Recent progress in computing zeta functions of varieties

Kiran S. Kedlaya

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

Number Theory and Physics
IMPA, Rio de Janeiro, Monday, June 22, 2015

Based in part on joint work (in preparation) with Edgar Costa (NYU/ICERM/Dartmouth) and David Harvey (U. New South Wales).

Zeta functions of algebraic varieties

Let $\mathbb{F}_q$ be a finite field of characteristic p. After Artin, Schmidt, and Weil, we define the *zeta function* of a variety X over $\mathbb{F}_q$ as the formal Dirichlet series

$$\zeta(X, s) = \prod_x (1 - \#\kappa(x)^{-s})^{-1},$$

where x runs over closed points of X and $\kappa(x)$ denotes the residue field. (Equivalently, x runs over Galois orbits of $\overline{\mathbb{F}}_q$-rational points and $\kappa(x)$ denotes the minimal field of definition.)

From now on, we write ζ as a formal power series in $T = q^{-s}$. Then

$$\zeta(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \#X(\mathbb{F}_{q^n})\right).$$

Zeta functions of algebraic varieties

Let $\mathbb{F}_q$ be a finite field of characteristic p. After Artin, Schmidt, and Weil, we define the *zeta function* of a variety X over $\mathbb{F}_q$ as the formal Dirichlet series

$$\zeta(X, s) = \prod_x (1 - \#\kappa(x)^{-s})^{-1},$$

where x runs over closed points of X and $\kappa(x)$ denotes the residue field. (Equivalently, x runs over Galois orbits of $\overline{\mathbb{F}}_q$-rational points and $\kappa(x)$ denotes the minimal field of definition.)

From now on, we write ζ as a formal power series in $T = q^{-s}$. Then

$$\zeta(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \#X(\mathbb{F}_{q^n})\right).$$

Examples of zeta functions

From the formula

$$\zeta(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \# X(\mathbb{F}_{q^n})\right),$$

one can compute $\zeta(X, T)$ in some explicit examples. For one:

$$\zeta(\mathbb{P}^d_{\mathbb{F}_q}, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^d T)}.$$

For another, if X is an elliptic curve over $\mathbb{F}_q$, then

$$\zeta(X, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}, \qquad a = q + 1 - \#X(\mathbb{F}_q).$$

Based on these (and more) examples, Weil predicted that $\zeta(X, T)$ obeys analogues of the properties of the Riemann zeta function (analytic continuation, functional equation, Riemann hypothesis).

Examples of zeta functions

From the formula

$$\zeta(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \#X(\mathbb{F}_{q^n})\right),$$

one can compute $\zeta(X, T)$ in some explicit examples. For one:

$$\zeta(\mathbb{P}^d_{\mathbb{F}_q}, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^d T)}.$$

For another, if X is an elliptic curve over $\mathbb{F}_q$, then

$$\zeta(X, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}, \qquad a = q + 1 - \#X(\mathbb{F}_q).$$

Based on these (and more) examples, Weil predicted that $\zeta(X, T)$ obeys analogues of the properties of the Riemann zeta function (analytic continuation, functional equation, Riemann hypothesis).

Examples of zeta functions

From the formula

$$\zeta(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} \# X(\mathbb{F}_{q^n})\right),$$

one can compute $\zeta(X, T)$ in some explicit examples. For one:

$$\zeta(\mathbb{P}^d_{\mathbb{F}_q}, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^d T)}.$$

For another, if X is an elliptic curve over $\mathbb{F}_q$, then

$$\zeta(X, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}, \qquad a = q + 1 - \#X(\mathbb{F}_q).$$

Based on these (and more) examples, Weil predicted that $\zeta(X, T)$ obeys analogues of the properties of the Riemann zeta function (analytic continuation, functional equation, Riemann hypothesis).

Rationality of the zeta function

The first of the *Weil conjectures* on zeta functions of algebraic varieties is:

Theorem

The power series $\zeta(X, T)$ represents a rational function of T.

This is widely known as a consequence of the construction of *étale cohomology* by Grothendieck et al. However, that was not the first proof!

Theorem (Dwork, 1960)

The power series $\zeta(X, T)$ is p-adic meromorphic: it is the ratio of two power series over $\mathbb{Q}_p$ with infinite radii of convergence.

Since $\zeta(X, T)$ converges for $T \in \mathbb{C}$ small (trivially), an argument of Borel (1894) then shows that $\zeta(X, T)$ is rational.

Rationality of the zeta function

The first of the *Weil conjectures* on zeta functions of algebraic varieties is:

Theorem

The power series $\zeta(X, T)$ represents a rational function of T.

This is widely known as a consequence of the construction of *étale cohomology* by Grothendieck et al. However, that was not the first proof!

Theorem (Dwork, 1960)

The power series $\zeta(X, T)$ is p-adic meromorphic: it is the ratio of two power series over $\mathbb{Q}_p$ with infinite radii of convergence.

Since $\zeta(X, T)$ converges for $T \in \mathbb{C}$ small (trivially), an argument of Borel (1894) then shows that $\zeta(X, T)$ is rational.

Rationality of the zeta function

The first of the *Weil conjectures* on zeta functions of algebraic varieties is:

Theorem

The power series $\zeta(X, T)$ represents a rational function of T.

This is widely known as a consequence of the construction of *étale cohomology* by Grothendieck et al. However, that was not the first proof!

Theorem (Dwork, 1960)

The power series $\zeta(X, T)$ is p-adic meromorphic: it is the ratio of two power series over $\mathbb{Q}_p$ with infinite radii of convergence.

Since $\zeta(X, T)$ converges for $T \in \mathbb{C}$ small (trivially), an argument of Borel (1894) then shows that $\zeta(X, T)$ is rational.

Rationality of the zeta function

The first of the *Weil conjectures* on zeta functions of algebraic varieties is:

Theorem

The power series $\zeta(X, T)$ represents a rational function of T.

This is widely known as a consequence of the construction of *étale cohomology* by Grothendieck et al. However, that was not the first proof!

Theorem (Dwork, 1960)

The power series $\zeta(X, T)$ is p-adic meromorphic: it is the ratio of two power series over $\mathbb{Q}_p$ with infinite radii of convergence.

Since $\zeta(X, T)$ converges for $T \in \mathbb{C}$ small (trivially), an argument of Borel (1894) then shows that $\zeta(X, T)$ is rational.

Rationality of the zeta function

The first of the *Weil conjectures* on zeta functions of algebraic varieties is:

Theorem

The power series $\zeta(X, T)$ represents a rational function of T.

This is widely known as a consequence of the construction of *étale cohomology* by Grothendieck et al. However, that was not the first proof!

Theorem (Dwork, 1960)

The power series $\zeta(X, T)$ is p-adic meromorphic: it is the ratio of two power series over $\mathbb{Q}_p$ with infinite radii of convergence.

Since $\zeta(X, T)$ converges for $T \in \mathbb{C}$ small (trivially), an argument of Borel (1894) then shows that $\zeta(X, T)$ is rational.

Zeta functions as empirical data

We are interested in algorithms that given an explicit definition of X (i.e., defining equations), returns the rational function $\zeta(X, T)$. Why?

- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#X(\mathbb{F}_q)$. Questions about this count, especially its extreme values, were originally inspired by algebraic coding theory (Goppa construction) and have been studied for decades; see `http://manypoints.org`.
- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#J(X)(\mathbb{F}_q)$. This is relevant for cryptography, especially when X is of genus ≤ 3.
- For X a variety over $\mathbb{F}_q$, $\zeta(X, T)$ contains (via the Tate conjecture) information about algebraic cycles on X, e.g., the Picard number.
- Computation of many types of exponential sums can be encoded into the problem of computing $\zeta(X, T)$ for suitable X.
- ...

Zeta functions as empirical data

We are interested in algorithms that given an explicit definition of X (i.e., defining equations), returns the rational function $\zeta(X, T)$. Why?

- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#X(\mathbb{F}_q)$. Questions about this count, especially its extreme values, were originally inspired by algebraic coding theory (Goppa construction) and have been studied for decades; see `http://manypoints.org`.
- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#J(X)(\mathbb{F}_q)$. This is relevant for cryptography, especially when X is of genus ≤ 3.
- For X a variety over $\mathbb{F}_q$, $\zeta(X, T)$ contains (via the Tate conjecture) information about algebraic cycles on X, e.g., the Picard number.
- Computation of many types of exponential sums can be encoded into the problem of computing $\zeta(X, T)$ for suitable X.
- ...

Zeta functions as empirical data

We are interested in algorithms that given an explicit definition of X (i.e., defining equations), returns the rational function $\zeta(X, T)$. Why?

- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#X(\mathbb{F}_q)$. Questions about this count, especially its extreme values, were originally inspired by algebraic coding theory (Goppa construction) and have been studied for decades; see `http://manypoints.org`.
- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#J(X)(\mathbb{F}_q)$. This is relevant for cryptography, especially when X is of genus ≤ 3.
- For X a variety over $\mathbb{F}_q$, $\zeta(X, T)$ contains (via the Tate conjecture) information about algebraic cycles on X, e.g., the Picard number.
- Computation of many types of exponential sums can be encoded into the problem of computing $\zeta(X, T)$ for suitable X.
- ...

Zeta functions as empirical data

We are interested in algorithms that given an explicit definition of X (i.e., defining equations), returns the rational function $\zeta(X, T)$. Why?

- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#X(\mathbb{F}_q)$. Questions about this count, especially its extreme values, were originally inspired by algebraic coding theory (Goppa construction) and have been studied for decades; see `http://manypoints.org`.
- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#J(X)(\mathbb{F}_q)$. This is relevant for cryptography, especially when X is of genus ≤ 3.
- For X a variety over $\mathbb{F}_q$, $\zeta(X, T)$ contains (via the Tate conjecture) information about algebraic cycles on X, e.g., the Picard number.
- Computation of many types of exponential sums can be encoded into the problem of computing $\zeta(X, T)$ for suitable X.
- ...

Zeta functions as empirical data

We are interested in algorithms that given an explicit definition of X (i.e., defining equations), returns the rational function $\zeta(X, T)$. Why?

- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#X(\mathbb{F}_q)$. Questions about this count, especially its extreme values, were originally inspired by algebraic coding theory (Goppa construction) and have been studied for decades; see `http://manypoints.org`.
- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#J(X)(\mathbb{F}_q)$. This is relevant for cryptography, especially when X is of genus ≤ 3.
- For X a variety over $\mathbb{F}_q$, $\zeta(X, T)$ contains (via the Tate conjecture) information about algebraic cycles on X, e.g., the Picard number.
- Computation of many types of exponential sums can be encoded into the problem of computing $\zeta(X, T)$ for suitable X.
- ...

Zeta functions as empirical data

We are interested in algorithms that given an explicit definition of X (i.e., defining equations), returns the rational function $\zeta(X, T)$. Why?

- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#X(\mathbb{F}_q)$. Questions about this count, especially its extreme values, were originally inspired by algebraic coding theory (Goppa construction) and have been studied for decades; see `http://manypoints.org`.
- For X a curve over $\mathbb{F}_q$, $\zeta(X, T)$ determines $\#J(X)(\mathbb{F}_q)$. This is relevant for cryptography, especially when X is of genus ≤ 3.
- For X a variety over $\mathbb{F}_q$, $\zeta(X, T)$ contains (via the Tate conjecture) information about algebraic cycles on X, e.g., the Picard number.
- Computation of many types of exponential sums can be encoded into the problem of computing $\zeta(X, T)$ for suitable X.
- ...

L-functions as empirical data

For X a variety over a number field, its associated L-functions are Euler products derived from zeta functions of the reductions of X to various finite fields. We are also interested in computing these. Why?

- Special values of these L-functions carry arithmetic information via many conjectures (Birch–Swinnerton-Dyer, Beilinson, Deligne, etc.).
- Additional arithmetic information can be seen in the statistics of variation of Euler factors, via many conjectures (Sato-Tate, Fité–Rotger–K–Sutherland, Serre, etc.).
- These L-functions are conjecturally related to automorphic forms via the Langlands correspondence. One hopes both to collect evidence to help make precise new cases of the correspondence (e.g., genus 2 curves and Siegel modular forms), and to use existing results to compute automorphic L-functions.
- Some L-functions may have arithmetic properties reminiscent of mirror symmetry (???).

L-functions as empirical data

For X a variety over a number field, its associated L-functions are Euler products derived from zeta functions of the reductions of X to various finite fields. We are also interested in computing these. Why?

- Special values of these L-functions carry arithmetic information via many conjectures (Birch–Swinnerton-Dyer, Beilinson, Deligne, etc.).
- Additional arithmetic information can be seen in the statistics of variation of Euler factors, via many conjectures (Sato-Tate, Fité–Rotger–K–Sutherland, Serre, etc.).
- These L-functions are conjecturally related to automorphic forms via the Langlands correspondence. One hopes both to collect evidence to help make precise new cases of the correspondence (e.g., genus 2 curves and Siegel modular forms), and to use existing results to compute automorphic L-functions.
- Some L-functions may have arithmetic properties reminiscent of mirror symmetry (???).

L-functions as empirical data

For X a variety over a number field, its associated L-functions are Euler products derived from zeta functions of the reductions of X to various finite fields. We are also interested in computing these. Why?

- Special values of these L-functions carry arithmetic information via many conjectures (Birch–Swinnerton-Dyer, Beilinson, Deligne, etc.).
- Additional arithmetic information can be seen in the statistics of variation of Euler factors, via many conjectures (Sato-Tate, Fité–Rotger–K–Sutherland, Serre, etc.).
- These L-functions are conjecturally related to automorphic forms via the Langlands correspondence. One hopes both to collect evidence to help make precise new cases of the correspondence (e.g., genus 2 curves and Siegel modular forms), and to use existing results to compute automorphic L-functions.
- Some L-functions may have arithmetic properties reminiscent of mirror symmetry (???).

L-functions as empirical data

For X a variety over a number field, its associated L-functions are Euler products derived from zeta functions of the reductions of X to various finite fields. We are also interested in computing these. Why?

- Special values of these L-functions carry arithmetic information via many conjectures (Birch–Swinnerton-Dyer, Beilinson, Deligne, etc.).
- Additional arithmetic information can be seen in the statistics of variation of Euler factors, via many conjectures (Sato-Tate, Fité–Rotger–K–Sutherland, Serre, etc.).
- These L-functions are conjecturally related to automorphic forms via the Langlands correspondence. One hopes both to collect evidence to help make precise new cases of the correspondence (e.g., genus 2 curves and Siegel modular forms), and to use existing results to compute automorphic L-functions.
- Some L-functions may have arithmetic properties reminiscent of mirror symmetry (???).

L-functions as empirical data

For X a variety over a number field, its associated L-functions are Euler products derived from zeta functions of the reductions of X to various finite fields. We are also interested in computing these. Why?

- Special values of these L-functions carry arithmetic information via many conjectures (Birch–Swinnerton-Dyer, Beilinson, Deligne, etc.).
- Additional arithmetic information can be seen in the statistics of variation of Euler factors, via many conjectures (Sato-Tate, Fité–Rotger–K–Sutherland, Serre, etc.).
- These L-functions are conjecturally related to automorphic forms via the Langlands correspondence. One hopes both to collect evidence to help make precise new cases of the correspondence (e.g., genus 2 curves and Siegel modular forms), and to use existing results to compute automorphic L-functions.
- Some L-functions may have arithmetic properties reminiscent of mirror symmetry (???).

How *not* to compute a zeta function (in general)

In most cases of interest, the Weil conjectures bound the degree of $\zeta(X, T)$ in terms of Betti numbers. One can then compute $\zeta(X, T)$ by simply enumerating the sets $\#X(\mathbb{F}_{q^n})$ for enough values of n.

This is almost never practical! One can occasionally gain something by exploiting geometric information, e.g., automorphisms or correspondences which impose constraints on the factorization of $\zeta(X, T)$.

However, direct counting offers no way to leverage additional constraints on $\zeta(X, T)$ provided by the Weil conjectures, notably:

- archimedean estimates provided by the Riemann Hypothesis;
- p-adic divisibility provided by the "Newton above Hodge" property of crystalline cohomology.

How *not* to compute a zeta function (in general)

In most cases of interest, the Weil conjectures bound the degree of $\zeta(X, T)$ in terms of Betti numbers. One can then compute $\zeta(X, T)$ by simply enumerating the sets $\#X(\mathbb{F}_{q^n})$ for enough values of n.

This is almost never practical! One can occasionally gain something by exploiting geometric information, e.g., automorphisms or correspondences which impose constraints on the factorization of $\zeta(X, T)$.

However, direct counting offers no way to leverage additional constraints on $\zeta(X, T)$ provided by the Weil conjectures, notably:

- archimedean estimates provided by the Riemann Hypothesis;
- p-adic divisibility provided by the "Newton above Hodge" property of crystalline cohomology.

How *not* to compute a zeta function (in general)

In most cases of interest, the Weil conjectures bound the degree of $\zeta(X, T)$ in terms of Betti numbers. One can then compute $\zeta(X, T)$ by simply enumerating the sets $\#X(\mathbb{F}_{q^n})$ for enough values of n.

This is almost never practical! One can occasionally gain something by exploiting geometric information, e.g., automorphisms or correspondences which impose constraints on the factorization of $\zeta(X, T)$.

However, direct counting offers no way to leverage additional constraints on $\zeta(X, T)$ provided by the Weil conjectures, notably:

- archimedean estimates provided by the Riemann Hypothesis;
- p-adic divisibility provided by the "Newton above Hodge" property of crystalline cohomology.

How *not* to compute a zeta function (in general)

In most cases of interest, the Weil conjectures bound the degree of $\zeta(X, T)$ in terms of Betti numbers. One can then compute $\zeta(X, T)$ by simply enumerating the sets $\#X(\mathbb{F}_{q^n})$ for enough values of n.

This is almost never practical! One can occasionally gain something by exploiting geometric information, e.g., automorphisms or correspondences which impose constraints on the factorization of $\zeta(X, T)$.

However, direct counting offers no way to leverage additional constraints on $\zeta(X, T)$ provided by the Weil conjectures, notably:

- archimedean estimates provided by the Riemann Hypothesis;
- p-adic divisibility provided by the "Newton above Hodge" property of crystalline cohomology.

How *not* to compute a zeta function (in general)

In most cases of interest, the Weil conjectures bound the degree of $\zeta(X, T)$ in terms of Betti numbers. One can then compute $\zeta(X, T)$ by simply enumerating the sets $\#X(\mathbb{F}_{q^n})$ for enough values of n.

This is almost never practical! One can occasionally gain something by exploiting geometric information, e.g., automorphisms or correspondences which impose constraints on the factorization of $\zeta(X, T)$.

However, direct counting offers no way to leverage additional constraints on $\zeta(X, T)$ provided by the Weil conjectures, notably:

- archimedean estimates provided by the Riemann Hypothesis;
- p-adic divisibility provided by the "Newton above Hodge" property of crystalline cohomology.

Zeta functions via Weil cohomology

A *Weil cohomology theory* provides an interpretation

$$\zeta(X,T) = \prod_i \det(1 - TF_i, V_i)^{(-1)^{i+1}}$$

for some endomorphism F_i on some vector spaces V_i over some field of characteristic 0. One can try to compute $\zeta(X,T)$ using this formula.

Unfortunately, *étale cohomology* is usually[1] very hard to handle from an explicit computational point of view.

Much more progress has been made using *p-adic cohomology* in the spirit of Dwork. While there are several related approaches, we will focus on the construction of *Monsky-Washnitzer*, which has a close relationship with algebraic de Rham cohomology.

[1] One exception is curves of low genus, where one can handle it via torsion points on Jacobian varieties.

Zeta functions via Weil cohomology

A *Weil cohomology theory* provides an interpretation

$$\zeta(X, T) = \prod_i \det(1 - TF_i, V_i)^{(-1)^{i+1}}$$

for some endomorphism F_i on some vector spaces V_i over some field of characteristic 0. One can try to compute $\zeta(X, T)$ using this formula.

Unfortunately, *étale cohomology* is usually[1] very hard to handle from an explicit computational point of view.

Much more progress has been made using *p-adic cohomology* in the spirit of Dwork. While there are several related approaches, we will focus on the construction of *Monsky-Washnitzer*, which has a close relationship with algebraic de Rham cohomology.

[1]One exception is curves of low genus, where one can handle it via torsion points on Jacobian varieties.

Zeta functions via Weil cohomology

A *Weil cohomology theory* provides an interpretation

$$\zeta(X, T) = \prod_i \det(1 - TF_i, V_i)^{(-1)^{i+1}}$$

for some endomorphism F_i on some vector spaces V_i over some field of characteristic 0. One can try to compute $\zeta(X, T)$ using this formula.

Unfortunately, *étale cohomology* is usually[1] very hard to handle from an explicit computational point of view.

Much more progress has been made using *p-adic cohomology* in the spirit of Dwork. While there are several related approaches, we will focus on the construction of *Monsky-Washnitzer*, which has a close relationship with algebraic de Rham cohomology.

[1] One exception is curves of low genus, where one can handle it via torsion points on Jacobian varieties.

A paradigm for zeta functions via p-adic cohomology

Let U be a smooth affine variety over $\mathbb{Q}$ (for simplicity). For some $N > 0$, it extends to a nice scheme[2] $\mathfrak{U}$ over $\mathbb{Z}[1/N]$.

The *algebraic de Rham cohomology* $H^i_{\mathrm{dR}}(U, \mathbb{Q})$ is the cohomology of (the global sections of) the de Rham complex

$$0 \to \mathcal{O}_U \to \Omega^1_{U/\mathbb{Q}} \to \Omega^2_{U/\mathbb{Q}} \to \cdots \to \Omega^d_{U/\mathbb{Q}} \to 0 \qquad (d = \dim(U)).$$

Typically, the most interesting group occurs for $i = d$, as the other ones can be described in terms of cohomology of lower-dimensional varieties (Lefschetz hyperplane theorem).

To use $H^d_{\mathrm{dR}}(U, \mathbb{Q})$ to compute zeta functions, it is critical to have a good algorithm to *reduce pole orders at infinity* in cohomology. Physicists may have more experience with this than number theorists...

[2] i.e., a smooth proper scheme minus a relative normal crossings divisor

A paradigm for zeta functions via p-adic cohomology

Let U be a smooth affine variety over $\mathbb{Q}$ (for simplicity). For some $N > 0$, it extends to a nice scheme[2] $\mathfrak{U}$ over $\mathbb{Z}[1/N]$.

The *algebraic de Rham cohomology* $H^i_{\mathrm{dR}}(U, \mathbb{Q})$ is the cohomology of (the global sections of) the de Rham complex

$$0 \to \mathcal{O}_U \to \Omega^1_{U/\mathbb{Q}} \to \Omega^2_{U/\mathbb{Q}} \to \cdots \to \Omega^d_{U/\mathbb{Q}} \to 0 \qquad (d = \dim(U)).$$

Typically, the most interesting group occurs for $i = d$, as the other ones can be described in terms of cohomology of lower-dimensional varieties (Lefschetz hyperplane theorem).

To use $H^d_{\mathrm{dR}}(U, \mathbb{Q})$ to compute zeta functions, it is critical to have a good algorithm to *reduce pole orders at infinity* in cohomology. Physicists may have more experience with this than number theorists...

[2] i.e., a smooth proper scheme minus a relative normal crossings divisor

A paradigm for zeta functions via p-adic cohomology

Let U be a smooth affine variety over $\mathbb{Q}$ (for simplicity). For some $N > 0$, it extends to a nice scheme[2] $\mathfrak{U}$ over $\mathbb{Z}[1/N]$.

The *algebraic de Rham cohomology* $H^i_{\mathrm{dR}}(U, \mathbb{Q})$ is the cohomology of (the global sections of) the de Rham complex

$$0 \to \mathcal{O}_U \to \Omega^1_{U/\mathbb{Q}} \to \Omega^2_{U/\mathbb{Q}} \to \cdots \to \Omega^d_{U/\mathbb{Q}} \to 0 \qquad (d = \dim(U)).$$

Typically, the most interesting group occurs for $i = d$, as the other ones can be described in terms of cohomology of lower-dimensional varieties (Lefschetz hyperplane theorem).

To use $H^d_{\mathrm{dR}}(U, \mathbb{Q})$ to compute zeta functions, it is critical to have a good algorithm to *reduce pole orders at infinity* in cohomology. Physicists may have more experience with this than number theorists...

[2] i.e., a smooth proper scheme minus a relative normal crossings divisor

A paradigm for zeta functions via p-adic cohomology

Let U be a smooth affine variety over $\mathbb{Q}$ (for simplicity). For some $N > 0$, it extends to a nice scheme[2] $\mathfrak{U}$ over $\mathbb{Z}[1/N]$.

The *algebraic de Rham cohomology* $H^i_{\mathrm{dR}}(U, \mathbb{Q})$ is the cohomology of (the global sections of) the de Rham complex

$$0 \to \mathcal{O}_U \to \Omega^1_{U/\mathbb{Q}} \to \Omega^2_{U/\mathbb{Q}} \to \cdots \to \Omega^d_{U/\mathbb{Q}} \to 0 \qquad (d = \dim(U)).$$

Typically, the most interesting group occurs for $i = d$, as the other ones can be described in terms of cohomology of lower-dimensional varieties (Lefschetz hyperplane theorem).

To use $H^d_{\mathrm{dR}}(U, \mathbb{Q})$ to compute zeta functions, it is critical to have a good algorithm to *reduce pole orders at infinity* in cohomology. Physicists may have more experience with this than number theorists...

[2] i.e., a smooth proper scheme minus a relative normal crossings divisor

A paradigm for zeta functions via p-adic cohomology

Let U be a smooth affine variety over $\mathbb{Q}$ (for simplicity). For some $N > 0$, it extends to a nice scheme[2] $\mathfrak{U}$ over $\mathbb{Z}[1/N]$.

The *algebraic de Rham cohomology* $H^i_{\mathrm{dR}}(U, \mathbb{Q})$ is the cohomology of (the global sections of) the de Rham complex

$$0 \to \mathcal{O}_U \to \Omega^1_{U/\mathbb{Q}} \to \Omega^2_{U/\mathbb{Q}} \to \cdots \to \Omega^d_{U/\mathbb{Q}} \to 0 \qquad (d = \dim(U)).$$

Typically, the most interesting group occurs for $i = d$, as the other ones can be described in terms of cohomology of lower-dimensional varieties (Lefschetz hyperplane theorem).

To use $H^d_{\mathrm{dR}}(U, \mathbb{Q})$ to compute zeta functions, it is critical to have a good algorithm to *reduce pole orders at infinity* in cohomology. Physicists may have more experience with this than number theorists...

[2] i.e., a smooth proper scheme minus a relative normal crossings divisor

de Rham cohomology and zeta functions

Let p be a prime not dividing N. Then $\mathfrak{U}_p$ (the reduction mod p) has a Frobenius endomorphism which does not typically lift to $\mathfrak{U}$; but it does lift to a p-adic completion of $\mathfrak{U}$. By formally applying this action to differentials, one obtains[3] endomorphisms F_i on $H^i_{\mathrm{dR}}(U, \mathbb{Q}_p)$.

Theorem (Monsky-Washnitzer)

We have

$$\zeta(\mathfrak{U}_p, T) = \prod_{i=0}^{d} \det(1 - p^i F_i^{-1} T, H^i_{\mathrm{dR}}(U, \mathbb{Q}_p))^{(-1)^{i+1}}.$$

Using p-adic numerical arithmetic, one can compute enough coefficients of $\zeta(\mathfrak{U}_p, T)$ with enough p-adic accuracy to determine them uniquely.

[3] This part is not formal; it amounts to saying that the de Rham cohomology doesn't change when you take the completion. This fails for the usual p-adic completion, so the slightly smaller *weak completion* is needed instead.

de Rham cohomology and zeta functions

Let p be a prime not dividing N. Then $\mathfrak{U}_p$ (the reduction mod p) has a Frobenius endomorphism which does not typically lift to $\mathfrak{U}$; but it does lift to a p-adic completion of $\mathfrak{U}$. By formally applying this action to differentials, one obtains[3] endomorphisms F_i on $H^i_{\mathrm{dR}}(U, \mathbb{Q}_p)$.

Theorem (Monsky-Washnitzer)

We have

$$\zeta(\mathfrak{U}_p, T) = \prod_{i=0}^{d} \det(1 - p^i F_i^{-1} T, H^i_{\mathrm{dR}}(U, \mathbb{Q}_p))^{(-1)^{i+1}}.$$

Using p-adic numerical arithmetic, one can compute enough coefficients of $\zeta(\mathfrak{U}_p, T)$ with enough p-adic accuracy to determine them uniquely.

[3] This part is not formal; it amounts to saying that the de Rham cohomology doesn't change when you take the completion. This fails for the usual p-adic completion, so the slightly smaller *weak completion* is needed instead.

de Rham cohomology and zeta functions

Let p be a prime not dividing N. Then $\mathfrak{U}_p$ (the reduction mod p) has a Frobenius endomorphism which does not typically lift to $\mathfrak{U}$; but it does lift to a p-adic completion of $\mathfrak{U}$. By formally applying this action to differentials, one obtains[3] endomorphisms F_i on $H^i_{\mathrm{dR}}(U, \mathbb{Q}_p)$.

Theorem (Monsky-Washnitzer)

We have

$$\zeta(\mathfrak{U}_p, T) = \prod_{i=0}^{d} \det(1 - p^i F_i^{-1} T, H^i_{\mathrm{dR}}(U, \mathbb{Q}_p))^{(-1)^{i+1}}.$$

Using p-adic numerical arithmetic, one can compute enough coefficients of $\zeta(\mathfrak{U}_p, T)$ with enough p-adic accuracy to determine them uniquely.

[3] This part is not formal; it amounts to saying that the de Rham cohomology doesn't change when you take the completion. This fails for the usual p-adic completion, so the slightly smaller *weak completion* is needed instead.

Hyperelliptic curves (K, 2001)

For example, let $P \in \mathbb{Q}[x]$ be a polynomial of degree $2g+1$ with no repeated roots, and put

$$U = \operatorname{Spec} \mathbb{Q}[x,y,z]/(y^2 - P(x), yz - 1).$$

Then for $\pm$ the eigenspaces of the involution $y \mapsto -y$,

$$\begin{aligned} H^1_{\mathrm{dR}}(U, \mathbb{Q}) &= H^1_{\mathrm{dR}}(U, \mathbb{Q})^+ \oplus H^1_{\mathrm{dR}}(U, \mathbb{Q})^- \\ &= \left(\bigoplus_{i=0}^{2g} \mathbb{Q} \frac{dx}{y^2} \right) \oplus \left(\bigoplus_{i=0}^{2g-1} \mathbb{Q} \frac{dx}{y} \right). \end{aligned}$$

It is easy to produce relations in $H^1_{\mathrm{dR}}(U, \mathbb{Q})$ to reduce pole orders, e.g.,

$$\frac{(A(x)P(x) + B(x)P'(x))dx}{y^{2n+1}} \equiv \frac{A(x)\,dx}{y^{2n-1}} + \frac{2B'(x)\,dx}{(2n-1)y^{2n-1}}$$

$$0 \equiv \frac{(2dx^{d-1}P(x) + x^d P'(x))\,dx}{(2d+2g+1)y} = \frac{(x^{d+2g} + \cdots)dx}{y}.$$

Hyperelliptic curves (K, 2001)

For example, let $P \in \mathbb{Q}[x]$ be a polynomial of degree $2g+1$ with no repeated roots, and put

$$U = \operatorname{Spec} \mathbb{Q}[x,y,z]/(y^2 - P(x), yz - 1).$$

Then for $\pm$ the eigenspaces of the involution $y \mapsto -y$,

$$\begin{aligned} H^1_{\mathrm{dR}}(U, \mathbb{Q}) &= H^1_{\mathrm{dR}}(U, \mathbb{Q})^+ \oplus H^1_{\mathrm{dR}}(U, \mathbb{Q})^- \\ &= \left(\bigoplus_{i=0}^{2g} \mathbb{Q} \frac{dx}{y^2} \right) \oplus \left(\bigoplus_{i=0}^{2g-1} \mathbb{Q} \frac{dx}{y} \right). \end{aligned}$$

It is easy to produce relations in $H^1_{\mathrm{dR}}(U, \mathbb{Q})$ to reduce pole orders, e.g.,

$$\frac{(A(x)P(x) + B(x)P'(x))dx}{y^{2n+1}} \equiv \frac{A(x)\,dx}{y^{2n-1}} + \frac{2B'(x)\,dx}{(2n-1)y^{2n-1}}$$

$$0 \equiv \frac{(2dx^{d-1}P(x) + x^d P'(x))\,dx}{(2d+2g+1)y} = \frac{(x^{d+2g} + \cdots)dx}{y}.$$

Hyperelliptic curves (K, 2001)

For example, let $P \in \mathbb{Q}[x]$ be a polynomial of degree $2g+1$ with no repeated roots, and put

$$U = \operatorname{Spec} \mathbb{Q}[x,y,z]/(y^2 - P(x), yz - 1).$$

Then for $\pm$ the eigenspaces of the involution $y \mapsto -y$,

$$\begin{aligned} H^1_{\mathrm{dR}}(U, \mathbb{Q}) &= H^1_{\mathrm{dR}}(U, \mathbb{Q})^+ \oplus H^1_{\mathrm{dR}}(U, \mathbb{Q})^- \\ &= \left(\bigoplus_{i=0}^{2g} \mathbb{Q} \frac{dx}{y^2} \right) \oplus \left(\bigoplus_{i=0}^{2g-1} \mathbb{Q} \frac{dx}{y} \right). \end{aligned}$$

It is easy to produce relations in $H^1_{\mathrm{dR}}(U, \mathbb{Q})$ to reduce pole orders, e.g.,

$$\frac{(A(x)P(x) + B(x)P'(x))dx}{y^{2n+1}} \equiv \frac{A(x)\,dx}{y^{2n-1}} + \frac{2B'(x)\,dx}{(2n-1)y^{2n-1}}$$

$$0 \equiv \frac{(2dx^{d-1}P(x) + x^d P'(x))\,dx}{(2d+2g+1)y} = \frac{(x^{d+2g} + \cdots)dx}{y}.$$

Hyperelliptic curves (K, 2001)

For example, let $P \in \mathbb{Q}[x]$ be a polynomial of degree $2g+1$ with no repeated roots, and put

$$U = \operatorname{Spec} \mathbb{Q}[x,y,z]/(y^2 - P(x), yz - 1).$$

Then for $\pm$ the eigenspaces of the involution $y \mapsto -y$,

$$\begin{aligned} H^1_{\mathrm{dR}}(U, \mathbb{Q}) &= H^1_{\mathrm{dR}}(U, \mathbb{Q})^+ \oplus H^1_{\mathrm{dR}}(U, \mathbb{Q})^- \\ &= \left(\bigoplus_{i=0}^{2g} \mathbb{Q} \frac{dx}{y^2} \right) \oplus \left(\bigoplus_{i=0}^{2g-1} \mathbb{Q} \frac{dx}{y} \right). \end{aligned}$$

It is easy to produce relations in $H^1_{\mathrm{dR}}(U, \mathbb{Q})$ to reduce pole orders, e.g.,

$$\frac{(A(x)P(x) + B(x)P'(x))dx}{y^{2n+1}} \equiv \frac{A(x)\,dx}{y^{2n-1}} + \frac{2B'(x)\,dx}{(2n-1)y^{2n-1}}$$

$$0 \equiv \frac{(2dx^{d-1}P(x) + x^d P'(x))\,dx}{(2d+2g+1)y} = \frac{(x^{d+2g} + \cdots)dx}{y}.$$

Hyperelliptic curves (K, 2001)

For example, let $P \in \mathbb{Q}[x]$ be a polynomial of degree $2g+1$ with no repeated roots, and put

$$U = \operatorname{Spec} \mathbb{Q}[x,y,z]/(y^2 - P(x), yz - 1).$$

Then for $\pm$ the eigenspaces of the involution $y \mapsto -y$,

$$\begin{aligned} H^1_{\mathrm{dR}}(U,\mathbb{Q}) &= H^1_{\mathrm{dR}}(U,\mathbb{Q})^+ \oplus H^1_{\mathrm{dR}}(U,\mathbb{Q})^- \\ &= \left(\bigoplus_{i=0}^{2g} \mathbb{Q} \frac{dx}{y^2} \right) \oplus \left(\bigoplus_{i=0}^{2g-1} \mathbb{Q} \frac{dx}{y} \right). \end{aligned}$$

It is easy to produce relations in $H^1_{\mathrm{dR}}(U,\mathbb{Q})$ to reduce pole orders, e.g.,

$$\frac{(A(x)P(x) + B(x)P'(x))dx}{y^{2n+1}} \equiv \frac{A(x)\,dx}{y^{2n-1}} + \frac{2B'(x)\,dx}{(2n-1)y^{2n-1}}$$

$$0 \equiv \frac{(2dx^{d-1}P(x) + x^d P'(x))\,dx}{(2d+2g+1)y} = \frac{(x^{d+2g} + \cdots)dx}{y}.$$

Hyperelliptic curves (continued)

One constructs a Frobenius lift by declaring that x maps to x^p; the image of y must then be y^p times the square root of $P(x^p)/P(x)^p$ congruent to 1 modulo p, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then (up to a suitably small p-adic error, in order to make the computation finite and tractable) apply this Frobenius lift formally to each basis differential of $H^i_{\mathrm{dR}}(U, \mathbb{Q})$, reduce pole orders to get the matrix of action of Frobenius, and read off $\zeta(U, T)$. This is extremely efficient in practice! (Implementations exist in MAGMA, SAGE.)

With some extra effort, one can treat more general hyperelliptic curves, including characteristic 2 (Harrison, Denef-Vercauteren).

In fact, it should be possible to make this method possible and practical for arbitrary curves! An approach has recently been proposed by Tuitman, who is also working on an implementation.

Hyperelliptic curves (continued)

One constructs a Frobenius lift by declaring that x maps to x^p; the image of y must then be y^p times the square root of $P(x^p)/P(x)^p$ congruent to 1 modulo p, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then (up to a suitably small p-adic error, in order to make the computation finite and tractable) apply this Frobenius lift formally to each basis differential of $H^i_{\mathrm{dR}}(U, \mathbb{Q})$, reduce pole orders to get the matrix of action of Frobenius, and read off $\zeta(U, T)$. This is extremely efficient in practice! (Implementations exist in MAGMA, SAGE.)

With some extra effort, one can treat more general hyperelliptic curves, including characteristic 2 (Harrison, Denef-Vercauteren).

In fact, it should be possible to make this method possible and practical for arbitrary curves! An approach has recently been proposed by Tuitman, who is also working on an implementation.

Hyperelliptic curves (continued)

One constructs a Frobenius lift by declaring that x maps to x^p; the image of y must then be y^p times the square root of $P(x^p)/P(x)^p$ congruent to 1 modulo p, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then (up to a suitably small p-adic error, in order to make the computation finite and tractable) apply this Frobenius lift formally to each basis differential of $H^i_{\mathrm{dR}}(U, \mathbb{Q})$, reduce pole orders to get the matrix of action of Frobenius, and read off $\zeta(U, T)$. This is extremely efficient in practice! (Implementations exist in MAGMA, SAGE.)

With some extra effort, one can treat more general hyperelliptic curves, including characteristic 2 (Harrison, Denef-Vercauteren).

In fact, it should be possible to make this method possible and practical for arbitrary curves! An approach has recently been proposed by Tuitman, who is also working on an implementation.

Hyperelliptic curves (continued)

One constructs a Frobenius lift by declaring that x maps to x^p; the image of y must then be y^p times the square root of $P(x^p)/P(x)^p$ congruent to 1 modulo p, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then (up to a suitably small p-adic error, in order to make the computation finite and tractable) apply this Frobenius lift formally to each basis differential of $H^i_{\mathrm{dR}}(U, \mathbb{Q})$, reduce pole orders to get the matrix of action of Frobenius, and read off $\zeta(U, T)$. This is extremely efficient in practice! (Implementations exist in MAGMA, SAGE.)

With some extra effort, one can treat more general hyperelliptic curves, including characteristic 2 (Harrison, Denef-Vercauteren).

In fact, it should be possible to make this method possible and practical for arbitrary curves! An approach has recently been proposed by Tuitman, who is also working on an implementation.

Smooth hypersurfaces in $\mathbb{P}^n$ (Abbott-K-Roe, 2009)

Let $f \in \mathbb{Q}[x_0, \dots, x_n]$ be a homogeneous polynomial of degree d cutting out a smooth hypersurface. Its complement is

$$U = \operatorname{Spec} \mathbb{Q}[x_0, \dots, x_n, f^{-1}]_0.$$

It is convenient to write differentials as degree 0 multiples of

$$\Omega = \sum_{i=0}^{n} (-1)^i x_i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n.$$

The reduction of pole orders is due to Griffiths-Dwork, using relations

$$\frac{\partial_i g}{f^m}\Omega \cong m \frac{g(\partial_i f)}{f^{m+1}}\Omega, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

In particular, one can construct a basis of $H^n_{\mathrm{dR}}(U, \mathbb{Q})$ consisting of forms of the shape $g\Omega/f^i$ for $i \in \{1, \dots, n\}$.

Smooth hypersurfaces in $\mathbb{P}^n$ (Abbott-K-Roe, 2009)

Let $f \in \mathbb{Q}[x_0, \dots, x_n]$ be a homogeneous polynomial of degree d cutting out a smooth hypersurface. Its complement is

$$U = \operatorname{Spec} \mathbb{Q}[x_0, \dots, x_n, f^{-1}]_0.$$

It is convenient to write differentials as degree 0 multiples of

$$\Omega = \sum_{i=0}^{n} (-1)^i x_i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n.$$

The reduction of pole orders is due to Griffiths-Dwork, using relations

$$\frac{\partial_i g}{f^m} \Omega \cong m \frac{g(\partial_i f)}{f^{m+1}} \Omega, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

In particular, one can construct a basis of $H^n_{\mathrm{dR}}(U, \mathbb{Q})$ consisting of forms of the shape $g\Omega/f^i$ for $i \in \{1, \dots, n\}$.

Smooth hypersurfaces in $\mathbb{P}^n$ (Abbott-K-Roe, 2009)

Let $f \in \mathbb{Q}[x_0, \dots, x_n]$ be a homogeneous polynomial of degree d cutting out a smooth hypersurface. Its complement is

$$U = \operatorname{Spec} \mathbb{Q}[x_0, \dots, x_n, f^{-1}]_0.$$

It is convenient to write differentials as degree 0 multiples of

$$\Omega = \sum_{i=0}^{n} (-1)^i x_i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n.$$

The reduction of pole orders is due to Griffiths-Dwork, using relations

$$\frac{\partial_i g}{f^m} \Omega \cong m \frac{g(\partial_i f)}{f^{m+1}} \Omega, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

In particular, one can construct a basis of $H^n_{\mathrm{dR}}(U, \mathbb{Q})$ consisting of forms of the shape $g\Omega/f^i$ for $i \in \{1, \dots, n\}$.

Smooth hypersurfaces in $\mathbb{P}^n$ (Abbott-K-Roe, 2009)

Let $f \in \mathbb{Q}[x_0, \dots, x_n]$ be a homogeneous polynomial of degree d cutting out a smooth hypersurface. Its complement is

$$U = \operatorname{Spec} \mathbb{Q}[x_0, \dots, x_n, f^{-1}]_0.$$

It is convenient to write differentials as degree 0 multiples of

$$\Omega = \sum_{i=0}^{n} (-1)^i x_i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n.$$

The reduction of pole orders is due to Griffiths-Dwork, using relations

$$\frac{\partial_i g}{f^m} \Omega \cong m \frac{g(\partial_i f)}{f^{m+1}} \Omega, \qquad \partial_i = \frac{\partial}{\partial x_i}.$$

In particular, one can construct a basis of $H^n_{\mathrm{dR}}(U, \mathbb{Q})$ consisting of forms of the shape $g\Omega/f^i$ for $i \in \{1, \dots, n\}$.

Smooth hypersurfaces in $\mathbb{P}^n$ (continued)

One constructs a Frobenius lift by declaring that x_i maps to x_i^p for $i = 0, \dots, d$; the image of f^{-1} must then be f^{-p} times the reciprocal of $f(x^p)/f(x)^p$, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then proceed as for hyperelliptic curves. However, a crude implementation of this idea (as in AKR, 2009) only yields practical results in a few small cases (e.g., $n = 3$, $d = 4$, $p < 20$).

A much better organization of the reduction process has been proposed by Harvey. Using this idea, Costa was able to calculate examples with $n = 3$, $d = 4$, $p < 2^{16}$.

Using similar methods, Costa also succeeded in computing a few examples with $n = 4, d = 5, p < 20$ in the Dwork pencil of quintic threefolds.

It is unclear how to make this method practical for arbitrary surfaces and threefolds. Instead, we focus on an easy generalization that will handle many new families of K3 surfaces and CY threefolds.

Smooth hypersurfaces in $\mathbb{P}^n$ (continued)

One constructs a Frobenius lift by declaring that x_i maps to x_i^p for $i = 0, \dots, d$; the image of f^{-1} must then be f^{-p} times the reciprocal of $f(x^p)/f(x)^p$, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then proceed as for hyperelliptic curves. However, a crude implementation of this idea (as in AKR, 2009) only yields practical results in a few small cases (e.g., $n = 3$, $d = 4$, $p < 20$).

A much better organization of the reduction process has been proposed by Harvey. Using this idea, Costa was able to calculate examples with $n = 3$, $d = 4$, $p < 2^{16}$.

Using similar methods, Costa also succeeded in computing a few examples with $n = 4, d = 5, p < 20$ in the Dwork pencil of quintic threefolds.

It is unclear how to make this method practical for arbitrary surfaces and threefolds. Instead, we focus on an easy generalization that will handle many new families of K3 surfaces and CY threefolds.

Smooth hypersurfaces in $\mathbb{P}^n$ (continued)

One constructs a Frobenius lift by declaring that x_i maps to x_i^p for $i = 0, \dots, d$; the image of f^{-1} must then be f^{-p} times the reciprocal of $f(x^p)/f(x)^p$, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then proceed as for hyperelliptic curves. However, a crude implementation of this idea (as in AKR, 2009) only yields practical results in a few small cases (e.g., $n = 3$, $d = 4$, $p < 20$).

A much better organization of the reduction process has been proposed by Harvey. Using this idea, Costa was able to calculate examples with $n = 3$, $d = 4$, $p < 2^{16}$.

Using similar methods, Costa also succeeded in computing a few examples with $n = 4, d = 5, p < 20$ in the Dwork pencil of quintic threefolds.

It is unclear how to make this method practical for arbitrary surfaces and threefolds. Instead, we focus on an easy generalization that will handle many new families of K3 surfaces and CY threefolds.

Smooth hypersurfaces in $\mathbb{P}^n$ (continued)

One constructs a Frobenius lift by declaring that x_i maps to x_i^p for $i = 0, \dots, d$; the image of f^{-1} must then be f^{-p} times the reciprocal of $f(x^p)/f(x)^p$, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then proceed as for hyperelliptic curves. However, a crude implementation of this idea (as in AKR, 2009) only yields practical results in a few small cases (e.g., $n = 3$, $d = 4$, $p < 20$).

A much better organization of the reduction process has been proposed by Harvey. Using this idea, Costa was able to calculate examples with $n = 3$, $d = 4$, $p < 2^{16}$.

Using similar methods, Costa also succeeded in computing a few examples with $n = 4, d = 5, p < 20$ in the Dwork pencil of quintic threefolds.

It is unclear how to make this method practical for arbitrary surfaces and threefolds. Instead, we focus on an easy generalization that will handle many new families of K3 surfaces and CY threefolds.

Smooth hypersurfaces in $\mathbb{P}^n$ (continued)

One constructs a Frobenius lift by declaring that x_i maps to x_i^p for $i = 0, \dots, d$; the image of f^{-1} must then be f^{-p} times the reciprocal of $f(x^p)/f(x)^p$, in the (weak) p-adic completion of $\mathcal{O}(\mathfrak{U})$.

One can then proceed as for hyperelliptic curves. However, a crude implementation of this idea (as in AKR, 2009) only yields practical results in a few small cases (e.g., $n = 3$, $d = 4$, $p < 20$).

A much better organization of the reduction process has been proposed by Harvey. Using this idea, Costa was able to calculate examples with $n = 3$, $d = 4$, $p < 2^{16}$.

Using similar methods, Costa also succeeded in computing a few examples with $n = 4, d = 5, p < 20$ in the Dwork pencil of quintic threefolds.

It is unclear how to make this method practical for arbitrary surfaces and threefolds. Instead, we focus on an easy generalization that will handle many new families of K3 surfaces and CY threefolds.

Toric varieties

Let Δ be a polytope with vertices in $\mathbb{Q}^n$ and choose a lattice $L \subset \mathbb{Q}^n$. We may then define a (projective, normal) toric variety X carrying an ample line bundle $\mathcal{O}(1)$ such that for $n = 0, 1, \ldots$, $\Gamma(X, \mathcal{O}(n))$ is the $\mathbb{Q}$-span of $L \cap n\Delta$. In particular, X contains an open dense torus[4] $T = \operatorname{Spec} \mathbb{Q}[L]$ which acts on X, and X admits a locally closed stratification by T-orbits.

For example, if Δ is the standard unit simplex (whose vertices are 0 and the standard basis) and $L = \mathbb{Z}^n$, then $X = \mathbb{P}^n$ with the usual $\mathcal{O}(1)$.

More generally, for any positive integers $a_0, \ldots, a_n$, if we keep the same Δ but take $L = (a_1/a_0)\mathbb{Z} + \cdots + (a_n/a_0)\mathbb{Z}$, we get the weighted projective space $\mathbb{P}^n(a_0, \ldots, a_n)$.

[4] By fixing a basis of L, we can write $\mathbb{Q}[L] \cong \mathbb{Q}[x_1^{\pm}, \ldots, x_n^{\pm}]$.

Toric varieties

Let Δ be a polytope with vertices in $\mathbb{Q}^n$ and choose a lattice $L \subset \mathbb{Q}^n$. We may then define a (projective, normal) toric variety X carrying an ample line bundle $\mathcal{O}(1)$ such that for $n = 0, 1, \ldots$, $\Gamma(X, \mathcal{O}(n))$ is the $\mathbb{Q}$-span of $L \cap n\Delta$. In particular, X contains an open dense torus[4] $T = \operatorname{Spec} \mathbb{Q}[L]$ which acts on X, and X admits a locally closed stratification by T-orbits.

For example, if Δ is the standard unit simplex (whose vertices are 0 and the standard basis) and $L = \mathbb{Z}^n$, then $X = \mathbb{P}^n$ with the usual $\mathcal{O}(1)$.

More generally, for any positive integers $a_0, \ldots, a_n$, if we keep the same Δ but take $L = (a_1/a_0)\mathbb{Z} + \cdots + (a_n/a_0)\mathbb{Z}$, we get the weighted projective space $\mathbb{P}^n(a_0, \ldots, a_n)$.

[4] By fixing a basis of L, we can write $\mathbb{Q}[L] \cong \mathbb{Q}[x_1^\pm, \ldots, x_n^\pm]$.

Toric varieties

Let Δ be a polytope with vertices in $\mathbb{Q}^n$ and choose a lattice $L \subset \mathbb{Q}^n$. We may then define a (projective, normal) toric variety X carrying an ample line bundle $\mathcal{O}(1)$ such that for $n = 0, 1, \dots$, $\Gamma(X, \mathcal{O}(n))$ is the $\mathbb{Q}$-span of $L \cap n\Delta$. In particular, X contains an open dense torus[4] $T = \operatorname{Spec} \mathbb{Q}[L]$ which acts on X, and X admits a locally closed stratification by T-orbits.

For example, if Δ is the standard unit simplex (whose vertices are 0 and the standard basis) and $L = \mathbb{Z}^n$, then $X = \mathbb{P}^n$ with the usual $\mathcal{O}(1)$.

More generally, for any positive integers $a_0, \dots, a_n$, if we keep the same Δ but take $L = (a_1/a_0)\mathbb{Z} + \cdots + (a_n/a_0)\mathbb{Z}$, we get the weighted projective space $\mathbb{P}^n(a_0, \dots, a_n)$.

[4] By fixing a basis of L, we can write $\mathbb{Q}[L] \cong \mathbb{Q}[x_1^{\pm}, \dots, x_n^{\pm}]$.

Examples of interesting toric hypersurfaces

By a result of Reid, there are 95 different polytopes Δ for which the generic section of $\mathcal{O}(1)$ in X is a K3 surface. This list can also be found in Yonamura [Tôhoku, 1990] or this online database (with codimension=1):

`http://www.grdb.co.uk/forms/k3`

By an analogous calculation of Kreuzer–Sisask–Skarke, there are 7555 different polytopes Δ for which the generic section of $\mathcal{O}(1)$ in X is a CY threefold. This list can be seen by querying:

`http://www.grdb.co.uk/forms/cy3hsf`

Examples of interesting toric hypersurfaces

By a result of Reid, there are 95 different polytopes Δ for which the generic section of $\mathcal{O}(1)$ in X is a K3 surface. This list can also be found in Yonamura [Tôhoku, 1990] or this online database (with codimension=1):

`http://www.grdb.co.uk/forms/k3`

By an analogous calculation of Kreuzer–Sisask–Skarke, there are 7555 different polytopes Δ for which the generic section of $\mathcal{O}(1)$ in X is a CY threefold. This list can be seen by querying:

`http://www.grdb.co.uk/forms/cy3hsf`

Nondegenerate hypersurfaces

We say $f \in \mathbb{Q}[L]$, or the hypersurface Z it cuts out, is *nondegenerate* if Z has transverse intersection with each T-orbit. This condition holds generically, and is easy to test on a computer.

For f nondegenerate and $U = T - Z$, there is a simple analogue[5] of the Griffiths-Dwork reduction process for computing $H^n_{\mathrm{dR}}(U, \mathbb{Q})$: for any $\mathbb{Q}[L] \cong \mathbb{Q}[x_1^{\pm}, \dots, x_n^{\pm}]$, $\Omega^n_{U/\mathbb{Q}}$ is generated by

$$\omega = (dx_1/x_1) \wedge \cdots \wedge (dx_n/x_n)$$

and for any derivation $\partial = i_1 \frac{\partial}{\partial x_1} + \cdots + i_n \frac{\partial}{\partial x_n}$ we have relations[6]

$$\frac{gf}{f^{m+1}}\omega \cong \frac{g}{f^m}\omega, \qquad \frac{g\partial(f)}{f^{m+1}}\omega \cong \frac{\partial g}{mf^m}\omega.$$

[5] Not a generalization per se, as we ignore hypersurfaces which are smooth but not nondegenerate. These can be handled, but with much extra complexity.

[6] Conveniently, these reductions preserve logarithmic singularities on $X - T$.

Nondegenerate hypersurfaces

We say $f \in \mathbb{Q}[L]$, or the hypersurface Z it cuts out, is *nondegenerate* if Z has transverse intersection with each T-orbit. This condition holds generically, and is easy to test on a computer.

For f nondegenerate and $U = T - Z$, there is a simple analogue[5] of the Griffiths-Dwork reduction process for computing $H^n_{\mathrm{dR}}(U, \mathbb{Q})$: for any $\mathbb{Q}[L] \cong \mathbb{Q}[x_1^\pm, \ldots, x_n^\pm]$, $\Omega^n_{U/\mathbb{Q}}$ is generated by

$$\omega = (dx_1/x_1) \wedge \cdots \wedge (dx_n/x_n)$$

and for any derivation $\partial = i_1 \frac{\partial}{\partial x_1} + \cdots + i_n \frac{\partial}{\partial x_n}$ we have relations[6]

$$\frac{gf}{f^{m+1}}\omega \cong \frac{g}{f^m}\omega, \qquad \frac{g\partial(f)}{f^{m+1}}\omega \cong \frac{\partial g}{mf^m}\omega.$$

[5] Not a generalization per se, as we ignore hypersurfaces which are smooth but not nondegenerate. These can be handled, but with much extra complexity.

[6] Conveniently, these reductions preserve logarithmic singularities on $X - T$.

Nondegenerate hypersurfaces

We say $f \in \mathbb{Q}[L]$, or the hypersurface Z it cuts out, is *nondegenerate* if Z has transverse intersection with each T-orbit. This condition holds generically, and is easy to test on a computer.

For f nondegenerate and $U = T - Z$, there is a simple analogue[5] of the Griffiths-Dwork reduction process for computing $H^n_{\mathrm{dR}}(U, \mathbb{Q})$: for any $\mathbb{Q}[L] \cong \mathbb{Q}[x_1^{\pm}, \dots, x_n^{\pm}]$, $\Omega^n_{U/\mathbb{Q}}$ is generated by

$$\omega = (dx_1/x_1) \wedge \cdots \wedge (dx_n/x_n)$$

and for any derivation $\partial = i_1 \frac{\partial}{\partial x_1} + \cdots + i_n \frac{\partial}{\partial x_n}$ we have relations[6]

$$\frac{gf}{f^{m+1}}\omega \cong \frac{g}{f^m}\omega, \qquad \frac{g\partial(f)}{f^{m+1}}\omega \cong \frac{\partial g}{mf^m}\omega.$$

[5] Not a generalization per se, as we ignore hypersurfaces which are smooth but not nondegenerate. These can be handled, but with much extra complexity.

[6] Conveniently, these reductions preserve logarithmic singularities on $X - T$.

Nondegenerate hypersurfaces

We say $f \in \mathbb{Q}[L]$, or the hypersurface Z it cuts out, is *nondegenerate* if Z has transverse intersection with each T-orbit. This condition holds generically, and is easy to test on a computer.

For f nondegenerate and $U = T - Z$, there is a simple analogue[5] of the Griffiths-Dwork reduction process for computing $H^n_{\mathrm{dR}}(U, \mathbb{Q})$: for any $\mathbb{Q}[L] \cong \mathbb{Q}[x_1^{\pm}, \dots, x_n^{\pm}]$, $\Omega^n_{U/\mathbb{Q}}$ is generated by

$$\omega = (dx_1/x_1) \wedge \cdots \wedge (dx_n/x_n)$$

and for any derivation $\partial = i_1 \frac{\partial}{\partial x_1} + \cdots + i_n \frac{\partial}{\partial x_n}$ we have relations[6]

$$\frac{gf}{f^{m+1}}\omega \cong \frac{g}{f^m}\omega, \qquad \frac{g\partial(f)}{f^{m+1}}\omega \cong \frac{\partial g}{mf^m}\omega.$$

[5]Not a generalization per se, as we ignore hypersurfaces which are smooth but not nondegenerate. These can be handled, but with much extra complexity.

[6]Conveniently, these reductions preserve logarithmic singularities on $X - T$.

Controlled reduction for nondegenerate hypersurfaces

In the context of computing zeta functions, one needs to apply a reduction process to forms generated by applying Frobenius. These turn out to be quite sparse!

By doing some extra linear algebra, we can construct extra relations which can be used to perform *controlled reduction*, in which sparseness is preserved: any form supported on a translate of $n\Delta$ reduces to another such form.

This is inspired by some related work of Harvey, who in the case of hyperelliptic curves obtained additional optimizations for the problem of computing L-functions (i.e., starting with a given U and reducing modulo many different primes). These optimizations are possible here too.

Controlled reduction for nondegenerate hypersurfaces

In the context of computing zeta functions, one needs to apply a reduction process to forms generated by applying Frobenius. These turn out to be quite sparse!

By doing some extra linear algebra, we can construct extra relations which can be used to perform *controlled reduction*, in which sparseness is preserved: any form supported on a translate of $n\Delta$ reduces to another such form.

This is inspired by some related work of Harvey, who in the case of hyperelliptic curves obtained additional optimizations for the problem of computing L-functions (i.e., starting with a given U and reducing modulo many different primes). These optimizations are possible here too.

Controlled reduction for nondegenerate hypersurfaces

In the context of computing zeta functions, one needs to apply a reduction process to forms generated by applying Frobenius. These turn out to be quite sparse!

By doing some extra linear algebra, we can construct extra relations which can be used to perform *controlled reduction*, in which sparseness is preserved: any form supported on a translate of $n\Delta$ reduces to another such form.

This is inspired by some related work of Harvey, who in the case of hyperelliptic curves obtained additional optimizations for the problem of computing L-functions (i.e., starting with a given U and reducing modulo many different primes). These optimizations are possible here too.

To come...

Costa–Harvey–K have developed an algorithm to compute zeta functions of nondegenerate toric hypersurfaces, following the above framework. The preceding examples of Costa are special cases of this. (Harvey has also implemented the case of plane quartics.)

Project for ICERM, fall 2015: implement this in some cases (e.g., for Δ a simplex), then generate interesting examples!

Possible followup: do something similar for complete intersections in toric varieties.

Are there other cases of pressing interest? Please let me know...

To come...

Costa–Harvey–K have developed an algorithm to compute zeta functions of nondegenerate toric hypersurfaces, following the above framework. The preceding examples of Costa are special cases of this. (Harvey has also implemented the case of plane quartics.)

Project for ICERM, fall 2015: implement this in some cases (e.g., for Δ a simplex), then generate interesting examples!

Possible followup: do something similar for complete intersections in toric varieties.

Are there other cases of pressing interest? Please let me know...

To come...

Costa–Harvey–K have developed an algorithm to compute zeta functions of nondegenerate toric hypersurfaces, following the above framework. The preceding examples of Costa are special cases of this. (Harvey has also implemented the case of plane quartics.)

Project for ICERM, fall 2015: implement this in some cases (e.g., for Δ a simplex), then generate interesting examples!

Possible followup: do something similar for complete intersections in toric varieties.

Are there other cases of pressing interest? Please let me know...

To come...

Costa–Harvey–K have developed an algorithm to compute zeta functions of nondegenerate toric hypersurfaces, following the above framework. The preceding examples of Costa are special cases of this. (Harvey has also implemented the case of plane quartics.)

Project for ICERM, fall 2015: implement this in some cases (e.g., for Δ a simplex), then generate interesting examples!

Possible followup: do something similar for complete intersections in toric varieties.

Are there other cases of pressing interest? Please let me know...