Computing zeta functions of nondegenerate toric hypersurfaces

Kiran S. Kedlaya

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

Arithmetic, Geometry, Cryptography, and Coding Theory (AGC^{2}T-16)
Centre International de Recherches Mathématiques
June 21, 2017

Joint work (in preparation) with Edgar Costa (Dartmouth) and David Harvey (University of New South Wales).

Kedlaya was supported by NSF grant DMS-1501214 and UCSD (Warschawski chair).

Contents

1. The zeta function problem
2. Review of AGCT 2005
3. Beyond projective space: toric varieties
4. Some numerical examples
5. Next steps

The zeta function of an algebraic variety

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

$$\zeta(X,T) := \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right) \in \mathbb{Z}[\![T]\!] \cap \mathbb{Q}(T).$$

We consider the algorithmic problem of recovering $\zeta(X,T)$ from an *explicit* description of X.

This problem is in principle solvable: use some geometric argument to bound the degree of the rational function, then enumerate $X(\mathbb{F}_{q^n})$ for enough values of n. However, in all but a few cases (e.g., curves of low genus over small $\mathbb{F}_q$) one needs a better approach in practice.

The zeta function of an algebraic variety

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

$$\zeta(X, T) := \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right) \in \mathbb{Z}[\![T]\!] \cap \mathbb{Q}(T).$$

We consider the algorithmic problem of recovering $\zeta(X, T)$ from an *explicit* description of X.

This problem is in principle solvable: use some geometric argument to bound the degree of the rational function, then enumerate $X(\mathbb{F}_{q^n})$ for enough values of n. However, in all but a few cases (e.g., curves of low genus over small $\mathbb{F}_q$) one needs a better approach in practice.

The zeta function of an algebraic variety

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

$$\zeta(X, T) := \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}\right) \in \mathbb{Z}[\![T]\!] \cap \mathbb{Q}(T).$$

We consider the algorithmic problem of recovering $\zeta(X, T)$ from an *explicit* description of X.

This problem is in principle solvable: use some geometric argument to bound the degree of the rational function, then enumerate $X(\mathbb{F}_{q^n})$ for enough values of n. However, in all but a few cases (e.g., curves of low genus over small $\mathbb{F}_q$) one needs a better approach in practice.

Use cases

- This might be easier than testing for isomorphisms (Voloch's talk).
- In cryptography, one often wants to know $\#J(C)$ for C a low-genus curve over a large $\mathbb{F}_q$, especially in the case $q = p$. We mostly ignore this case.
- In coding theory, one may want $\#X(\mathbb{F}_q)$ in order to control a Riemann–Roch space.
- One can also use $\zeta(X, T)$ to control other numerical invariants. E.g., for X a smooth projective surface, $\zeta(X, T)$ reflects the Picard number (Voloch–Zarzar, AGCT 2005) and the order of the Brauer group.
- …

Use cases

- This might be easier than testing for isomorphisms (Voloch's talk).
- In cryptography, one often wants to know $\#J(C)$ for C a low-genus curve over a large $\mathbb{F}_q$, especially in the case $q = p$. We mostly ignore this case.
- In coding theory, one may want $\#X(\mathbb{F}_q)$ in order to control a Riemann–Roch space.
- One can also use $\zeta(X, T)$ to control other numerical invariants. E.g., for X a smooth projective surface, $\zeta(X, T)$ reflects the Picard number (Voloch–Zarzar, AGCT 2005) and the order of the Brauer group.
- ...

Use cases

- This might be easier than testing for isomorphisms (Voloch's talk).
- In cryptography, one often wants to know $\#J(C)$ for C a low-genus curve over a large $\mathbb{F}_q$, especially in the case $q = p$. We mostly ignore this case.
- In coding theory, one may want $\#X(\mathbb{F}_q)$ in order to control a Riemann–Roch space.
- One can also use $\zeta(X, T)$ to control other numerical invariants. E.g., for X a smooth projective surface, $\zeta(X, T)$ reflects the Picard number (Voloch–Zarzar, AGCT 2005) and the order of the Brauer group.
- ...

Use cases

- This might be easier than testing for isomorphisms (Voloch's talk).
- In cryptography, one often wants to know $\#J(C)$ for C a low-genus curve over a large $\mathbb{F}_q$, especially in the case $q = p$. We mostly ignore this case.
- In coding theory, one may want $\#X(\mathbb{F}_q)$ in order to control a Riemann–Roch space.
- One can also use $\zeta(X, T)$ to control other numerical invariants. E.g., for X a smooth projective surface, $\zeta(X, T)$ reflects the Picard number (Voloch–Zarzar, AGCT 2005) and the order of the Brauer group.
- …

Use cases

- This might be easier than testing for isomorphisms (Voloch's talk).
- In cryptography, one often wants to know $\#J(C)$ for C a low-genus curve over a large $\mathbb{F}_q$, especially in the case $q = p$. We mostly ignore this case.
- In coding theory, one may want $\#X(\mathbb{F}_q)$ in order to control a Riemann–Roch space.
- One can also use $\zeta(X, T)$ to control other numerical invariants. E.g., for X a smooth projective surface, $\zeta(X, T)$ reflects the Picard number (Voloch–Zarzar, AGCT 2005) and the order of the Brauer group.
- ...

More use cases: number fields

If one starts with a variety over a number field K, it admits *L-functions* built out of the zeta functions of its reductions. Computing these for *all* primes of norm up to some bound has several applications.

- The distribution of the factors reflects interesting geometry (Sato–Tate conjecture, Lang–Trotter conjecture, etc.)
- Computing special values of L-functions may shed light on Birch–Swinnerton-Dyer and related conjectures.
- One may want to match these L-functions up with automorphic ones, as in the Langlands correspondence.
- …

More use cases: number fields

If one starts with a variety over a number field K, it admits *L-functions* built out of the zeta functions of its reductions. Computing these for *all* primes of norm up to some bound has several applications.

- The distribution of the factors reflects interesting geometry (Sato–Tate conjecture, Lang–Trotter conjecture, etc.)
- Computing special values of L-functions may shed light on Birch–Swinnerton-Dyer and related conjectures.
- One may want to match these L-functions up with automorphic ones, as in the Langlands correspondence.
- ...

More use cases: number fields

If one starts with a variety over a number field K, it admits *L-functions* built out of the zeta functions of its reductions. Computing these for *all* primes of norm up to some bound has several applications.

- The distribution of the factors reflects interesting geometry (Sato–Tate conjecture, Lang–Trotter conjecture, etc.)
- Computing special values of L-functions may shed light on Birch–Swinnerton-Dyer and related conjectures.
- One may want to match these L-functions up with automorphic ones, as in the Langlands correspondence.
- ...

More use cases: number fields

If one starts with a variety over a number field K, it admits *L-functions* built out of the zeta functions of its reductions. Computing these for *all* primes of norm up to some bound has several applications.

- The distribution of the factors reflects interesting geometry (Sato–Tate conjecture, Lang–Trotter conjecture, etc.)
- Computing special values of L-functions may shed light on Birch–Swinnerton-Dyer and related conjectures.
- One may want to match these L-functions up with automorphic ones, as in the Langlands correspondence.
- ...

More use cases: number fields

If one starts with a variety over a number field K, it admits *L-functions* built out of the zeta functions of its reductions. Computing these for *all* primes of norm up to some bound has several applications.

- The distribution of the factors reflects interesting geometry (Sato–Tate conjecture, Lang–Trotter conjecture, etc.)
- Computing special values of L-functions may shed light on Birch–Swinnerton-Dyer and related conjectures.
- One may want to match these L-functions up with automorphic ones, as in the Langlands correspondence.
- ...

Some taxonomy of cases

Say we want $\zeta(X, T)$ for some quasi-projective X over $\mathbb{F}_q$.

- For $\dim(X)$ large, this is NP-complete and hence (?) intractable.
- For $\dim(X)$ fixed, no polynomial-time algorithm in $\log p$, $\log_p q$, $\deg(X)$ is known.
- For p large, little is known. Schoof–Pila is polynomial-time for curves of genus g, but only practical if $g \leq 2$ or some extra structure is available (e.g., real multiplication).
- For p fixed, a polynomial-time algorithm can be derived from Dwork's p-adic analytic proof that $\zeta(X, T) \in \mathbb{Q}(T)$ (Lauder–Wan; Harvey). This is not practical, but is closely related to methods of *p-adic cohomlogy* which do work well in practice.

Some taxonomy of cases

Say we want $\zeta(X, T)$ for some quasi-projective X over $\mathbb{F}_q$.

- For $\dim(X)$ large, this is NP-complete and hence (?) intractable.
- For $\dim(X)$ fixed, no polynomial-time algorithm in $\log p$, $\log_p q$, $\deg(X)$ is known.
- For p large, little is known. Schoof–Pila is polynomial-time for curves of genus g, but only practical if $g \leq 2$ or some extra structure is available (e.g., real multiplication).
- For p fixed, a polynomial-time algorithm can be derived from Dwork's p-adic analytic proof that $\zeta(X, T) \in \mathbb{Q}(T)$ (Lauder–Wan; Harvey). This is not practical, but is closely related to methods of *p-adic cohomlogy* which do work well in practice.

Some taxonomy of cases

Say we want $\zeta(X, T)$ for some quasi-projective X over $\mathbb{F}_q$.

- For $\dim(X)$ large, this is NP-complete and hence (?) intractable.
- For $\dim(X)$ fixed, no polynomial-time algorithm in $\log p$, $\log_p q$, $\deg(X)$ is known.
- For p large, little is known. Schoof–Pila is polynomial-time for curves of genus g, but only practical if $g \leq 2$ or some extra structure is available (e.g., real multiplication).
- For p fixed, a polynomial-time algorithm can be derived from Dwork's p-adic analytic proof that $\zeta(X, T) \in \mathbb{Q}(T)$ (Lauder–Wan; Harvey). This is not practical, but is closely related to methods of *p-adic cohomlogy* which do work well in practice.

Some taxonomy of cases

Say we want $\zeta(X, T)$ for some quasi-projective X over $\mathbb{F}_q$.

- For $\dim(X)$ large, this is NP-complete and hence (?) intractable.
- For $\dim(X)$ fixed, no polynomial-time algorithm in $\log p$, $\log_p q$, $\deg(X)$ is known.
- For p large, little is known. Schoof–Pila is polynomial-time for curves of genus g, but only practical if $g \leq 2$ or some extra structure is available (e.g., real multiplication).
- For p fixed, a polynomial-time algorithm can be derived from Dwork's p-adic analytic proof that $\zeta(X, T) \in \mathbb{Q}(T)$ (Lauder–Wan; Harvey). This is not practical, but is closely related to methods of *p-adic cohomology* which do work well in practice.

Some taxonomy of cases

Say we want $\zeta(X, T)$ for some quasi-projective X over $\mathbb{F}_q$.

- For $\dim(X)$ large, this is NP-complete and hence (?) intractable.
- For $\dim(X)$ fixed, no polynomial-time algorithm in $\log p$, $\log_p q$, $\deg(X)$ is known.
- For p large, little is known. Schoof–Pila is polynomial-time for curves of genus g, but only practical if $g \leq 2$ or some extra structure is available (e.g., real multiplication).
- For p fixed, a polynomial-time algorithm can be derived from Dwork's p-adic analytic proof that $\zeta(X, T) \in \mathbb{Q}(T)$ (Lauder–Wan; Harvey). This is not practical, but is closely related to methods of *p-adic cohomlogy* which do work well in practice.

Methods based on p-adic cohomology

Hereafter, we focus on algorithms derived from spectral interpretations

$$\zeta(X,T) := \prod_{i=0}^{2\dim(X)} \det(1-FT, H^i(X))^{(-1)^{i+1}}$$

where $H^i(X)$ are some *computable* finite-dimensional $\mathbb{Q}_p$-vector spaces. (By contrast, ℓ-adic étale cohomology gives a spectral interpretation which is generally not easily computable.)

The spaces $H^i(X)$ are related to *crystalline cohomology* and *de Rham cohomology* (i.e., differential forms). In practice, we assume that X lifts "nicely" to some number field K; then $H^i(X)$ is computed in terms of generators and relations over K, using *exact* linear algebra.

By contrast, the linear operator F on $H^i(X)$ is intrinsically p-adic analytic; in particular, the matrix via which it acts on some basis cannot be represented exactly. One computes it to sufficient p-adic accuracy by carefully truncating some series representation.

Methods based on p-adic cohomology

Hereafter, we focus on algorithms derived from spectral interpretations

$$\zeta(X,T) := \prod_{i=0}^{2\dim(X)} \det(1-FT, H^i(X))^{(-1)^{i+1}}$$

where $H^i(X)$ are some *computable* finite-dimensional $\mathbb{Q}_p$-vector spaces. (By contrast, ℓ-adic étale cohomology gives a spectral interpretation which is generally not easily computable.)

The spaces $H^i(X)$ are related to *crystalline cohomology* and *de Rham cohomology* (i.e., differential forms). In practice, we assume that X lifts "nicely" to some number field K; then $H^i(X)$ is computed in terms of generators and relations over K, using *exact* linear algebra.

By contrast, the linear operator F on $H^i(X)$ is intrinsically p-adic analytic; in particular, the matrix via which it acts on some basis cannot be represented exactly. One computes it to sufficient p-adic accuracy by carefully truncating some series representation.

Methods based on p-adic cohomology

Hereafter, we focus on algorithms derived from spectral interpretations

$$\zeta(X,T) := \prod_{i=0}^{2\dim(X)} \det(1-FT, H^i(X))^{(-1)^{i+1}}$$

where $H^i(X)$ are some *computable* finite-dimensional $\mathbb{Q}_p$-vector spaces. (By contrast, ℓ-adic étale cohomology gives a spectral interpretation which is generally not easily computable.)

The spaces $H^i(X)$ are related to *crystalline cohomology* and *de Rham cohomology* (i.e., differential forms). In practice, we assume that X lifts "nicely" to some number field K; then $H^i(X)$ is computed in terms of generators and relations over K, using *exact* linear algebra.

By contrast, the linear operator F on $H^i(X)$ is intrinsically p-adic analytic; in particular, the matrix via which it acts on some basis cannot be represented exactly. One computes it to sufficient p-adic accuracy by carefully truncating some series representation.

Contents

1. The zeta function problem
2. Review of AGCT 2005
3. Beyond projective space: toric varieties
4. Some numerical examples
5. Next steps

Background: computations on curves

In 2001, I described a practical algorithm for computing zeta functions of (some) hyperelliptic curves. This has been implemented (in MAGMA, SAGE, PARI) and generalized to various extents, notably to (essentially) arbitrary curves (Tuitman).

My talk at AGCT 2005 was about a first attempt to compute examples for higher-dimensional varieties, especially smooth quartic (K3) surfaces in $\mathbb{P}^3$. The immediate motivation was to generate examples of a construction of Voloch–Zarzar of algebraic geometry codes derived from surfaces (also presented at AGCT 2005).

These computations became a summer research project with two MIT undergraduates (Tim Abbott and David Roe). Our resulting paper appears in the AGCT 2005 proceedings.

Background: computations on curves

In 2001, I described a practical algorithm for computing zeta functions of (some) hyperelliptic curves. This has been implemented (in MAGMA, SAGE, PARI) and generalized to various extents, notably to (essentially) arbitrary curves (Tuitman).

My talk at AGCT 2005 was about a first attempt to compute examples for higher-dimensional varieties, especially smooth quartic (K3) surfaces in $\mathbb{P}^3$. The immediate motivation was to generate examples of a construction of Voloch–Zarzar of algebraic geometry codes derived from surfaces (also presented at AGCT 2005).

These computations became a summer research project with two MIT undergraduates (Tim Abbott and David Roe). Our resulting paper appears in the AGCT 2005 proceedings.

Background: computations on curves

In 2001, I described a practical algorithm for computing zeta functions of (some) hyperelliptic curves. This has been implemented (in Magma, Sage, Pari) and generalized to various extents, notably to (essentially) arbitrary curves (Tuitman).

My talk at AGCT 2005 was about a first attempt to compute examples for higher-dimensional varieties, especially smooth quartic (K3) surfaces in $\mathbb{P}^3$. The immediate motivation was to generate examples of a construction of Voloch–Zarzar of algebraic geometry codes derived from surfaces (also presented at AGCT 2005).

These computations became a summer research project with two MIT undergraduates (Tim Abbott and David Roe). Our resulting paper appears in the AGCT 2005 proceedings.

More on the computation: de Rham cohomology

Let X be a smooth hypersurface in $\mathbb{P}^n_{\mathbb{F}_q}$ cut out by the homogeneous polynomial $P(x_0, \dots, x_n)$. For $U = \mathbb{P}^n_{\mathbb{F}_q} - X$, we have

$$\zeta(X, T)\zeta(U, T) = \zeta(\mathbb{P}^n, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}$$

so computing $\zeta(X, T)$ and $\zeta(U, T)$ are equivalent tasks. Note that

$$U = \mathrm{Spec}(\text{degree 0 part of } \mathbb{F}_q[x_0, \dots, x_n, f^{-1}])$$

is an affine variety. For example, algebraic de Rham cohomology of U, defined as hypercohomology of the complex of sheaves

$$0 \to \mathcal{O} \xrightarrow{d} \Omega^1 \to \cdots \to \Omega^n \to 0,$$

equals ordinary cohomology of the complex of global sections.

More on de Rham cohomology

Because de Rham cohomology behaves strangely in characteristic p, we instead work with the hypersurface $\tilde{X}$ cut out by a lift $\tilde{P}$ of P. This lift can be taken over a number field K with an ideal of norm q. The algebraic de Rham cohomology of the complement $\tilde{U}$ (in degree n, the rest being negligible) can be computed using the *Griffiths–Dwork reduction process*.

Represent each differential as a degree 0 quotient

$$\frac{A\Omega}{P^m}, \qquad \Omega = \sum_{i=0}^{n} (-1)^i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_m.$$

For $m > n$, we can reduce the pole order in cohomology using the relations

$$\frac{(\partial_i A)\Omega}{P^m} \equiv m \frac{A(\partial_i P)\Omega}{P^{m+1}}, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

(A theorem of Macaulay guarantees that these relations suffice.)

More on de Rham cohomology

Because de Rham cohomology behaves strangely in characteristic p, we instead work with the hypersurface $\tilde{X}$ cut out by a lift $\tilde{P}$ of P. This lift can be taken over a number field K with an ideal of norm q. The algebraic de Rham cohomology of the complement $\tilde{U}$ (in degree n, the rest being negligible) can be computed using the *Griffiths–Dwork reduction process*.

Represent each differential as a degree 0 quotient

$$\frac{A\Omega}{P^m}, \qquad \Omega = \sum_{i=0}^{n} (-1)^i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_m.$$

For $m > n$, we can reduce the pole order in cohomology using the relations

$$\frac{(\partial_i A)\Omega}{P^m} \equiv m \frac{A(\partial_i P)\Omega}{P^{m+1}}, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

(A theorem of Macaulay guarantees that these relations suffice.)

More on de Rham cohomology

Because de Rham cohomology behaves strangely in characteristic p, we instead work with the hypersurface $\tilde{X}$ cut out by a lift $\tilde{P}$ of P. This lift can be taken over a number field K with an ideal of norm q. The algebraic de Rham cohomology of the complement $\tilde{U}$ (in degree n, the rest being negligible) can be computed using the *Griffiths–Dwork reduction process*.

Represent each differential as a degree 0 quotient

$$\frac{A\Omega}{P^m}, \qquad \Omega = \sum_{i=0}^{n} (-1)^i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_m.$$

For $m > n$, we can reduce the pole order in cohomology using the relations

$$\frac{(\partial_i A)\Omega}{P^m} \equiv m \frac{A(\partial_i P)\Omega}{P^{m+1}}, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

(A theorem of Macaulay guarantees that these relations suffice.)

More on de Rham cohomology

Because de Rham cohomology behaves strangely in characteristic p, we instead work with the hypersurface $\tilde{X}$ cut out by a lift $\tilde{P}$ of P. This lift can be taken over a number field K with an ideal of norm q. The algebraic de Rham cohomology of the complement $\tilde{U}$ (in degree n, the rest being negligible) can be computed using the *Griffiths–Dwork reduction process*.

Represent each differential as a degree 0 quotient

$$\frac{A\Omega}{P^m}, \qquad \Omega = \sum_{i=0}^{n} (-1)^i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_m.$$

For $m > n$, we can reduce the pole order in cohomology using the relations

$$\frac{(\partial_i A)\Omega}{P^m} \equiv m \frac{A(\partial_i P)\Omega}{P^{m+1}}, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

(A theorem of Macaulay guarantees that these relations suffice.)

The action of Frobenius on de Rham cohomology

The action of Frobenius on cohomology is induced by the substitution $\sigma : x_i \mapsto x_i^q$, using the expansion

$$P^{-m} \mapsto \sum_{i=0}^{\infty} \binom{-m}{i} \frac{(P^\sigma - P^q)^i}{P^{q(m+i)}}.$$

In 2005, we computed the matrix of action by expanding the numerators, then using commutative algebra in MAGMA. In this way, we were able to compute $\zeta(X, T)$ for some examples with $n = 3$, $\deg(X) = 4$, $q \leq 17$.

The action of Frobenius on de Rham cohomology

The action of Frobenius on cohomology is induced by the substitution $\sigma : x_i \mapsto x_i^q$, using the expansion

$$P^{-m} \mapsto \sum_{i=0}^{\infty} \binom{-m}{i} \frac{(P^\sigma - P^q)^i}{P^{q(m+i)}}.$$

In 2005, we computed the matrix of action by expanding the numerators, then using commutative algebra in Magma. In this way, we were able to compute $\zeta(X, T)$ for some examples with $n = 3$, $\deg(X) = 4$, $q \leq 17$.

Taking advantage of sparsity: controlled reduction

In order to proceed further, we need a crucial improvement introduced by Harvey in the context of hyperelliptic curves. First, rewrite the expansion as

$$P^{-m} \mapsto \sum_{i=0}^{\infty} \sum_{j=0}^{i} (-1)^{j-i} \binom{-m}{i} \binom{i}{j} \frac{(P^\sigma)^j}{P^{q(m+j)}}$$

so the numerators all become sparse polynomials.

Second, combine the Griffiths–Dwork relations to get some new relations that preserve sparsity.

At a mild cost in the other parameters, the dependence on p is improved from p^n to p^1. This already makes it possible to compute much bigger examples, e.g., $n = 3$, $\deg(X) = 4$, $q \leq 50000$.

Taking advantage of sparsity: controlled reduction

In order to proceed further, we need a crucial improvement introduced by Harvey in the context of hyperelliptic curves. First, rewrite the expansion as

$$P^{-m} \mapsto \sum_{i=0}^{\infty} \sum_{j=0}^{i} (-1)^{j-i} \binom{-m}{i} \binom{i}{j} \frac{(P^\sigma)^j}{P^{q(m+j)}}$$

so the numerators all become sparse polynomials.

Second, combine the Griffiths–Dwork relations to get some new relations that preserve sparsity.

At a mild cost in the other parameters, the dependence on p is improved from p^n to p^1. This already makes it possible to compute much bigger examples, e.g., $n = 3$, $\deg(X) = 4$, $q \leq 50000$.

Taking advantage of sparsity: controlled reduction

In order to proceed further, we need a crucial improvement introduced by Harvey in the context of hyperelliptic curves. First, rewrite the expansion as

$$P^{-m} \mapsto \sum_{i=0}^{\infty} \sum_{j=0}^{i} (-1)^{j-i} \binom{-m}{i} \binom{i}{j} \frac{(P^\sigma)^j}{P^{q(m+j)}}$$

so the numerators all become sparse polynomials.

Second, combine the Griffiths–Dwork relations to get some new relations that preserve sparsity.

At a mild cost in the other parameters, the dependence on p is improved from p^n to p^1. This already makes it possible to compute much bigger examples, e.g., $n = 3$, $\deg(X) = 4$, $q \leq 50000$.

Contents

1 The zeta function problem

2 Review of AGCT 2005

3 Beyond projective space: toric varieties

4 Some numerical examples

5 Next steps

Toric varieties

If one is interested in "naturally occurring" classes of varieties, one does not get many of these from smooth projective hypersurfaces. (Already for curves, most genera do not occur.)

However, the Griffiths–Dwork method is easily adapted to a hypersurface X in a general toric variety, at least if we replace smoothness by a slightly stronger (but still generic) condition: X is *nondegenerate*[1] if its intersection with each toric stratum is transversal.

For curves, something similar is done by Castryck–Denef–Vercauteren; I proposed a higher-dimensional version some years ago. What makes the key difference for practicality is again *controlled reduction*. (Sperber–Voight have a different approach based on Dwork cohomology.)

[1] The term *schön* is also used.

Toric varieties

If one is interested in "naturally occurring" classes of varieties, one does not get many of these from smooth projective hypersurfaces. (Already for curves, most genera do not occur.)

However, the Griffiths–Dwork method is easily adapted to a hypersurface X in a general toric variety, at least if we replace smoothness by a slightly stronger (but still generic) condition: X is *nondegenerate*[1] if its intersection with each toric stratum is transversal.

For curves, something similar is done by Castryck–Denef–Vercauteren; I proposed a higher-dimensional version some years ago. What makes the key difference for practicality is again *controlled reduction*. (Sperber–Voight have a different approach based on Dwork cohomology.)

[1] The term *schön* is also used.

Toric varieties

If one is interested in “naturally occurring” classes of varieties, one does not get many of these from smooth projective hypersurfaces. (Already for curves, most genera do not occur.)

However, the Griffiths–Dwork method is easily adapted to a hypersurface X in a general toric variety, at least if we replace smoothness by a slightly stronger (but still generic) condition: X is *nondegenerate*[1] if its intersection with each toric stratum is transversal.

For curves, something similar is done by Castryck–Denef–Vercauteren; I proposed a higher-dimensional version some years ago. What makes the key difference for practicality is again *controlled reduction*. (Sperber–Voight have a different approach based on Dwork cohomology.)

[1] The term *schön* is also used.

Executive summary of toric varieties

Write down a toric hypersurface defined by a Laurent polynomial

$$P = \sum_{\underline{i} \in \mathbb{Z}^n} P_{\underline{i}} \underline{x}^{\underline{i}} \in \mathbb{F}_q[x_1^{\pm}, \dots, x_n^{\pm}].$$

Its *Newton polytope* is the convex hull in $\mathbb{R}^n$ of the support of P; this defines a projective toric variety. Nondegeneracy means this hypersurface *and* the cross-section by any bounding hyperplane (in any dimension) are all smooth in their respective tori.

Bonus feature: if the support of P lies in a sublattice of $\mathbb{Z}^n$, we can use that instead. This amounts to quotienting by a finite abelian group to get an easier calculation; the "interesting" part of cohomology persists in the quotient, but extra work may be needed to recover a "trivial" cofactor.

Contents

1. The zeta function problem
2. Review of AGCT 2005
3. Beyond projective space: toric varieties
4. Some numerical examples
5. Next steps

Example: a random dense quartic

Consider the surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ for $p = 49999$ given by

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

In 1h5m5s, we obtain

$$\begin{aligned}\zeta(X, T) &= (1-T)^{-1}(1-pT)^{-1}(1-p^2T)^{-1}Q(T)^{-1} \\ pQ(p^{-1}T) &= (1-T)(49999 + 63115T + 14796T^2 + 42361T^3 \\ &\quad + 49443T^4 + 11718T^5 + 42046T^6 + 51501T^7 + 20534T^8 \\ &\quad + 27146T^9 + 38370T^{10} + 27146T^{11} + 20534T^{12} + 51501T^{13} \\ &\quad + 42046T^{14} + 11718T^{15} + 49443T^{16} + 42361T^{17} + 14796T^{18} \\ &\quad + 63115T^{19} + 49999T^{20}).\end{aligned}$$

Example: a random dense quartic

Consider the surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ for $p = 49999$ given by

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

In 1h5m5s, we obtain

$$\begin{aligned}
\zeta(X, T) &= (1-T)^{-1}(1-pT)^{-1}(1-p^2T)^{-1}Q(T)^{-1} \\
pQ(p^{-1}T) &= (1-T)(49999 + 63115\,T + 14796\,T^2 + 42361\,T^3 \\
&\quad + 49443\,T^4 + 11718\,T^5 + 42046\,T^6 + 51501\,T^7 + 20534\,T^8 \\
&\quad + 27146\,T^9 + 38370\,T^{10} + 27146\,T^{11} + 20534\,T^{12} + 51501\,T^{13} \\
&\quad + 42046\,T^{14} + 11718\,T^{15} + 49443\,T^{16} + 42361\,T^{17} + 14796\,T^{18} \\
&\quad + 63115\,T^{19} + 49999\,T^{20}).
\end{aligned}$$

Example: a quartic surface in the Dwork pencil

Consider the surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ for $p = 49999$ given by

$$x_0^4 + \cdots + x_3^4 + x_0x_1x_2x_3 = 0.$$

In 4.3s, we compute that

$$\zeta(X, T) = \frac{1}{(1-T)(1-pT)R_1(pT)^3R_2(pT)^6(1-p^2T)Q(T)}$$

where the "interesting" factor $Q(T)$ equals $(1-pT)(1+95902T+p^2T^2)$.

In this case, the monomials generate a sublattice of index 4^2 in $\mathbb{Z}^3$. The polynomials R_1 and R_2 arise from the action of Frobenius on the Néron–Severi lattice; by a p-adic formula of de la Ossa–Kadir,

$$R_1(T) = (1 \pm T)(1 \pm T), \qquad R_2(T) = 1 - T^2.$$

Example: a quartic surface in the Dwork pencil

Consider the surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ for $p = 49999$ given by

$$x_0^4 + \cdots + x_3^4 + x_0x_1x_2x_3 = 0.$$

In 4.3s, we compute that

$$\zeta(X, T) = \frac{1}{(1-T)(1-pT)R_1(pT)^3R_2(pT)^6(1-p^2T)Q(T)}$$

where the "interesting" factor $Q(T)$ equals $(1-pT)(1+95902T+p^2T^2)$.

In this case, the monomials generate a sublattice of index 4^2 in $\mathbb{Z}^3$. The polynomials R_1 and R_2 arise from the action of Frobenius on the Néron–Severi lattice; by a p-adic formula of de la Ossa–Kadir,

$$R_1(T) = (1 \pm T)(1 \pm T), \qquad R_2(T) = 1 - T^2.$$

Example: a quartic surface in the Dwork pencil

Consider the surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ for $p = 49999$ given by

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

In 4.3s, we compute that

$$\zeta(X, T) = \frac{1}{(1-T)(1-pT)R_1(pT)^3 R_2(pT)^6 (1-p^2T)Q(T)}$$

where the "interesting" factor $Q(T)$ equals $(1-pT)(1+95902T+p^2T^2)$.

In this case, the monomials generate a sublattice of index 4^2 in $\mathbb{Z}^3$. The polynomials R_1 and R_2 arise from the action of Frobenius on the Néron–Severi lattice; by a p-adic formula of de la Ossa–Kadir,

$$R_1(T) = (1 \pm T)(1 \pm T), \qquad R_2(T) = 1 - T^2.$$

Example: a quintic threefold in the Dwork pencil

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

$$x_0^5 + \cdots + x_4^5 + x_0x_1x_2x_3x_4 = 0.$$

In 657s, we compute that

$$\zeta(X, T) = \frac{R_1(pT)^{20} R_2(pT)^{30} Q(T)}{(1-T)(1-pT)(1-p^2T)(1-p^3T)}$$

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

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

The factor $Q(T)$ also shows up in the zeta function of the *mirror quintic*...

Example: a quintic threefold in the Dwork pencil

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

$$x_0^5 + \cdots + x_4^5 + x_0x_1x_2x_3x_4 = 0.$$

In 657s, we compute that

$$\zeta(X, T) = \frac{R_1(pT)^{20} R_2(pT)^{30} Q(T)}{(1-T)(1-pT)(1-p^2T)(1-p^3T)}$$

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

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

The factor $Q(T)$ also shows up in the zeta function of the *mirror quintic*...

Example: a quintic threefold in the Dwork pencil

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

$$x_0^5 + \cdots + x_4^5 + x_0x_1x_2x_3x_4 = 0.$$

In 657s, we compute that

$$\zeta(X, T) = \frac{R_1(pT)^{20}R_2(pT)^{30}Q(T)}{(1-T)(1-pT)(1-p^2T)(1-p^3T)}$$

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

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

The factor $Q(T)$ also shows up in the zeta function of the *mirror quintic*...

Example: another family of K3 surfaces

Consider 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

$$\zeta(X,T) = \frac{1}{(1-T)R(pT)(1-p^2T)Q(T)}$$

where (I think) $R(T) = (1-T)^6(1+T)^4(1+T^2)(1+T^4)$ and

$$pQ(p^{-1}T) = p - 14662T - 31559T^2 - 5620T^3 - 31559T^4 - 14662T^5 + pT^6.$$

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

Example: another family of K3 surfaces

Consider 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

$$\zeta(X,T) = \frac{1}{(1-T)R(pT)(1-p^2T)Q(T)}$$

where (I think) $R(T) = (1-T)^6(1+T)^4(1+T^2)(1+T^4)$ and

$$pQ(p^{-1}T) = p - 14662T - 31559T^2 - 5620T^3 - 31559T^4 - 14662T^5 + pT^6.$$

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

Example: another family of K3 surfaces

Consider 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

$$\zeta(X,T) = \frac{1}{(1-T)R(pT)(1-p^2T)Q(T)}$$

where (I think) $R(T) = (1-T)^6(1+T)^4(1+T^2)(1+T^4)$ and

$$pQ(p^{-1}T) = p - 14662T - 31559T^2 - 5620T^3 - 31559T^4 - 14662T^5 + pT^6.$$

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

Example: a hypergeometric motive

Consider the appropriate completion of the toric surface over $\mathbb{F}_p$ with $p = 71$ given by

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

In 0.14s, we compute that the “interesting” factor of $\zeta(X, T)$ is

$$1 - 75T - 55pT^2 + 134p^2T^3 - 55p^3T^4 - 75p^4T^5 + p^6T^6.$$

This example (from arXiv:1612.09249) can be confirmed using MAGMA:

```
EulerFactor(HypergeometricData([1/12,1/6,5/12,7/12,
10/12,11/12],[0,0,0,1/3,1/2,2/3]),2^10 * 3^6, 71);
```

however, we can handle much larger p (e.g., $p = 49999$), for which MAGMA can only compute the coefficient of T.

Example: a hypergeometric motive

Consider the appropriate completion of the toric surface over $\mathbb{F}_p$ with $p = 71$ given by

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

In 0.14s, we compute that the “interesting” factor of $\zeta(X, T)$ is

$$1 - 75T - 55pT^2 + 134p^2T^3 - 55p^3T^4 - 75p^4T^5 + p^6T^6.$$

This example (from arXiv:1612.09249) can be confirmed using Magma:

```
EulerFactor(HypergeometricData([1/12,1/6,5/12,7/12,
10/12,11/12],[0,0,0,1/3,1/2,2/3]),2^10 * 3^6, 71);
```

however, we can handle much larger p (e.g., $p = 49999$), for which Magma can only compute the coefficient of T.

Example: a hypergeometric motive

Consider the appropriate completion of the toric surface over $\mathbb{F}_p$ with $p = 71$ given by

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

In 0.14s, we compute that the "interesting" factor of $\zeta(X, T)$ is

$$1 - 75T - 55pT^2 + 134p^2T^3 - 55p^3T^4 - 75p^4T^5 + p^6T^6.$$

This example (from arXiv:1612.09249) can be confirmed using MAGMA:

```
EulerFactor(HypergeometricData([1/12,1/6,5/12,7/12,
10/12,11/12],[0,0,0,1/3,1/2,2/3]),2^10 * 3^6, 71);
```

however, we can handle much larger p (e.g., $p = 49999$), for which MAGMA can only compute the coefficient of T.

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

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

In 401s, we compute that the "interesting" factor of $\zeta(X, T)$ 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 nondegenerate toric hypersurfaces; there are 7555 such families. See http://hep.itp.tuwien.ac.at/~kreuzer/CY/.

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

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

In 401s, we compute that the "interesting" factor of $\zeta(X, T)$ 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 nondegenerate toric hypersurfaces; there are 7555 such families. See `http://hep.itp.tuwien.ac.at/~kreuzer/CY/`.

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

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

In 401s, we compute that the "interesting" factor of $\zeta(X, T)$ is

$$\begin{gathered} 1 + 6423186T + 2211095838pT^2 - 127485903944p^2T^3 \\ +2211095838p^4T^4 + 6423186p^6T^5 + p^9T^6. \end{gathered}$$

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

Contents

1 The zeta function problem

2 Review of AGCT 2005

3 Beyond projective space: toric varieties

4 Some numerical examples

5 Next steps

Next steps

- Use average polynomial-time methods and/or Harvey's method for reducing the p-dependence to $p^{1/2}$ (after Chudnovsky^2, Bostan–Gaudry–Schost).
- Use the Cayley trick to treat nondegenerate complete intersections in toric varieties. This gives many additional classes of Calabi–Yau threefolds.
- Use this to examine jumping of Picard ranks for K3 surfaces (Costa–Tschinkel, Costa–Elsenhans–Jahnel).
- Use this to examine Sato–Tate distributions for surfaces and threefolds.
- Finish writing the paper already...

Next steps

- Use average polynomial-time methods and/or Harvey's method for reducing the p-dependence to $p^{1/2}$ (after Chudnovsky^2, Bostan–Gaudry–Schost).
- Use the Cayley trick to treat nondegenerate complete intersections in toric varieties. This gives many additional classes of Calabi–Yau threefolds.
- Use this to examine jumping of Picard ranks for K3 surfaces (Costa–Tschinkel, Costa–Elsenhans–Jahnel).
- Use this to examine Sato–Tate distributions for surfaces and threefolds.
- Finish writing the paper already...

Next steps

- Use average polynomial-time methods and/or Harvey's method for reducing the p-dependence to $p^{1/2}$ (after Chudnovsky^2, Bostan–Gaudry–Schost).
- Use the Cayley trick to treat nondegenerate complete intersections in toric varieties. This gives many additional classes of Calabi–Yau threefolds.
- Use this to examine jumping of Picard ranks for K3 surfaces (Costa–Tschinkel, Costa–Elsenhans–Jahnel).
- Use this to examine Sato–Tate distributions for surfaces and threefolds.
- Finish writing the paper already...

Next steps

- Use average polynomial-time methods and/or Harvey's method for reducing the p-dependence to $p^{1/2}$ (after Chudnovsky^2, Bostan–Gaudry–Schost).
- Use the Cayley trick to treat nondegenerate complete intersections in toric varieties. This gives many additional classes of Calabi–Yau threefolds.
- Use this to examine jumping of Picard ranks for K3 surfaces (Costa–Tschinkel, Costa–Elsenhans–Jahnel).
- Use this to examine Sato–Tate distributions for surfaces and threefolds.
- Finish writing the paper already...

Next steps

- Use average polynomial-time methods and/or Harvey's method for reducing the p-dependence to $p^{1/2}$ (after Chudnovsky^2, Bostan–Gaudry–Schost).
- Use the Cayley trick to treat nondegenerate complete intersections in toric varieties. This gives many additional classes of Calabi–Yau threefolds.
- Use this to examine jumping of Picard ranks for K3 surfaces (Costa–Tschinkel, Costa–Elsenhans–Jahnel).
- Use this to examine Sato–Tate distributions for surfaces and threefolds.
- Finish writing the paper already...