Zeta functions with p-adic cohomology

David Roe

Harvard University / University of Calgary

Geocrypt 2011

Outline

p-adic point counting

Kedlaya [Ked01] gives an algorithm for computing the number of $\mathbb{F}_q$-rational points on a hyperelliptic curve using p-adic cohomology. Suppose that X is a hyperelliptic curve of genus g, whose affine locus is defined by the equation

$$y^2 = f(x)$$

for some $f(x) \in \mathbb{F}_q[x]$. Kedlaya's key idea is that we can determine the size of $X(\mathbb{F}_q)$ from the action of Frobenius on a Weil cohomology theory applied to X.

Notation

We first work with a more general smooth projective X. Let U be an affine open in X (for hyperelliptic curves we will set U as the subset of the standard affine chart with $y \neq 0$). Set $\bar{A}$ as the coordinate ring of U, and choose a smooth $\mathbb{Z}_q$-algebra A with $A \otimes_{\mathbb{Z}_q} \mathbb{F}_q = \bar{A}$. In the curve case

$$A = \mathbb{Z}_q[x, y, y^{-1}]/(y^2 - f(x)).$$

Monsky-Washnitzer cohomology

Unfortunately, we cannot lift Frobenius to an endomorphism of A: we need to p-adically complete A somehow. The full completion is too big, so instead we use the weak completion $A^\dagger$. Fix $x_1, \ldots, x_n \in A$ whose images in $\bar{A}$ generate it over $\mathbb{F}_q$. Then

$$A^\dagger = \Big\{ \sum_{n=0}^{\infty} a_n P_n(x_1, \ldots, x_n) : v_p(a_n) \geq n, \quad \text{and } \exists c > 0 \text{ with} \deg(P_n) < c(n+1) \text{ for all } n \Big\}$$

The Monsky-Washnitzer cohomology of U is the cohomology of the algebraic de Rham complex over $A^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$.

$A^\dagger$ for hyperelliptic curves

We can be more explicit for hyperelliptic curves. For $P(x) \in \mathbb{Z}_q[x]$, let $v_p(P)$ be the minimum valuation of any coefficient. Then

$$A^\dagger = \left\{ \sum_{n=-\infty}^{\infty} P_n(x) y^n : \liminf_{n\to\infty} \frac{v_p(P_n(x))}{n} > 0, \liminf_{n\to\infty} \frac{v_p(P_{-n}(x))}{n} > 0 \right\}.$$

Lifting Frobenius

We define a lift of Frobenius $\sigma\colon A^\dagger \to A^\dagger$ by setting

- σ is the standard Frobenius on coefficients in $\mathbb{Z}_q$,
- $\sigma(x) = x^p$,
- and defining $\sigma(y)$ by

$$\begin{aligned}\sigma(y) &= y^p \left(1 + \frac{\sigma(f(x)) - f(x)^p}{y^{2p}}\right)^{1/2} \\ &= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(\sigma(f(x)) - f(x)^p)^i}{y^{pi}}\end{aligned}$$

Lefschetz fixed-point theorem

The key theorem which will allow us to use this cohomology theory to count rational points is the following.

Theorem

Suppose that $\bar{A}$ is smooth and integral of dimension n over $\mathbb{F}_q$, and that the weak completion $A^\dagger$ of $\bar{A}$ admits a Frobenius F lifting the q-Frobenius on $\bar{A}$. Then the number of homomorphisms $\bar{A} \to \mathbb{F}_q$ is given by

$$\sum_{i=0}^{n} (-1)^i \operatorname{Tr}(q^n F^{-1} \mid \mathrm{H}^i(A; \mathbb{Q}_q)).$$

Kedlaya's Algorithm

The plan:

1. Write down a basis for $\mathrm{H}^1(A; \mathbb{Q}_q)$ and apply Frobenius to each basis element.
2. Subtract coboundaries in order to write these images in terms of the original basis, obtaining a matrix M for the p-power Frobenius.
3. Determine a matrix M' for the q-power Frobenius by taking a product of conjugates of M. Recover the zeta function (or the cardinality of $X(\mathbb{F}_q)$) from the characteristic polynomial of M' and the Weil conjectures.

A basis for $H^1(A; \mathbb{Q}_q)$

A priori, our one-forms have the shape

$$\sum_{n=-\infty}^{\infty} \sum_{i=0}^{d_n} a_{i,n} x^i dx/y^n.$$

In fact, we can determine that

$$\left\{ x^i \frac{dx}{y} \right\}_{i=0}^{2g-1} \cup \left\{ x^i \frac{dx}{y^2} \right\}_{i=0}^{2g-1}$$

is a basis for $H^1(A; \mathbb{Q}_q)$ using the following reduction formulas.

Reduction in cohomology

Suppose $B(x) \in \mathbb{Z}_q[x]$. Then we can write $B(x) = R(x)f(x) + S(x)f'(x)$ and this gives

$$\frac{B(x)dx}{y^s} \equiv \frac{R(x)dx}{y^{s-2}} + \frac{2S'(x)dx}{(s-2)y^{s-2}}$$

allowing us to collect terms in the $n = 1$ and $n = 2$ components. Moreover, the relation

$$[S(x)f'(x) + 2S'(x)f(x)]dx/y \equiv 0$$

with $S(x) = x^{m-2g}$ then allows us to reduce the degree of the coefficient of dx/y and dx/y^2.

Zeta functions

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

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

Zeta functions

$X \subset \mathbb{P}^n_{\mathbb{F}_q}$ 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, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{Tr}(F_i^m | H^i(X))$.

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, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{Tr}(F_i^m | H^i(X))$.
- Write $H^i(X)(k)$ for $H^i(X)$ with Frobenius $q^{-k}F_i$. If $n = \dim(X)$, one has functorial, F-equivariant $\operatorname{Tr}_X \colon H^{2n}(X)(n) \to K$, 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, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{Tr}(F_i^m | H^i(X))$.
- Write $H^i(X)(k)$ for $H^i(X)$ with Frobenius $q^{-k} F_i$. If $n = \dim(X)$, one has functorial, F-equivariant $\operatorname{Tr}_X \colon H^{2n}(X)(n) \to K$, isomorphisms if X is geometrically irreducible.
- Associative, functorial, F-equivariant cup products so that $H^i(X) \times H^{2n-i}(X)(n) \xrightarrow{\cup} H^{2n}(X)(n) \xrightarrow{\operatorname{Tr}_X} K$ 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, $\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{Tr}(F_i^m | H^i(X))$.
- Write $H^i(X)(k)$ for $H^i(X)$ with Frobenius $q^{-k}F_i$. If $n = \dim(X)$, one has functorial, F-equivariant $\operatorname{Tr}_X \colon H^{2n}(X)(n) \to K$, isomorphisms if X is geometrically irreducible.
- Associative, functorial, F-equivariant cup products so that $H^i(X) \times H^{2n-i}(X)(n) \xrightarrow{\cup} H^{2n}(X)(n) \xrightarrow{\operatorname{Tr}_X} K$ is perfect.
- Rigid cohomology is an example of a Weil cohomology.

Notation

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 $\mathfrak{f}$,
- $\mathfrak{U} = \mathbb{P}^n_{\mathbb{Z}_q} \backslash \mathfrak{X}$
- $\tilde{X} = \mathfrak{X}_{\mathbb{Q}_q}$, $\tilde{U} = \mathfrak{U}_{\mathbb{Q}_q}$.

Relating the cohomology of X and U

- 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 $q^{i/2}$.

Relating the cohomology of X and U

- By the Lefschetz hyperplane theorem, $H^i_{\text{rig}}(X) \cong H^i_{\text{rig}}(\mathbb{P}^n_{\mathbb{F}_q})$ for $i \leq n-2$.
- By Poincare duality and a computation with projective space, $H^i_{\text{rig}}(X)$ 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

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

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

Zeta functions in terms of a Weil cohomology theory

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.

Rigid cohomology of U

Berthelot gives a description of $H^i_{\text{rig}}(U)$ 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 $A^\dagger = \mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger / I\mathbb{Z}_q\langle x_1, \ldots, x_m\rangle^\dagger$.

Rigid cohomology of U

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

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

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

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

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 [Har10] to the algorithm improve the runtime and make the analysis simpler. Using some additional tricks (sparse power series and an algorithm of Chudnovsky for factorials), he manages to reduce the computation of the zeta function to time

$$p^{0.5+\epsilon} d^{n^2+O(n)} a^{n+O(1)},$$

where $q = p^a$ and d is the degree of $X \subset \mathbb{P}^n$.

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?

David Harvey.
Computing zeta functions of projective hypersurfaces in large characteristic.
Conference talk, available at `http://www.crm.umontreal.ca/Points10/pdf/Harvey_slides.pdf`, April 2010.

Kiran S. Kedlaya.
Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology.
Journal of the Ramanujan Mathematical Society, 16:323–338, 2001.