X}_{\mathcal{F}_q}, \mathbb{Q}_\ell)) \in 1 + \mathbb{Z}[t] \)
Setup

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

\[ X := \text{Proj} P_\Delta/(f) \subset \mathbb{P}_\Delta \text{ a nondegenerate hypersurface} \]

\[ \sigma := p\text{-th power Frobenius map} \]

Goal

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

\[ Q(t) = \det(1 - q^{-1}t \text{ Frob}|PH_{\text{rig}}^{n-1}(X)) \in 1 + \mathbb{Z}[t]. \]
### Setup

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

### Goal

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

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

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

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

Goal

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

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

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

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

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

$$PH^{n-1}_{dR}(X_{\mathbb{Q}_q}) \xrightarrow{\sim} id \Rightarrow PH^{\dagger,n-1}(X)$$
Goal

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

\[ PH^{n-1}_{dR}(X_{\mathbb{Q}_p}) \xrightarrow{\sim} \xrightarrow{id} PH^{\dagger,n-1}(X) \]

explicit description over $\mathbb{C}$

[Dwork–Griffiths, Batyrev–Cox]
Overall picture

Goal

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

$$PH^{n-1}_{dR}(X_{\mathbb{Q}_p}) \xrightarrow{\sim} id \xrightarrow{\sigma} PH^{1,n-1}(X)$$

- explicit description over $\mathbb{C}$
- dR cohomology with overconvergent power series

[Dwork–Griffiths, Batyrev–Cox]
Goal

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

$$PH^{n-1}_{dR}(X_{\mathbb{Q}_q}) \xrightarrow{\sim \text{id}} PH^{1,n-1}(X)$$

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

de Rham cohomology with overconvergent power series

cohomology relations

$$\implies$$

commutative algebra

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

reduction algorithm

Computing zeta functions of nondegenerate hypersurfaces in toric varieties
Generic algorithm – Abbott–Kedlaya–Roe type

\[ PH_{dR}^{n-1}(X_{\mathbb{Q}_q}) \xrightarrow{\sim} PH^{\dagger,n-1}(X) \]

1. Compute \( \left\{ \frac{x^\beta}{fm} \omega \right\}_\beta \) a monomial basis for \( PH_{dR}^{n-1}(X_{\mathbb{Q}_q}) \)

where \( \omega := \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n} \)
Generic algorithm – Abbott–Kedlaya–Roe type

\[ PH_{dR}^{n-1}(X_{Q_q}) \xrightarrow{\sim} PH^{\dagger,n-1}(X) \]

1. Compute \( \left\{ \frac{x^\beta}{f^m} \omega \right\} \) a monomial basis for \( PH_{dR}^{n-1}(X_{Q_q}) \)

where \( \omega := \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n} \)

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

\[ PH_{dR}^{n-1}(X_{\mathbb{Q}_q}) \xrightarrow{\sim} \xrightarrow{id} PH^\dagger,n-1(X) \]

1. Compute \( \left\{ \frac{x^\beta}{f^m} \omega \right\}_\beta \) a monomial basis for \( PH_{dR}^{n-1}(X_{\mathbb{Q}_q}) \)

where \( \omega := \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n} \)

2. In \( PH^\dagger,n \) compute a series approximation for

\[ \sigma \left( \frac{x^\beta}{f^m} \omega \right) = p^n \frac{x^{p\beta}}{f^{pm}} \omega \sum_{i \geq 0} \left( \begin{array}{c} -m \\ i \end{array} \right) \left( \frac{\sigma(f) - f^p}{f^p} \right)^i \]

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.
Generic algorithm – Abbott–Kedlaya–Roe type

$$\text{PH}_d^{n-1}(X_{\mathbb{Q}_q}) \xrightarrow{\sim} \text{PH}_{dR}^{n-1}(X)$$

1. Compute $$\left\{ \frac{x^\beta}{f_m} \omega \right\}_{\beta}$$ a monomial basis for $$\text{PH}_d^{n-1}(X_{\mathbb{Q}_q})$$
   where $$\omega := \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n}$$

2. In $$\text{PH}_{dR}^{n-1}(X)$$ 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

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

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

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

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.

\[
\sum_{i=0}^{K-1} \binom{-m}{i} \left( \frac{\sigma(f) - f^p}{f^p} \right)^i = \cdots = \sum_{i=0}^{K-1} \binom{-m}{i} \binom{m + K - 1}{K - i - 1} \sigma(f)^i f^{-p(m+i)}
\]
<table>
<thead>
<tr>
<th>Abbott–Kedlaya–Roe</th>
<th>vs</th>
<th>C.–Harvey–Kedlaya</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sum_{i=0}^{K-1} (-m)^i \left( \frac{\sigma(f)}{f_p} \right)^i$</td>
<td></td>
<td>$\sum_{i=0}^{K-1} (-m)^i \binom{m+K-1}{K-i-1} \sigma(f)^i f - p^{m+i}$</td>
</tr>
<tr>
<td>$(pdK)^n + O(1)$ terms</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Schematically

<table>
<thead>
<tr>
<th>Abbott–Kedlaya–Roe</th>
<th>vs</th>
<th>C.–Harvey–Kedlaya</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sum_{i=0}^{K-1} \left( \begin{array}{c} -m \ i \end{array} \right) \left( \frac{\sigma(f) - f^p}{f^p} \right)^i )</td>
<td>( \sum_{i=0}^{K-1} \left( \begin{array}{c} -m \ i \end{array} \right) \left( \begin{array}{c} m + K - 1 \ K - i - 1 \end{array} \right) \sigma(f)^i f^{-p(m+i)} )</td>
<td></td>
</tr>
<tr>
<td>( (pdK)^{n+O(1)} ) terms</td>
<td>( (dK)^{n+O(1)} ) terms</td>
<td></td>
</tr>
</tbody>
</table>
Schematically

Abbott–Kedlaya–Roe vs C.–Harvey–Kedlaya

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

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

\[ \sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)} \]

\((dK)^{n+O(1)}\) terms
Schematically

Abbott–Kedlaya–Roe vs C.–Harvey–Kedlaya

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

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

\[
\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}
\]

\((dK)^{n+O(1)}\) terms
Schematically

Abbott–Kedlaya–Roe vs C.–Harvey–Kedlaya

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

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

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

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

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

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

$p \ell + 1 \rightarrow p \ell$
Schematically

Abbott–Kedlaya–Roe vs C.–Harvey–Kedlaya

\[
\sum_{i=0}^{K-1} \left( -\frac{m}{i} \right) \left( \frac{\sigma(f) - f^p}{f^p} \right)^i
\]

\[(pdK)^{n+O(1)} \text{ terms}\]

\[
\rho : P_{\ell+1} \longrightarrow P_{\ell}
\]

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

\[
\pi : P_n \longrightarrow P_n
\]

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

\[(dK)^{n+O(1)} \text{ terms}\]
Schematically

Abbott–Kedlaya–Roe vs C.–Harvey–Kedlaya

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

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

\[ \sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)} \]

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

\[ \rho : P_{\ell+1} \mapsto P_{\ell} \]

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

“slice” \mapsto “slice”

\[ \pi : P_n \mapsto P_n \]

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

“dot” \mapsto “dot”

Computing zeta functions of nondegenerate hypersurfaces in toric varieties
Generic algorithm – C.–Harvey–Kedlaya

\[ PH_{dR}^{n-1}(X_{\mathbb{Q}_q}) \xrightarrow{\sim} PH^{\dagger,n-1}(X) \]

1. Compute \( \left\{ \frac{x^\beta f^m}{\omega} \right\}_\beta \) a monomial basis for \( PH_{dR}^n(X_{\mathbb{Q}_q}) \)

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

\[
\#(n\Delta \cap L) \sim n^n \text{ vol } \Delta
\]
Compute $\left\{ \frac{x^\beta}{f^m \omega} \right\}_\beta$ a monomial basis for $PH_{dR}^n(X_{Q_q})$

2. In $PH^{\dag,n}$ compute a \textbf{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 \textbf{sparse} reduction algorithm to reduce expansion to basis elements.

- Involves multiplying together $O(p)$ matrices of size
  $$\#(n\Delta \cap L) \sim n^n \text{ vol } \Delta$$
- In a more convoluted process, we can reduce the matrix size to $n! \text{ vol } \Delta$, saving a factor of $e^n \approx n^n / n!$ (e.g. 220 $\sim$ 64)
Generic algorithm – C.–Harvey–Kedlaya

\[
PH_{dR}^{n-1}(X_{\mathbb{Q}_q}) \xrightarrow{\sim} PH_{dR}^{+,n-1}(X)
\]

1. Compute \( \left\{ \frac{x^\beta}{f^{m/\omega}} \right\}_\beta \) a monomial basis for \( PH_{dR}^n(X_{\mathbb{Q}_q}) \)

2. In \( PH_{dR}^{+,n} \) 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
     \( \#(n \Delta \cap L) \sim n^n \text{vol} \Delta \)
   - In a more convoluted process, we can reduce the matrix size to
     \( n! \text{vol} \Delta \), saving a factor of \( e^n \approx n^n/n! \) (e.g. 220 \( \sim \) 64)

For large \( p \), all the work is in step 3.
Some Remarks

• Complexity
  First version of our new algorithm has complexity roughly

\[ p^{1+o(1)} \cdot \text{vol}(\Delta)^{O(n)} \]

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 Remarks

- **Complexity**
  First version of our new algorithm has complexity roughly
  \[ p^{1+o(1)} \text{vol}(\Delta)^{O(n)} \]
  and space complexity is only
  \[ \log p \text{vol}(\Delta)^{O(n)}. \]
Some Remarks

• Complexity
First version of our new algorithm has complexity roughly

\[ p^{1+o(1)} \cdot \text{vol}(\Delta)^{O(n)} \]

and space complexity is only

\[ \log p \cdot \text{vol}(\Delta)^{O(n)}. \]

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

\[ p^{1+o(1)} \mathrm{vol}(\Delta)^{O(n)} \]

and space complexity is only

\[ \log p \ \mathrm{vol}(\Delta)^{O(n)}. \]

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
  \[ p^{1+o(1)} \cdot \text{vol}(\Delta)^{O(n)} \]
  and space complexity is only
  \[ \log p \cdot \text{vol}(\Delta)^{O(n)}. \]
  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
  • 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

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

where the “interesting” factor is

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

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 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 code in $\text{old projective code in } 1m33s$ 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 $2/3 \approx 0.6$).
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.
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 $\zeta_X(t)$:

$$pQ(t/p) = (1 - t) \cdot (1 + t) \cdot (p + 3305t^1 + 1564t^2 - 14296t^3 - 11865t^4$$

$$+ 5107t^5 + 27955t^6 + 25963t^7 + 27955t^8 + 5107t^9$$

$$- 11865t^{10} - 14296t^{11} + 1564t^{12} + 3305t^{13} + pt^{14}).$$

We know of no previous algorithm that can compute $\zeta_X(t)$ for $p$ in this range!
Example: random dense K3 surface

\[ X \subset \mathbb{P}^3_{\mathbb{F}_p} \text{ given by} \]
\[ -9x^4 - 10x^3y - 9x^2y^2 + 2xy^3 - 7y^4 + 6x^3z + 9x^2yz - 2xy^2z + 3y^3z \]
\[ + 8x^2z^2 + 6y^2z^2 + 2xz^3 + 7yz^3 + 9z^4 + 8x^3w + x^2yw - 8xy^2w - 7y^3w \]
\[ + 9x^2zw - 9xyzw + 3y^2zw - xz^2w - 3yz^2w + z^3w - x^2w^2 - 4xyw^2 \]
\[ - 3xzw^2 + 8yzw^2 - 6z^2w^2 + 4xw^3 + 3yw^3 + 4zw^3 - 5w^4 = 0 \]

For \( p = 2^{15} - 19 \), in 38m27s, we obtain

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

where

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

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

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

In $11m18s$, we compute that

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

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

\[x_0^2 x_1 + x_0 x_1^2 + x_1^2 x_2 + x_0 x_2^2 + 4x_0^2 x_3 + x_1^2 x_3
+ 8x_0 x_2 x_3 + 2x_1 x_2 x_3 + 2x_2^2 x_3 + 4x_0 x_3^2 + x_1 x_3^2 + x_3^3 + 8x_0 x_1 x_4
+ x_1^2 x_4 + 4x_1 x_2 x_4 + x_2^2 x_4 + 8x_0 x_3 x_4 + 2x_2 x_3 x_4 + 8x_0 x_4^2
+ x_1 x_4^2 + 2x_3 x_4^2 + x_4^3 + 2x_0^2 x_5 + x_1^2 x_5 + x_1 x_2 x_5 + x_2^2 x_5
+ 8x_0 x_3 x_5 + x_1 x_3 x_5 + x_3^2 x_5 + 4x_0 x_4 x_5 + 3x_3 x_4 x_5 + 2x_0 x_5^2 + x_4 x_5^2.\]

For \( p = 23 \), in 22h52m, we computed \( \zeta_X(t) \) using 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

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

For \( p = 23 \), in \( 22\text{h} 52\text{m} \), we computed \( \zeta_X(t) \) using 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 \( 26\text{h} 34\text{m} \) and for \( p = 499 \) it was \( 33\text{h} 47\text{m} \).

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


- **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

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

- **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

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

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