Computing L-functions

Edgar Costa (MIT)

November 12, 2024, Murmurations in Arithmetic Geometry and Related Topics
Slides available at edgarcosta.org under Talks

Riemann zeta function: the prototypical L-function

$$\zeta(s = x + iy) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$

$$= \left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \cdots = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}$$

Riemann zeta function: the prototypical L-function

$$\zeta(s = x + iy) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$
$$= \left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \cdots = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}$$

Used by Chebyshev to study the distribution of primes.

The formula above works for $x > 1$, e.g., $\zeta(2) = \sum_{n \geq 1} \frac{1}{n^2} = \pi^2/6$.

Riemann was the first to consider it as a complex function and showed it has meromorphic continuation to $\mathbb{C}$.

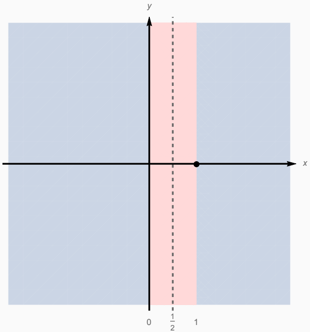
Riemann zeta function functional equation

$$\zeta(s = x + iy) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}, \qquad \Re(s) > 1$$

Functional equation relates $s \leftrightarrow 1 - s$

$$\zeta(s) = \Gamma_\zeta(s)\zeta(1 - s)$$

Riemann showed $\zeta(s) = 0 \Leftrightarrow \begin{cases} s = -2n \; n \in \mathbb{N} \\ 0 < \Re(s) < 1 \end{cases}$



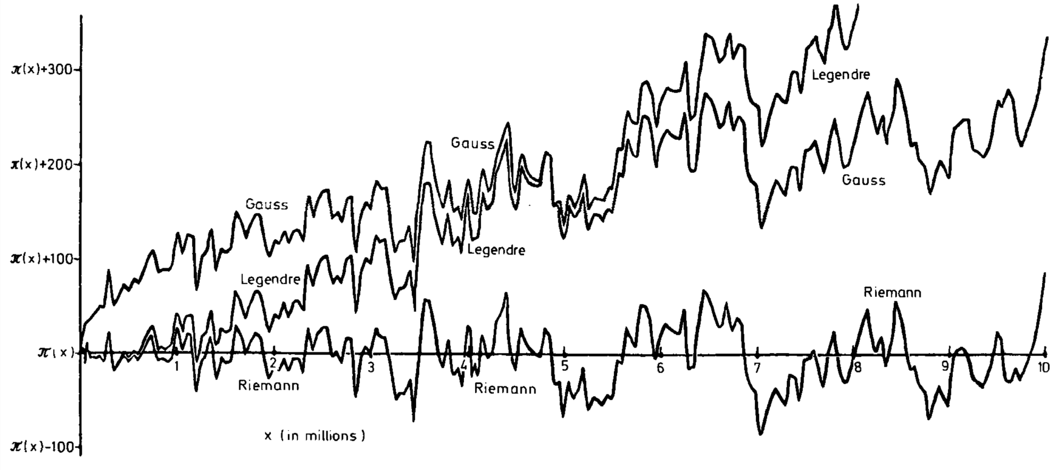
Riemann hypothesis

$\zeta(s) = 0$ and $0 < \Re(s) < 1 \Longrightarrow \Re(s) = 1/2$

One of the Millennium Prize Problems.

The roots $\zeta(s)$ describe the distribution of the primes.

Comparison by Zagier (1977)



$$x/(\log x - 1.08366) \quad \text{vs} \quad \mathrm{li}(x) \quad \text{vs} \quad R_0(x)$$

Rational L-functions

- Euler products $L(s) = \prod_p F_p(p^{-s})^{-1}$ with

$$F_p(t) = 1 - a_p t + \cdots \in \mathbb{Z}[t] \text{ and } \deg F_p(t) \leq d$$

Rational L-functions

- Euler products $L(s) = \prod_p F_p(p^{-s})^{-1}$ with

$$F_p(t) = 1 - a_p t + \cdots \in \mathbb{Z}[t] \text{ and } \deg F_p(t) \leq d$$

- $\Rightarrow$ Dirichlet series

$$L(s) = \sum_{n \geq 1} a_n n^{-s} \text{ where } a_{nm} = a_n a_m \text{ if } gcd(n, m) = 1$$

  Enough to know a_{p^n} to deduce the rest, for p a prime number.

Rational L-functions

- Euler products $L(s) = \prod_p F_p(p^{-s})^{-1}$ with

$$F_p(t) = 1 - a_p t + \cdots \in \mathbb{Z}[t] \text{ and } \deg F_p(t) \leq d$$

- $\Rightarrow$ Dirichlet series

$$L(s) = \sum_{n\geq 1} a_n n^{-s} \text{ where } a_{nm} = a_n a_m \text{ if } gcd(n,m) = 1$$

  Enough to know a_{p^n} to deduce the rest, for p a prime number.

- Functional equation

$$\Lambda(s) := N^{s/2}\Gamma_L(s) \cdot L(s) = \varepsilon\overline{\Lambda}((1+w)-s),$$

  - $\Gamma_L(s)$ are defined in terms of Γ-function.
  - $\varepsilon \in \{z \in \mathbb{C} : |z| = 1\}$ is the root number
  - N is the conductor of $L(s)$,
  - $w \in \mathbb{N}$ is the (motivic) weight of $L(s)$.

Sources of L-functions

- Characters χ associated to a number field F give us an L-function of degree $[F : \mathbb{Q}]$ and motivic weight 0

Sources of L-functions

- Characters χ associated to a number field F give us an L-function of degree $[F : \mathbb{Q}]$ and motivic weight 0
- Artin representations associated to a Galois number field F give us an L-function of degree at most $[F : \mathbb{Q}]$ and motivic weight 0

Sources of L-functions

- Characters χ associated to a number field F give us an L-function of degree $[F:\mathbb{Q}]$ and motivic weight 0
- Artin representations associated to a Galois number field F give us an L-function of degree at most $[F:\mathbb{Q}]$ and motivic weight 0
- Classical modular forms $f = \sum_{n>0} a_n q^n$ of weight k give us an L-function of degree degree $2[\mathbb{Q}(a_n):\mathbb{Q}]$, motivic weight $k-1$, and conductor $N^{[\mathbb{Q}(a_n):\mathbb{Q}]}$.

Sources of L-functions

- Classical modular forms $f = \sum_{n>0} a_n q^n$ of weight k give us an L-function of degree degree $2[\mathbb{Q}(a_n) : \mathbb{Q}]$, motivic weight $k-1$, and conductor $N^{[\mathbb{Q}(a_n):\mathbb{Q}]}$.
- Elliptic curves gives us degree 2 L-functions with motivic weight 1

$$F_p(t) = 1 - a_p t + pt^2, \quad a_p := p + 1 - \#E(\mathbb{F}_p)$$

- In general, for a projective variety X, we can associate an L-function to $H^n(X)$

$$F_p(t) = \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{et}}(X)).$$

  This gives an L-function of degree $\dim H^n(X)$ and motivic weight n.
  Note that by Lefschetz fixed-point theorem, we have

$$\exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} t^m\right) = \prod_i \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{et}}(X))^{(-1)^{i+1}}$$

Computing the Dirichlet series

For several applications (special values, zeros, statistics, $\cdots$) one desires to compute an approximation by truncating the Dirichlet series $\sum_{n \leq B} a_n n^{-s}$. Depending on the application B we may want $B = O(\sqrt{N})$, $O(N)$, or simply $O(1)$.

Computing the Dirichlet series

For several applications (special values, zeros, statistics, $\cdots$) one desires to compute an approximation by truncating the Dirichlet series $\sum_{n \leq B} a_n n^{-s}$. Depending on the application B we may want $B = O(\sqrt{N})$, $O(N)$, or simply $O(1)$.

Theorem [Harvey]

One can compute

$$\exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} t^m\right) = \prod_i \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{et}}(X))^{(-1)^{i+1}}$$

for all primes $p < B$ in $B(\log B)^{3+o(1)}$.

Computing the Dirichlet series

For several applications (special values, zeros, statistics, $\cdots$) one desires to compute an approximation by truncating the Dirichlet series $\sum_{n \le B} a_n n^{-s}$. Depending on the application B we may want $B = O(\sqrt{N})$, $O(N)$, or simply $O(1)$.

Theorem [Harvey]

One can compute

$$\exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} t^m\right) = \prod_i \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{et}}(X))^{(-1)^{i+1}}$$

for all primes $p < B$ in $B(\log B)^{3+o(1)}$.

In other words, we can compute $F_p(t)$ on average in $(\log p)^{4+o(1)}$. Unfortunately, the constants involved make it unpractical without further specialization.

Computing Dirichlet series

Goal

Compute $F_p(t)$ for all primes $p < B$ in $B(\log B)^{3+o(1)}$.

In other words, we can compute $F_p(t)$ on average in $(\log p)^{4+o(1)}$.

There are several classes of L-functions for which we can do better:

- Dirichlet/Hecke characters
- Artin representations
- Elliptic curves

Computing Dirichlet series

Goal

Compute $F_p(t)$ for all primes $p < B$ in $B(\log B)^{3+o(1)}$.

In other words, we can compute $F_p(t)$ on average in $(\log p)^{4+o(1)}$.

There are several classes of L-functions for which we can do better:

- Dirichlet/Hecke characters
- Artin representations
- Elliptic curves

We do not need the full Euler factor $F_p(t)$ for most p.
For example, $F_p(t) \bmod t^2$ is sufficient for all $p \in [B^{1/2}, B]$.

Example: Remainder tree for Hyperelliptic curves

$X\colon y^2 = f(x,z)$, with $f \in \mathbb{Z}[x,y]$ a homogeneous polynomial of degree $2g+2$.
X is an hyperelliptic curve of genus g.

$$\#X(\mathbb{F}_p) = \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} \left[\left(\frac{f(t)}{p} \right) + 1 \right]$$

Example: Remainder tree for Hyperelliptic curves

$X\colon y^2 = f(x,z)$, with $f \in \mathbb{Z}[x,y]$ a homogeneous polynomial of degree $2g+2$.
X is an hyperelliptic curve of genus g.

$$\#X(\mathbb{F}_p) = \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} \left[\left(\frac{f(t)}{p} \right) + 1 \right] \equiv 1 + \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} f(t)^{(p-1)/2} \equiv 1 - \sum_{i=1}^{g} f_{(p-1)i}^{(p-1)/2} \pmod{p},$$

where f_i^k is the coefficient of x^i in $f(x,1)^k$.

Example: Remainder tree for Hyperelliptic curves

$X : y^2 = f(x,z)$, with $f \in \mathbb{Z}[x,y]$ a homogeneous polynomial of degree $2g+2$.
X is an hyperelliptic curve of genus g.

$$\#X(\mathbb{F}_p) = \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} \left[\left(\frac{f(t)}{p} \right) + 1 \right] \equiv 1 + \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} f(t)^{(p-1)/2} \equiv 1 - \sum_{i=1}^{g} f_{(p-1)i}^{(p-1)/2} \pmod{p},$$

where f_i^k is the coefficient of x^i in $f(x,1)^k$.

Therefore, we may compute $\#X(\mathbb{F}_p)$ by computing g coefficients of $f^{(p-1)/2}$.

Example: Remainder tree for Hyperelliptic curves

$X: y^2 = f(x,z)$, with $f \in \mathbb{Z}[x,y]$ a homogeneous polynomial of degree $2g+2$.
X is an hyperelliptic curve of genus g.

$$\#X(\mathbb{F}_p) = \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} \left[\left(\frac{f(t)}{p} \right) + 1 \right] \equiv 1 + \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} f(t)^{(p-1)/2} \equiv 1 - \sum_{i=1}^{g} f_{(p-1)i}^{(p-1)/2} \pmod{p},$$

where f_i^k is the coefficient of x^i in $f(x,1)^k$.

Therefore, we may compute $\#X(\mathbb{F}_p)$ by computing g coefficients of $f^{(p-1)/2}$.

Each of the desired coefficients may be obtained via a matrix-vector product

$$v \cdot A(1) \cdots A(\tfrac{p-1}{2}) \bmod p, \text{ where } A(x) \in M_{2g+2}(\mathbb{Z}[x]).$$

Example: Remainder tree for Hyperelliptic curves

$X : y^2 = f(x,z)$, with $f \in \mathbb{Z}[x,y]$ a homogeneous polynomial of degree $2g+2$.
X is an hyperelliptic curve of genus g.

$$\#X(\mathbb{F}_p) = \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} \left[\left(\frac{f(t)}{p} \right) + 1 \right] \equiv 1 + \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} f(t)^{(p-1)/2} \equiv 1 - \sum_{i=1}^{g} f_{(p-1)i}^{(p-1)/2} \pmod p,$$

where f_i^k is the coefficient of x^i in $f(x,1)^k$.

Therefore, we may compute $\#X(\mathbb{F}_p)$ by computing g coefficients of $f^{(p-1)/2}$.

Each of the desired coefficients may be obtained via a matrix-vector product

$$v \cdot A(1) \cdots A(\tfrac{p-1}{2}) \bmod p, \ \text{where } A(x) \in M_{2g+2}(\mathbb{Z}[x]).$$

One can amortize these products by taking advantage of the redundancies.
This leads to an algorithm to compute a_p for $p < B$ in $B(\log B)^{3+o(1)}$ time.

L-functions via remainder tree algorithms

These techniques have lead to several practical algorithms:

- Wilson primes search: $(p-1)! \bmod p^2$ [C–Gerbicz–Harvey]

L-functions via remainder tree algorithms

These techniques have lead to several practical algorithms:

- Wilson primes search: $(p-1)! \bmod p^2$ [C–Gerbicz–Harvey]
- L-functions of hyperelliptic curves $y^2 = f(x)$: $v \cdot A(1) \cdots A(\frac{p-1}{2}) \bmod p$ [Harvey, Harvey–Sutherland^2, Harvey–Massierer–Sutherland]

L-functions via remainder tree algorithms

These techniques have lead to several practical algorithms:

- Wilson primes search: $(p-1)! \bmod p^2$ [C–Gerbicz–Harvey]
- L-functions of hyperelliptic curves $y^2 = f(x)$: $v \cdot A(1) \cdots A(\frac{p-1}{2}) \bmod p$ [Harvey, Harvey–Sutherland[2], Harvey–Massierer–Sutherland]
- L-functions of superelliptic curves $y^r = f(x)$: $v \cdot A(1) \cdots A(\frac{p-\bullet}{r}) \bmod p$ [Sutherland]

L-functions via remainder tree algorithms

These techniques have lead to several practical algorithms:

- Wilson primes search: $(p-1)! \bmod p^2$ [C–Gerbicz–Harvey]
- L-functions of hyperelliptic curves $y^2 = f(x)$: $v \cdot A(1) \cdots A(\frac{p-1}{2}) \bmod p$ [Harvey, Harvey–Sutherland², Harvey–Massierer–Sutherland]
- L-functions of superelliptic curves $y^r = f(x)$: $v \cdot A(1) \cdots A(\frac{p-\bullet}{r}) \bmod p$ [Sutherland]
- L-functions of smooth plane quartics: $v \cdot A(1) \cdots A(p-1) \bmod p$ [C–Harvey–Sutherland]

L-functions via remainder tree algorithms

These techniques have lead to several practical algorithms:

- Wilson primes search: $(p-1)! \bmod p^2$ [C–Gerbicz–Harvey]
- L-functions of hyperelliptic curves $y^2 = f(x)$: $v \cdot A(1) \cdots A(\frac{p-1}{2}) \bmod p$ [Harvey, Harvey–Sutherland[2], Harvey–Massierer–Sutherland]
- L-functions of superelliptic curves $y^r = f(x)$: $v \cdot A(1) \cdots A(\frac{p-\bullet}{r}) \bmod p$ [Sutherland]
- L-functions of smooth plane quartics: $v \cdot A(1) \cdots A(p-1) \bmod p$ [C–Harvey–Sutherland]
- L-functions of Hypergeometric motives: $\sum_{m=0}^{p-1} \frac{(\alpha)_m}{(\beta)_m} z^m$ [C–Kedlaya–Roe[2]]

All these algorithms have a p-adic flavor.

Given a projective variety X, we can associate an L-function to $H^n(X)$ via

$$F_p(t) = \operatorname{det}(1 - t \operatorname{Frob} | H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell)) \in \mathbb{Z}[x].$$

One approach to compute F_p, is to compute $F_p(t) \bmod \ell$ for several ℓ. This is only practical if there is a nice description of $H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell))$, e.g., Tate modules.

p-adic algorithms for L-functions

Given a projective variety X, we can associate an L-function to $H^n(X)$ via

$$F_p(t) = \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell)) \in \mathbb{Z}[x].$$

One approach to compute F_p, is to compute $F_p(t) \bmod \ell$ for several ℓ. This is only practical if there is a nice description of $H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell))$, e.g., Tate modules.

Alternatively, one may replace $H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell)$ with a p-adic cohomology theory, i.e., a cohomology theory with coefficients in $\mathbb{Q}_p$, e.g.,

$$F_p(t) = \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{rig}}(X)) \in \mathbb{Z}[x].$$

and compute a p-adic approximation of the matrix representing Frob.

p-adic algorithms for L-functions

Given a projective variety X, we can associate an L-function to $H^n(X)$ via

$$F_p(t) = \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell)) \in \mathbb{Z}[x].$$

One approach to compute F_p, is to compute $F_p(t) \bmod \ell$ for several ℓ. This is only practical if there is a nice description of $H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell))$, e.g., Tate modules.

Alternatively, one may replace $H^n_{\mathrm{et}}(X, \mathbb{Z}_\ell)$ with a p-adic cohomology theory, i.e., a cohomology theory with coefficients in $\mathbb{Q}_p$, e.g.,

$$F_p(t) = \det(1 - t\,\mathrm{Frob}\,|H^n_{\mathrm{rig}}(X)) \in \mathbb{Z}[x].$$

and compute a p-adic approximation of the matrix representing Frob.

If X is an hypersurface, Monsky–Washnitzer cohomology provides a nice description for the primitive cohomology of X $PH^{\dagger,n}(X)$ in terms of de Rham cohomology with overconvergent power series.

Overall picture

Goal

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

Overall picture

Goal

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

$$PH^n_{\mathrm{dR}}(X_{\mathbb{Q}_p}) \xrightarrow[\mathrm{id}]{\sim} PH^{\dagger,n-1}(X) \circlearrowright \mathrm{Frob}$$

Overall picture

Goal

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

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

$\downarrow$

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

Overall picture

Goal

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

$$
\begin{array}{ccc}
 & & \text{Frob} \circlearrowright \\
PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_p}) & \xrightarrow[\text{id}]{\sim} & PH^{\dagger,n-1}(X) \\
\downarrow & & \downarrow \\
\text{explicit description over } \mathbb{C} & & \text{de Rham cohomology} \\
\text{[Dwork–Griffiths, Batyrev–Cox]} & & \text{with overconvergent power series}
\end{array}
$$

Overall picture

Goal

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

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

$PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_p})$ ⇢ explicit description over $\mathbb{C}$ [Dwork–Griffiths, Batyrev–Cox]

$PH^{\dagger,n-1}(X)$ ⇢ de Rham cohomology with overconvergent power series

cohomology relations + commutative algebra $\Longrightarrow$ basis for $PH^{n-1}_{\mathrm{dR}}(X_{\mathbb{Q}_p})$ + reduction algorithm

L-functions of hypersurfaces in a toric variety

Theorem [C–Harvey–Kedlaya]

Given a polynomial $f = \sum_{\alpha \in \mathbb{Z}^{n+1}} c_\alpha x^\alpha \in \mathbb{F}_p[x_1^{\pm}, \ldots, x_n^{\pm}]$ defining nondegenerate hypersurface $V(f)$ in a toric variety $\mathbb{P}_\Delta$ one can compute

$$\det(1 - t\,\mathrm{Frob}\,|PH^n_{\mathrm{rig}}(X)) \in \mathbb{Z}[x]$$

in $p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$ time.

To compute a_n for $n \leq B$, this leads to a $B^{2+o(1)}$ algorithm.

L-functions of hypersurfaces in a toric variety

Theorem [C–Harvey–Kedlaya]

Given a polynomial $f = \sum_{\alpha \in \mathbb{Z}^{n+1}} c_\alpha x^\alpha \in \mathbb{F}_p[x_1^\pm, \ldots, x_n^\pm]$ defining nondegenerate hypersurface $V(f)$ in a toric variety $\mathbb{P}_\Delta$ one can compute

$$\det(1 - t\,\mathrm{Frob}\,|PH^n_{\mathrm{rig}}(X)) \in \mathbb{Z}[x]$$

in $p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$ time.

To compute a_n for $n \leq B$, this leads to a $B^{2+o(1)}$ algorithm. **Implementation**

- Projective hypersurfaces:

  C++ library: `github.com/edgarcosta/controlledreduction`

  Sage wrapper: `github.com/edgarcosta/pycontrolledreduction`
- Toric hypersurfaces:

  C++ library: `github.com/edgarcosta/ToricControlledReduction`

L-functions of hypersurfaces in a toric variety

Theorem [C–Harvey–Kedlaya]

Given a polynomial $f = \sum_{\alpha \in \mathbb{Z}^{n+1}} c_\alpha x^\alpha \in \mathbb{F}_p[x_1^{\pm}, \ldots, x_n^{\pm}]$ defining nondegenerate hypersurface $V(f)$ in a toric variety $\mathbb{P}_\Delta$ one can compute

$$\det(1 - t\,\mathrm{Frob}\,|PH^n_{\mathrm{rig}}(X)) \in \mathbb{Z}[x]$$

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

L-functions of hypersurfaces in a toric variety

Theorem [C–Harvey–Kedlaya]

Given a polynomial $f = \sum_{\alpha \in \mathbb{Z}^{n+1}} c_\alpha x^\alpha \in \mathbb{F}_p[x_1^{\pm}, \ldots, x_n^{\pm}]$ defining nondegenerate hypersurface $V(f)$ in a toric variety $\mathbb{P}_\Delta$ one can compute

$$\det(1 - t \,\mathrm{Frob}\, | PH^n_{\mathrm{rig}}(X)) \in \mathbb{Z}[x]$$

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

To compute a_n for $n \leq B$, this leads to a $B^{2+o(1)}$ algorithm.

Fits well in the remainder tree algorithm infrastructure, so in theory, can reduce the average time complexity for each prime to

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

L-functions of hypersurfaces in a toric variety

Theorem [C–Harvey–Kedlaya]

Given a polynomial $f = \sum_{\alpha \in \mathbb{Z}^{n+1}} c_\alpha x^\alpha \in \mathbb{F}_p[x_1^{\pm}, \ldots, x_n^{\pm}]$ defining nondegenerate hypersurface $V(f)$ in a toric variety $\mathbb{P}_\Delta$ one can compute

$$\det(1 - t\,\mathrm{Frob}\,|PH^n_{\mathrm{rig}}(X)) \in \mathbb{Z}[x]$$

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

Implementations:

- Projective hypersurfaces:
  C++ library: github.com/edgarcosta/controlledreduction
  Sage wrapper: github.com/edgarcosta/pycontrolledreduction
- Toric hypersurfaces:
  C++ library: github.com/edgarcosta/ToricControlledReduction

K3 surfaces

Naturally arise as hypersurfaces in 95 weighted projective spaces.

- smooth quartic surface in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of $\mathbb{P}^2$ branched over a sextic curve $\mathbb{P}(3, 1, 1, 1)$

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

K3 surfaces

Naturally arise as hypersurfaces in 95 weighted projective spaces.

- smooth quartic surface in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of $\mathbb{P}^2$ branched over a sextic curve $\mathbb{P}(3, 1, 1, 1)$

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

$$\operatorname{Pic}(X^{\mathrm{al}}) \simeq H^{1,1}(X) \cap H^2(X, \mathbb{Z}) \subsetneq H^2(X, \mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

$$H^2(X, \mathbb{Q}) \simeq \operatorname{Pic}(X^{\mathrm{al}})_{\mathbb{Q}} \oplus T(X)_{\mathbb{Q}}$$

The L-functions associated to $\operatorname{Pic}(X^{\mathrm{al}})$ are associated to Artin representations. New and interesting L-functions arise from $T(X)$.

If X is an hypersurface in a toric variety $\mathbb{P}_\Delta$, then $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq \operatorname{rk}\operatorname{Pic} X_\Delta$.

Example: K3 surface in the Dwork pencil

Consider the projective quartic surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ given by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0.$$

For $\lambda = 1$ and $p = 2^{20} - 3$, using the old projective code in `3h36m` we compute that

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

where the "interesting" factor is

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

The polynomials R_1 and R_2 arise from the action of Frobenius on the Picard lattice; by a p-adic formula of de la Ossa–Kadir.

$Q(t)$ can be interpreted as an Euler factor of $\mathrm{Sym}^2 E$.

Example: a quartic surface in the Dwork pencil

Consider the projective quartic surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ given by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0.$$

For $\lambda = 1$ and $p = 2^{20} - 3$, using the toric ~~old projective~~ code in `37s` ~~`3h36m`~~ we compute

$$\zeta_X(t)^{-1} = (1-t)(1-pt)^{16}(1+pt)^3(1-p^2t)(1+pt)(1-1688538t+p^2t^2).$$

Example: a quartic surface in the Dwork pencil

Consider the projective quartic surface X in $\mathbb{P}^3_{\mathbb{F}_p}$ given by

$$x^4 + y^4 + z^4 + w^4 + \lambda xyzw = 0.$$

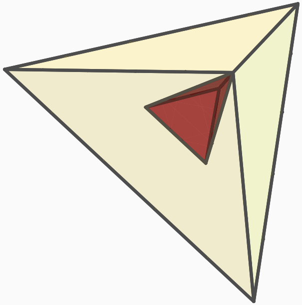
For $\lambda = 1$ and $p = 2^{20} - 3$, using the toric ~~old projective~~ code in 37s ~~3h36m~~ we compute

$$\zeta_X(t)^{-1} = (1-t)(1-pt)^{16}(1+pt)^3(1-p^2t)(1+pt)(1-1688538t+p^2t^2).$$

The defining monomials of X generate a sublattice of index 4^2 in $\mathbb{Z}^3$, and we can work “in” that sublattice, by using

$$x^4y^{-1}z^{-1} + \lambda x + y + z + 1 = 0$$

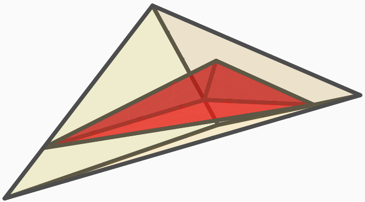
which has a polytope much smaller than the full simplex ($32/3 \approx 10.6$ vs $2/3 \approx 0.6$).



Example: a hypergeometric motive (also a K3 surface)

Consider the appropriate completion
of the toric surface over $\mathbb{F}_p$ with $p = 2^{15} - 19$ given by

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



In `1.3s`, we compute
that the "interesting" factor of $\zeta_X(t)$ is (up to rescaling)

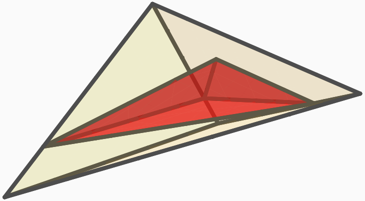
$$pQ(t/p) = p + 20508t^1 - 18468t^2 - 26378t^3 - 18468t^4 + 20508t^5 + pt^6.$$

In $\mathbb{P}^3$ this surface is degenerate, and would have taken us `13m26s` to do the same computation with a dense model.

Example: a hypergeometric motive (also a K3 surface)

Consider the appropriate completion
of the toric surface over $\mathbb{F}_p$ with $p = 2^{15} - 19$ given by

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



In `1.3s`, we compute
that the "interesting" factor of $\zeta_X(t)$ is (up to rescaling)

$$pQ(t/p) = p + 20508t^1 - 18468t^2 - 26378t^3 - 18468t^4 + 20508t^5 + pt^6.$$

In $\mathbb{P}^3$ this surface is degenerate, and would have taken us `13m26s` to do the same computation with a dense model.

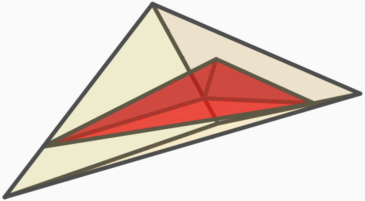
We can confirm the linear term with Magma:

```
C2F2 := HypergeometricData([6,12], [1,1,1,2,3]);
EulerFactor(C2F2, 2^10 * 3^6, 2^15-19: Degree:=1);
1 + 20508*$.1 + O($.1^2)
```

Example: a hypergeometric motive (also a K3 surface)

Consider the appropriate completion
of the toric surface over $\mathbb{F}_p$ with $p = 2^{15} - 19$ given by

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



In `1.3s`, we compute
that the "interesting" factor of $\zeta_X(t)$ is (up to rescaling)

$$pQ(t/p) = p + 20508t^1 - 18468t^2 - 26378t^3 - 18468t^4 + 20508t^5 + pt^6.$$

In $\mathbb{P}^3$ this surface is degenerate, and would have taken us `13m26s` to do the same computation with a dense model.

We can compute all the a_p for $p \leq 2^{18}$ in 4s

```
H = AmortizingHypergeometricData(cyclotomic=[[6,12],[1,1,1,2,3]])
time aps = H.amortized_padic_H_values(1/(2^10*3^6), 2^18)
user 4.01 s, sys: 15.9 ms, total: 4.02 s
```

Example: a K3 surface in a non weighted projective space

Consider the surface X defined as the closure (in $\mathbb{P}_\Delta$) of the affine surface defined by the Laurent polynomial

$$3x + y + z + x^{-2}y^2z + x^3y^{-6}z^{-2} + 3x^{-2}y^{-1}z^{-2} - 2 - x^{-1}y - y^{-1}z^{-1} - x^2y^{-4}z^{-1} - xy^{-3}z^{-1}.$$

The Hodge numbers of $PH^2(X)$ are $(1, 14, 1)$. For $p = 2^{15} - 19$, in `2m14s` we obtain the "interesting" factor of $\zeta_X(t)$:

$$pQ(t/p) = (1 - t) \cdot (1 + t) \cdot (p + 33305t^1 + 1564t^2 - 14296t^3 - 11865t^4 + 5107t^5 + 27955t^6 + 25963t^7 + 27955t^8 + 5107t^9 - 11865t^{10} - 14296t^{11} + 1564t^{12} + 33305t^{13} + pt^{14}).$$

We know of no previous algorithm that can compute $\zeta_X(t)$ for p in this range!

Example: random dense K3 surface

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

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

For $p = 2^{15} - 19$, in `38m27s`, we obtain

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

where

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

Example: a quintic threefold in the Dwork pencil

Consider the threefold X in $\mathbb{P}^4_{\mathbb{F}_p}$ for $p = 2^{20} - 3$ given by

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

In `5m48s`, we compute that

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

where the "interesting" factor is

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

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

Using the old projective code, we extrapolate it would have taken us at least 120 days.

Example: a Calabi–Yau 3fold in a non weighted projective space

Let X be the closure (in $\mathbb{P}_\Delta$) of the affine threefold

$$xyz^2w^3 + x + y + z - 1 + y^{-1}z^{-1} + x^{-2}y^{-1}z^{-2}w^{-3} = 0.$$

For $p = 2^{20} - 3$, in `42m`, we computed the “interesting” factor of $\zeta_X(t)$

$$(1 + 718pt + p^3t^2)(1 + 1188466826t + 1915150034310pt^2 + 1188466826p^3t^3 + p^6t^4).$$

Example: a Calabi–Yau 3fold in a non weighted projective space

Let X be the closure (in $\mathbb{P}_\Delta$) of the affine threefold

$$xyz^2w^3 + x + y + z - 1 + y^{-1}z^{-1} + x^{-2}y^{-1}z^{-2}w^{-3} = 0.$$

For $p = 2^{20} - 3$, in `42m`, we computed the "interesting" factor of $\zeta_X(t)$

$$(1 + 718pt + p^3t^2)(1 + 1188466826t + 1915150034310pt^2 + 1188466826p^3t^3 + p^6t^4).$$

Calabi–Yau threefolds can arise as hypersurfaces in:

- 7555 weighted projective spaces;
- 473,800,776 toric varieties.

See `http://hep.itp.tuwien.ac.at/~kreuzer/CY/`.