Zeta functions with p-adic cohomology

David Roe

Harvard University

Counting Points: Theory, Algorithms and Practice

$X \subset \mathbb{P}^n_{\mathbb{F}_q}$ smooth, given by $f \in \mathbb{F}_q[x_0, \ldots, x_n]$, $\deg(f) = d$.

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

$X \subset \mathbb{P}^n_{\mathbb{F}_q}$ smooth, given by $f \in \mathbb{F}_q[x_0, \ldots, x_n]$, $\deg(f) = d$.

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

$$Z_X(T) = \prod_{i=0}^{2n-2} P_i(T)^{(-1)^{i+1}},$$

where $P_i(T) = \det(1 - TF_i | H^i(X))$.
This works when H^* is a Weil cohomology theory, where each $H^i(X)$ comes equipped with a Frobenius.

Weil cohomology

- Contravariant functors H^i from smooth proper varieties over $\mathbb{F}_q$ to finite dimensional K-vector spaces

Weil cohomology

- Contravariant functors H^i from smooth proper varieties over $\mathbb{F}_q$ to finite dimensional K-vector spaces
- equipped with endomorphisms F_i with $P_i(T) = \det(1 - TF_i | H^i(X))$.

Weil cohomology

- Contravariant functors H^i from smooth proper varieties over $\mathbb{F}_q$ to finite dimensional K-vector spaces
- equipped with endomorphisms F_i with $P_i(T) = \det(1 - TF_i | H^i(X))$.
- Lefschetz: for any m, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{trace}(F_i^m | H^i(X))$.

Weil cohomology

- Contravariant functors H^i from smooth proper varieties over $\mathbb{F}_q$ to finite dimensional K-vector spaces
- equipped with endomorphisms F_i with $P_i(T) = \det(1 - TF_i|H^i(X))$.
- Lefschetz: for any m, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)}(-1)^i \operatorname{trace}(F_i^m|H^i(X))$.
- Write $H^i(X)(k)$ for $H^i(X)$ with Frobenius $q^{-k}F_i$. If $n = \dim(X)$, one has functorial, F-equivariant $\operatorname{trace}_X : H^{2n}(X)(n) \to K$, isomorphisms if X is geometrically irreducible.

Weil cohomology

- Contravariant functors H^i from smooth proper varieties over $\mathbb{F}_q$ to finite dimensional K-vector spaces
- equipped with endomorphisms F_i with $P_i(T) = \det(1 - TF_i | H^i(X))$.
- Lefschetz: for any m, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{trace}(F_i^m | H^i(X))$.
- Write $H^i(X)(k)$ for $H^i(X)$ with Frobenius $q^{-k}F_i$. If $n = \dim(X)$, one has functorial, F-equivariant $\operatorname{trace}_X \colon H^{2n}(X)(n) \to K$, isomorphisms if X is geometrically irreducible.
- Associative, functorial, F-equivariant cup products so that $H^i(X) \times H^{2n-i}(X)(n) \xrightarrow{\cup} H^{2n}(X)(n) \xrightarrow{\operatorname{trace}_X} K$ is perfect.

Weil cohomology

- Contravariant functors H^i from smooth proper varieties over $\mathbb{F}_q$ to finite dimensional K-vector spaces
- equipped with endomorphisms F_i with $P_i(T) = \det(1 - TF_i | H^i(X))$.
- Lefschetz: for any m, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{trace}(F_i^m | H^i(X))$.
- Write $H^i(X)(k)$ for $H^i(X)$ with Frobenius $q^{-k}F_i$. If $n = \dim(X)$, one has functorial, F-equivariant $\operatorname{trace}_X \colon H^{2n}(X)(n) \to K$, isomorphisms if X is geometrically irreducible.
- Associative, functorial, F-equivariant cup products so that $H^i(X) \times H^{2n-i}(X)(n) \xrightarrow{\cup} H^{2n}(X)(n) \xrightarrow{\operatorname{trace}_X} K$ is perfect.
- Rigid cohomology is an example of a Weil cohomology.

Let

- $U = \mathbb{P}^n_{\mathbb{F}_q} \backslash X$,
- $\mathfrak{f} \in \mathbb{Z}_q[x_0, \ldots, x_n]$ a lift of f,
- $\mathfrak{X}$ the zero locus of $\mathfrak{f}$,
- $\mathfrak{U} = \mathbb{P}^n_{\mathbb{Z}_q} \backslash \mathfrak{X}$
- $\tilde{X} = \mathfrak{X}_{\mathbb{Q}_q}$, $\tilde{U} = \mathfrak{U}_{\mathbb{Q}_q}$.

- By the Lefschetz hyperplane theorem, $H^i_{\mathrm{rig}}(X) \cong H^i_{\mathrm{rig}}(\mathbb{P}^n_{\mathbb{F}_q})$ for $i \leq n-2$.
- By Poincare duality and a computation with projective space, $H^i_{\mathrm{rig}}(X)$ is zero for $i \neq n-1$ odd and is one dimensional for $i \neq n-1$ even, with q-Frobenius acting by multiplication by $q^{i/2}$.

- By the Lefschetz hyperplane theorem, $H^i_{\mathrm{rig}}(X) \cong H^i_{\mathrm{rig}}(\mathbb{P}^n_{\mathbb{F}_q})$ for $i \leq n-2$.
- By Poincare duality and a computation with projective space, $H^i_{\mathrm{rig}}(X)$ is zero for $i \neq n-1$ odd and is one dimensional for $i \neq n-1$ even, with q-Frobenius acting by multiplication by $q^{i/2}$.
- The Gysin sequence yields Frobenius-equivariant exact sequences

$$0 \to H^n_{\mathrm{rig}}(U) \to H^{n-1}_{\mathrm{rig}}(X)(-1) \to 0 \qquad \text{if } n \text{ even,}$$

$$0 \to H^n_{\mathrm{rig}}(U) \to H^{n-1}_{\mathrm{rig}}(X)(-1) \to H^{n+1}_{\mathrm{rig}}(\mathbb{P}^n_{\mathbb{F}_q}) \to 0 \qquad \text{if } n \text{ odd.}$$

Thus

$$Z_X(T) = P_{n-1}(T)^{(-1)^n} \prod_{i=0}^{n-1} \frac{1}{1 - q^i T},$$

where

$$P_{n-1}(T) = \det(1 - q^{-1} F_q | H^n_{\mathrm{rig}}(U)).$$

Algorithm Summary

To find an approx. matrix for Frobenius on $H^n_{\mathrm{rig}}(U)$ (modulo p^r):

- Compute a basis for $H^n_{\mathrm{rig}}(U) = H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$.
- Apply absolute Frobenius to each basis element, truncating the result modulo p^s for some $s \geq r$.
- Apply a reduction process to write each result as a linear combination of basis elements plus a coboundary.
- Obtain q-power Frobenius as the product of conjugates of the resulting matrix.

Berthelot gives a description of $H^i_{\mathrm{rig}}(U)$ in terms of Monsky-Washnitzer cohomology:

- Since U is affine, we can find some $A \cong \mathbb{Z}_q[x_1, \ldots, x_m]/I$ with $\mathfrak{U} = \operatorname{Spec} A$.
- Let $\mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger$ be the ring of power series in $\mathbb{Z}_q[\![x_1, \ldots, x_m]\!]$ converging on an open polydisk of radius greater than 1. Set $A^\dagger = \mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger / I\mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger$.

Berthelot gives a description of $H^i_{\mathrm{rig}}(U)$ in terms of Monsky-Washnitzer cohomology:

- Since U is affine, we can find some $A \cong \mathbb{Z}_q[x_1, \ldots, x_m]/I$ with $\mathfrak{U} = \operatorname{Spec} A$.
- Let $\mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger$ be the ring of power series in $\mathbb{Z}_q[\![x_1, \ldots, x_m]\!]$ converging on an open polydisk of radius greater than 1. Set $A^\dagger = \mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger / I\mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger$.
- $H^i_{\mathrm{rig}}(U)$ is isomorphic to the ith cohomology of the complex

$$\Omega^\bullet_{A/\mathbb{Z}_q} \otimes_A A^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q.$$

Description of $H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$, after Griffiths

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

- $A^\dagger$ is the ring of formal sums $\sum_{i=0}^{\infty} g_i \mathfrak{f}^{-i}$, where $g_i \in \mathbb{Z}_q[x_0, \ldots, x_n]$ is homogenous of degree di, and

$$\liminf_{i \to \infty} v(g_i)/i > 0,$$

where $v(\sum c_I x^I) = \min_I v(c_I)$.

Description of $H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$, after Griffiths

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

- $A^\dagger$ is the ring of formal sums $\sum_{i=0}^{\infty} g_i \mathfrak{f}^{-i}$, where $g_i \in \mathbb{Z}_q[x_0, \ldots, x_n]$ is homogenous of degree di, and

  $$\liminf_{i\to\infty} v(g_i)/i > 0,$$

  where $v(\sum c_I x^I) = \min_I v(c_I)$.
- $H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$ is the quotient of the group of n-forms generated by $g\Omega/\mathfrak{f}^m$ ($m \in \mathbb{Z}, g \in \mathbb{Q}_q[x_0, \ldots, x_n]$ homogeneous degree $md - n - 1$) by the subgroup generated by those of the form

  $$\frac{(\partial_i g)\Omega}{\mathfrak{f}^m} - m\frac{(\partial_i \mathfrak{f})g\Omega}{\mathfrak{f}^{m+1}}.$$

Reduction

$$\frac{(\partial_i g)\Omega}{\mathfrak{f}^m} - m\frac{(\partial_i \mathfrak{f})g\Omega}{\mathfrak{f}^{m+1}}.$$

Since X is smooth, a theorem of Macauly implies

$$(\partial_0 \mathfrak{f}, \ldots, \partial_n \mathfrak{f}) \supset (x_0, \ldots, x_n)^\alpha,$$

where $\alpha = (n+1)(d-2)+1$.
We now have a *reduction algorithm*: if

$$\deg(g) = md - n - 1 \geq \alpha,$$

then $g = \sum_{i=0}^{n} g_i(\partial_i \mathfrak{f})$, and

$$\frac{g\Omega}{\mathfrak{f}^{m+1}} \equiv \frac{1}{m\mathfrak{f}^m}\sum_{i=0}^{n}(\partial_i g_i)\Omega.$$

Basis for $H^n_{\mathrm{rig}}(U)$

$$\frac{(\partial_i g)\Omega}{\mathfrak{f}^m} - m\frac{(\partial_i \mathfrak{f}) g\Omega}{\mathfrak{f}^{m+1}}.$$

- Define M_h to be a set of monomials that generate the degree $hd - n - 1$ part of $\mathbb{F}_q[x_0, \ldots, x_n]/(\partial_0\mathfrak{f}, \ldots, \partial_n\mathfrak{f})$.
- Then we can choose a basis for $H^n_{\mathrm{rig}}(U)$ to be

$$\left\{ \frac{\mu\Omega}{\mathfrak{f}^h} \mid 1 \leq h \leq n, \mu \in M_h \right\}.$$

Frobenius

Lift absolute frobenius to $F\colon A^\dagger \to A^\dagger$ by $F(x_i) = x_i^p$ (acting via Frobenius on the coefficients) and

$$\begin{aligned} F(\mathfrak{f}^{-1}) &= \mathfrak{f}^{-p}\left(1 + p\frac{F(\mathfrak{f}) - \mathfrak{f}^p}{p\mathfrak{f}^p}\right)^{-1} \\ &= \mathfrak{f}^{-p}\sum_{j\geq 0}(F(\mathfrak{f}) - \mathfrak{f}^p)^j \mathfrak{f}^{-pj} \end{aligned}$$

This extends to $H^n_{\mathrm{dR}}(\tilde{U}/\mathbb{Q}_q)$ by setting $F(dx_i/x_i) = p\,dx_i/x_i$ and $F(\Omega) = F(x_0\cdots x_n)F(x_0^{-1}\cdots x_n^{-1}\Omega)$.

Precision

We must truncate the power series expansion for the image of each basis element under Frobenius. The level at which we truncate needs to be larger than our desired final precision, since the reduction step

$$\frac{g\Omega}{\mathfrak{f}^{m+1}} \equiv \frac{1}{m\mathfrak{f}^m} \sum_{i=0}^{n} (\partial_i g_i)\Omega$$

can lose precision when m is a multiple of p. Figuring out exactly how much precision is lost is tricky.

Runtime

In our implementation, we use Gröbner bases for some of the reduction steps, and this makes the analysis of the runtime difficult. David Harvey's improvements to the algorithm improve the runtime and make the analysis simpler; I'll leave a discussion of the theoretical runtime to him.

We computed the zeta function of the quartic surface over $\mathbb{F}_3$ defined by the polynomial

$$x^4 - xy^3 + xy^2w + xyzw + xyw^2 - xzw^2 + y^4 + y^3w - y^2zw + z^4 + w^4.$$

On a dual Opteron 246 running at 2 GHz with 2GB of RAM, we have the following timings:

Final Precision	Initial Precision	CPU sec	MB
3^2	3^6	227	37
3^3	3^7	731	53
—	3^8	907	64
—	3^9	4705	124
3^4	3^{10}	13844	906
3^5	3^{11}	15040	1103
3^6	3^{12}	40144	1795

In fact, in this case

$$P_{n-1}(T) = \frac{1}{3}(3T^{21} + 5T^{20} + 6T^{19} + 7T^{18} + 5T^{17} + 4T^{16} + 2T^{15} - T^{14} - 3T^{13} - 5T^{12} - 5T^{11} - 5T^{10} - 5T^{9} - 3T^{8} - T^{7} + 2T^{6} + 4T^{5} + 5T^{4} + 7T^{3} + 6T^{2} + 5T + 3)$$

Questions?