Counting points on (more general) curves

Jan Tuitman, KU Leuven

May 21, 2014

Zeta functions

Suppose that

- $\mathbf{F}_q$ finite field of cardinality $q = p^n$.
- $X/\mathbf{F}_q$ a smooth proper algebraic curve of genus g.

Recall that the zeta function of X is defined as

$$Z(X, T) = \exp(\sum_{i=1}^{\infty} |X(\mathbf{F}_{q^i})| \frac{T^i}{i}).$$

It follows from the Weil conjectures that $Z(X, T)$ is of the form

$$\frac{\chi(T)}{(1-T)(1-qT)},$$

where $\chi(T) \in \mathbf{Z}[T]$ of degree $2g$, with inverse roots that

- have absolute value $q^{\frac{1}{2}}$
- are permuted by the map $x \to q/x$.

Computing zeta functions

Problem

How to compute $Z(X, T)$ (efficiently)?

Note that this problem has cryptographic applications when X is a (hyper)elliptic curve.

Theorem

Let F_p denote the pth power Frobenius map and $H^*_{rig}(X)$ the rigid cohomology. Then

$$\chi(T) = \det(1 - T\,\mathrm{F}_p^n \,|H^1_{rig}(X)).$$

Hyperelliptic curves

We first consider hyperelliptic curves.

Suppose that $p \neq 2$. A hyperelliptic curve X is given by an (affine) equation of the form

$$y^2 = Q(x),$$

with $Q \in \mathbf{F}_q[x]$ a monic polynomial of degree $2g+1$ with $\gcd(Q, Q') = 1$.

To define $H^1_{\mathrm{rig}}(X)$, we start by lifting Q to characteristic 0:

Let $\mathcal{Q} \in \mathbf{Z}_q[x]$ denote a monic lift of Q of degree $2g+1$.

Some rings

We define a ring $\mathbf{Z}_q\langle x, y, y^{-1}\rangle^\dagger$ of overconvergent functions:

$$\{\sum_{i=0}^{\infty}\sum_{j=-\infty}^{\infty} a_{i,j}x^i y^j | a_{i,j} \in \mathbf{Z}_q, \exists \rho > 1\colon \lim_{i+|j|\to\infty} |a_{i,j}|\rho^i = 0\}.$$

Moreover, we denote

$$\mathcal{R} = \mathbf{Z}_q[x, y, y^{-1}]/(y^2 - \mathcal{Q}), \quad \mathcal{R}^\dagger = \mathbf{Z}_q\langle x, y, y^{-1}\rangle^\dagger/(y^2 - \mathcal{Q}),$$

$$\mathcal{U} = \operatorname{Spec}\mathcal{R}, \qquad \mathbb{U} = \mathcal{U} \otimes \mathbf{Q}_q, \qquad U = \mathcal{U} \otimes \mathbf{F}_q.$$

Rigid cohomology

We define the overconvergent Kähler differentials

$$\Omega^1_{\mathcal{R}^\dagger} = \frac{R^\dagger dx \oplus R^\dagger dy}{(2ydy - \mathcal{Q}' dx)}$$

and the overconvergent De Rham complex

$$\Omega^\bullet_{\mathcal{R}^\dagger} : \quad 0 \longrightarrow \mathcal{R}^\dagger \xrightarrow{d} \Omega_{\mathcal{R}^\dagger} \longrightarrow 0.$$

We then have

$$H^1_{\mathrm{rig}}(U) = H^1(\Omega^\bullet_{\mathcal{R}^\dagger} \otimes \mathbf{Q}_q) = \operatorname{coker}(d) \otimes \mathbf{Q}_q.$$

Frobenius lift

The pth power Frobenius map on $\mathcal{R} \otimes \mathbf{F}_q$ can be lifted to $\mathcal{R}$.

If $\sigma \in \mathrm{Gal}(\mathbf{Q}_q/\mathbf{Q}_p)$ denotes the unique lift of the pth power Frobenius map on $\mathbf{F}_q$, then

$$F_p(y)^2 = \mathcal{Q}^\sigma(F_p(x)).$$

So we define

$$\begin{aligned} F_p(x) &= x^p, \\ F_p(y) &= \mathcal{Q}^\sigma(x^p)^{\frac{1}{2}} = y^p\Big(1 + \frac{\mathcal{Q}^\sigma(x^p) - \mathcal{Q}(x)^p}{y^{2p}}\Big)^{\frac{1}{2}}. \end{aligned}$$

The square root can be computed efficiently by Hensel lifting.

Computing in the cohomology

We can write any 1-form $\omega \in \Omega_{\mathcal{R}^\dagger}$ as

$$\sum_{i=-\infty}^{\infty} \frac{a_i(x)}{y^i} dx,$$

with $a_i \in \mathbf{Z}_q[x]$ of degree $< 2g+1$ for all $i \in \mathbf{Z}$. Writing $B(x) = A_1(x)\mathcal{Q}(x) + A_2(x)Q'(x)$, we have

$$B(x)\frac{dx}{y^i} \equiv \left(A_1(x) + \frac{2A_2'(x)}{(i-2)}\right)\frac{dx}{y^{i-2}}.$$

This allows us to eliminate all terms with $i > 2$. We can do something similar for the terms with $i \leq 0$.

A basis for the cohomology

As a consequence, one can show that:

Theorem

A basis for $H^1_{rig}(U)$ is given by

$$[x^0 \frac{dx}{y}, \ldots, x^{2g-1} \frac{dx}{y}, x^0 \frac{dx}{y^2}, \ldots, x^{2g} \frac{dx}{y^2}]$$

and the first $2g$ vectors form a basis for the subspace $H^1_{rig}(X)$.

Kedlaya's algorithm

Kedlaya, *'Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology'* (2001):

- Compute $F_p(\frac{1}{y})$ and $F_p(x^i \frac{dx}{y}) = px^{ip+p-1} F_p(\frac{1}{y}) dx$.
- Reduce back to the basis $[x^0 \frac{dx}{y}, \ldots, x^{2g-1} \frac{dx}{y}]$ and read off the matrix Φ of F_p on $H^1_{\mathrm{rig}}(X)$.
- Compute the matrix $\Phi^{(n)} = \Phi^{\sigma^{n-1}} \ldots \Phi^{\sigma} \Phi$ of F_p^n on $H^1_{\mathrm{rig}}(X)$.
- Determine $\chi(T) = \det(1 - \mathrm{F}_p^n T | H^1_{\mathrm{rig}}(X))$.

The polynomial $\chi(T) = \sum_{i=0}^{2g} \chi_i T^i \in \mathbf{Z}[T]$ is determined exactly if known to high enough p-adic precision, since there are explicit bounds for the size of its coefficients.

More general curves

We let $X/\mathbf{F}_q$ denote the smooth projective curve birational to

$$Q(x,y) = y^{d_x} + Q_{d-1}(x)y^{d_x-1} + \ldots + Q_0 = 0,$$

where $Q(x,y)$ is irreducible separable and $Q_i(x) \in \mathbf{F}_q[x]$ for all $0 \leq i \leq d_x - 1$.

We let $\mathcal{Q} \in \mathbf{Z}_q[x]$ denote a lift of Q that is monic of degree d_x in y.

Proposition

The $\mathbf{Z}_q[x]$*-module* $\mathbf{Z}_q[x,y]/(\mathcal{Q})$ *is free with basis* $[1, y, \ldots, y^{d_x-1}]$.

Some notation

Definition

We let $\Delta(x) \in \mathbf{Z}_q[x]$ denote the resultant of $\mathcal{Q}$ and $\frac{\partial \mathcal{Q}}{\partial y}$ with respect to the variable y and $r(x) \in \mathbf{Z}_q[x]$ the squarefree polynomial $r = \Delta/(\gcd(\Delta, \frac{d\Delta}{dx}))$.

Note that $\Delta(x) \neq 0 \pmod{p}$ since the map x is separable.

Definition

$$\mathcal{S} = \mathbf{Z}_q[x, \frac{1}{r}], \qquad \mathcal{R} = \mathbf{Z}_q[x, \frac{1}{r}, y]/(\mathcal{Q}),$$
$$\mathcal{S}^\dagger = \mathbf{Z}_q\langle x, \frac{1}{r}\rangle^\dagger, \qquad \mathcal{R}^\dagger = \mathbf{Z}_q\langle x, \frac{1}{r}, y\rangle^\dagger/(\mathcal{Q}),$$

and write $\mathcal{V} = \operatorname{Spec} \mathcal{S}$, $\mathcal{U} = \operatorname{Spec} \mathcal{R}$, so that x defines a finite étale morphism from $\mathcal{U}$ to $\mathcal{V}$.

Assumptions

Now we need some assumptions.

Assumption

1. *There exists a smooth proper curve* $\mathcal{X}$ *over* $\mathbf{Z}_q$ *and a smooth relative divisor* $\mathcal{D}_{\mathcal{X}}$ *on* $\mathcal{X}$ *such that* $\mathcal{U} = \mathcal{X} \setminus \mathcal{D}_{\mathcal{X}}$. *We write* $\mathbb{X} = \mathcal{X} \otimes \mathbf{Q}_q$ *for the generic fibre of* $\mathcal{X}$.
2. *There exists a smooth relative divisor* $\mathcal{D}_{\mathbf{P}^1}$ *on* $\mathbf{P}^1_{\mathbf{Z}_q}$ *such that* $\mathcal{V} = \mathbf{P}^1_{\mathbf{Z}_q} \setminus \mathcal{D}_{\mathbf{P}^1}$.

Definition

We let $U = \mathcal{U} \otimes_{\mathbf{Z}_q} \mathbf{F}_q$, $V = \mathcal{V} \otimes_{\mathbf{Z}_q} \mathbf{F}_q$ *denote the special fibres and* $\mathbb{U} = \mathcal{U} \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$, $\mathbb{V} = \mathcal{V} \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$ *the generic fibres of* $\mathcal{U}$ *and* $\mathcal{V}$, *respectively.*

More assumptions

Assumption

We assume that the zero locus of $\mathcal{Q}$ *in* $\mathbf{A}^2_{\mathbf{Z}_q}$ *is smooth over* $\mathbf{Z}_q$.

Assumption

We assume that a matrix $W^{\infty} \in Gl_{d_x}(\mathbf{Z}_q[x, x^{-1}])$ *is known such that if we denote*

$$b_j^{\infty} = \sum_{i=0}^{d_x-1} W^{\infty}_{i+1,j+1} y^i,$$

then $[b_0^{\infty}, \ldots, b_{d_x-1}^{\infty}]$ *is an integral basis for the function field* $\mathbf{Q}_q(x, y)$ *over* $\mathbf{Q}_q[x^{-1}]$.

An auxiliary polynomial

Proposition

The element $s = r/\frac{\partial \mathcal{Q}}{\partial y}$ of $\mathbf{Q}_q(x,y)$ is contained in $\mathbf{Z}_q[x,y]/(\mathcal{Q})$.

Sketch of the proof: $\Delta/\frac{\partial \mathcal{Q}}{\partial y}$ is contained in $\mathbf{Z}_q[x,y]/(\mathcal{Q})$ by the definition of Δ as the determinant of the Sylvester matrix. By the assumption, $[1, y, \ldots, y^{d_x-1}]$ is an integral basis of $\mathbf{Q}_q[x,y]/(\mathcal{Q})$ over $\mathbf{Q}_q[x]$. So for any monic irreducible polynomial $\pi \in \mathbf{Z}_q[x]$, the element $\frac{\partial \mathcal{Q}}{\partial y}/\pi$ of $\mathbf{Q}_q(x,y)$ is not integral at (π) because of the term $(d/\pi)y^{d_x-1}$, hence its inverse $\pi/\frac{\partial \mathcal{Q}}{\partial y}$ is integral (even zero) at (π). Since $\prod_{\pi|\Delta} \pi = r$, this proves the Proposition.

Rigid cohomology

Again we define the overconvergent Kähler differentials

$$\Omega^1_{\mathcal{R}^\dagger} = \frac{R^\dagger dx \oplus R^\dagger dy}{d\mathcal{Q}}$$

and the overconvergent De Rham complex

$$\Omega^\bullet_{\mathcal{R}^\dagger}: \quad 0 \longrightarrow \mathcal{R}^\dagger \xrightarrow{d} \Omega_{\mathcal{R}^\dagger} \longrightarrow 0.$$

We then still have

$$H^1_{\mathrm{rig}}(U) = H^1(\Omega^\bullet_{\mathcal{R}^\dagger} \otimes \mathbf{Q}_q) = \mathrm{coker}(d) \otimes \mathbf{Q}_q.$$

Frobenius lift

Define sequences $(\alpha_i)_{i\geq 0}$, $(\beta_i)_{i\geq 0}$, with $\alpha_i \in S^\dagger$ and $\beta_i \in \mathcal{R}^\dagger$, by the following recursion:

$$\begin{aligned}
\alpha_0 &= \frac{1}{r^p}, \\
\beta_0 &= y^p, \\
\alpha_{i+1} &= \alpha_i(2 - \alpha_i r^\sigma(x^p)) && \pmod{p^{2^{i+1}}}, \\
\beta_{i+1} &= \beta_i - \mathcal{Q}^\sigma(x^p, \beta_i) s^\sigma(x^p, \beta_i)\alpha_i && \pmod{p^{2^{i+1}}}.
\end{aligned}$$

Then one easily checks that the σ-semilinear ringhomomorphism $\mathrm{F}_p : \mathcal{R}^\dagger \to \mathcal{R}^\dagger$ defined by

$$\mathrm{F}_p(x) = x^p, \qquad \mathrm{F}_p(\frac{1}{r}) = \lim_{i\to\infty} \alpha_i, \qquad \mathrm{F}_p(y) = \lim_{i\to\infty} \beta_i,$$

is a Frobenius lift.

The connection matrix

Definition

Let $G \in M_{d_x \times d_x}(\mathbf{Z}_q[x, 1/r])$ *denote the matrix such that*

$$d(y^j) = jy^{j-1}dy = -jy^{j-1}\frac{s}{r}\frac{\partial \mathcal{Q}}{\partial x}dx = \sum_{i=0}^{d_x-1} G_{i+1,j+1}y^i dx.$$

Note that Gdx *has at most a simple pole at the zeros of* r*.*

Proposition

Let $G^\infty \in M_{d_x \times d_x}(\mathbf{Z}_q[x, x^{-1}, 1/r])$ *denote the matrix such that*

$$db_j^\infty = \sum_{i=0}^{d_x-1} G^\infty_{i+1,j+1} b_i^\infty dx.$$

Then $G^\infty dx$ *has at most a simple pole at* $x = \infty$*.*

The exponents

Definition

Let $x_0 \in \mathbf{P}^1(\bar{\mathbf{Q}}_q)$ be a geometric point $\neq \infty$. The exponents of $G dx$ at x_0 are defined as the eigenvalues of the residue matrix $(x - x_0)G|_{x=x_0}$. The exponents of $G^{\infty} dx$ at ∞ are defined as its exponents at $t = 0$, after substituting $x = 1/t$.

Proposition

The exponents of $G dx$ at any point $x_0 \neq \infty$ and the exponents of $G^{\infty} dx$ at $x = \infty$ are elements of $\mathbf{Q} \cap \mathbf{Z}_p$ and are contained in the interval $[0, 1)$.

Effective convergence bounds

Proposition

Let $N \in \mathbf{N}$. Then modulo p^N:

1. $\mathrm{F}_p(1/r)$ *is congruent to* $\sum_{i=p}^{pN} \frac{\rho_i(x)}{r^i}$*, where for all* $p \leq i \leq pN$ *the polynomial* $\rho_i \in \mathbf{Z}_q[x]$ *satisfies* $\deg(\rho_i) < \deg(r)$.
2. $\mathrm{F}_p(y^i)$ *is congruent to* $\sum_{j=0}^{d_x-1} \phi_{i,j}(x) y^j$*, where*

$$\phi_{i,j} = \sum_{k=0}^{p(N-1)} \frac{\phi_{i,j,k}(x)}{r^k},$$

and $\phi_{i,j,k} \in \mathbf{Z}_q[x]$ *satisfies:*
$\deg(\phi_{i,j,0}) < -\operatorname{ord}_\infty(W^\infty) - p\operatorname{ord}_\infty((W^\infty)^{-1})$,
$\deg(\phi_{i,j,k}) < \deg(r)$*, for all* $k > 0$.

Sketch of the proof: Effective bounds for Frobenius structures on connections, T. and Kedlaya, 2013.

Computing in the cohomology: finite points

Proposition

For all $\ell \in \mathbf{N}$ and every vector $w \in \mathbf{Q}_q[x]^{\oplus d_x}$, there exist vectors $u, v \in \mathbf{Q}_q[x]^{\oplus d_x}$ with $\deg(v) < \deg(r)$, such that

$$\frac{\sum_{i=0}^{d_x-1} w_i y^i}{r^{\ell}} \frac{dx}{r} = d\left(\frac{\sum_{i=0}^{d_x-1} v_i y^i}{r^{\ell}}\right) + \frac{\sum_{i=0}^{d_x-1} u_i y^i}{r^{\ell-1}} \frac{dx}{r}.$$

Sketch of the proof: r is separable, so r' is invertible in $\mathbf{Q}_q[x]/(r)$. v has to satisfy $\left(\frac{M}{r'} - \ell I\right) v \equiv \frac{u}{r'} \pmod r$ over $\mathbf{Q}_q[x]/(r)$. The finite exponents of $G dx = (M/r)dx$ are contained in $[0,1)$, hence $\det(\ell I - M/r')$ is invertible in $\mathbf{Q}_q[x]/(r)$, so there is a unique solution v. We now take

$$u = \frac{w - \left(M - \ell r' I\right) v}{r} - \frac{dv}{dx}.$$

Computing in the cohomology: infinite points

Proposition

For every vector $w \in \mathbf{Q}_q[x, x^{-1}]^{\oplus d_x}$ *with*

$$\mathrm{ord}_\infty(w) \leq -\deg(r),$$

there exist vectors $u, v \in \mathbf{Q}_q[x, x^{-1}]^{\oplus d_x}$ *with* $\mathrm{ord}_\infty(u) > \mathrm{ord}_\infty(w)$, *such that*

$$\Big(\sum_{i=0}^{d_x-1} w_i b_i^\infty\Big)\frac{dx}{r} = d\Big(\sum_{i=0}^{d_x-1} v_i b_i^\infty\Big) + \Big(\sum_{i=0}^{d_x-1} u_i b_i^\infty\Big)\frac{dx}{r}.$$

Precision loss: finite points

Proposition

Let $\omega \in \Omega^1(\mathcal{U})$ *be of the form*

$$\omega = \frac{\sum_{i=0}^{d_x-1} w_i y^i}{r^\ell} \frac{dx}{r},$$

where $\ell \in \mathbf{N}$ *and* $\deg(w) < \deg(r)$. *We define*

$$e = \max\{e_P | P \in \mathcal{X} \setminus \mathcal{U}, x(P) \neq \infty\}.$$

If we represent the class of ω *in* $H^1_{rig}(U)$ *by* $\left(\sum_{i=0}^{d_x-1} u_i y^i\right) \frac{dx}{r}$, *with* $u \in \mathbf{Q}_q[x]^{\oplus d_x}$, *then*

$$p^{\lfloor \log_p(\ell e) \rfloor} u \in \mathbf{Z}_q[x]^{\oplus d_x}.$$

Precision loss: infinite points

Proposition

Let $\omega \in \Omega^1(\mathcal{U})$ *be of the form*

$$\omega = (\sum_{i=0}^{d_x-1} w_i(x, x^{-1}) b_i^{\infty}) \frac{dx}{r},$$

with $\mathrm{ord}_{\infty}(w) \leq \mathrm{ord}_0(W^{\infty}) - \deg(r) + 1$*. Put*

$$m = -\mathrm{ord}_{\infty}(w) - \deg(r) + 1, e_{\infty} = \max\{e_P | P \in \mathcal{X} \setminus \mathcal{U}, x(P) = \infty\}.$$

If we represent the class of ω *in* $H^1_{rig}(U)$ *by* $\left(\sum_{i=0}^{d_x-1} u_i y^i\right) \frac{dx}{r}$*, with* $u \in \mathbf{Q}_q[x, x^{-1}]^{\oplus d_x}$ *such that* $\mathrm{ord}_{\infty}(u) > \mathrm{ord}_0(W^{\infty}) - \deg(r) + 1$*, then*

$$p^{\lfloor \log_p(m e_{\infty}) \rfloor} u \in \mathbf{Z}_q[x, x^{-1}]^{\oplus d_x}.$$

Computing a basis for $H^1_{\mathrm{rig}}(U)$

We can use these theorems to compute a basis for the cohomology using linear algebra.

Theorem

Define the following $\mathbf{Q}_q$*-vector spaces:*

$$E_0 = \{ (\sum_{i=0}^{d_x-1} u_i(x) y^i) \frac{dx}{r} \quad : u \in \mathbf{Q}_q[x]^{\oplus d_x} \},$$

$$E_\infty = \{ (\sum_{i=0}^{d_x-1} u_i(x,x^{-1}) b_i^\infty) \frac{dx}{r} \quad : u \in \mathbf{Q}_q[x,x^{-1}]^{\oplus d_x}, \mathrm{ord}_\infty(u) > \mathrm{ord}_0(W^\infty) - \deg(r) + 1 \},$$

$$B_0 = \{ \sum_{i=0}^{d_x-1} v_i(x) y^i \quad : v \in \mathbf{Q}_q[x]^{\oplus d_x} \},$$

$$B_\infty = \{ \sum_{i=0}^{d_x-1} v_i(x,x^{-1}) b_i^\infty \quad : v \in \mathbf{Q}_q[x,x^{-1}]^{\oplus d_x}, \mathrm{ord}_\infty(v) > \mathrm{ord}_0(W^\infty) \}.$$

Then $E_0 \cap E_\infty$ *and* $d(B_0 \cap B_\infty)$ *are finite dimensional* $\mathbf{Q}_q$*-vector spaces and*

$$H^1_{rig}(U) \cong (E_0 \cap E_\infty) / d(B_0 \cap B_\infty).$$

Some remarks

Computing a basis for $H^1_{\mathrm{rig}}(U)$ is now a matter of linear algebra. Any 1-form on $\mathbb{U}$ can be reduced to this basis using the theorems above. We can also recover $H^1_{\mathrm{rig}}(X)$ inside $H^1_{\mathrm{rig}}(U)$ as the kernel of a *cohomological residue map*.

We have now generalised all the steps in Kedlaya's algorithm (lifting Frobenius, computing in cohomology, bounding the loss of p-adic precision) from hyperelliptic curves to much more general curves.

Our assumptions can be weakened. We only need a good lift of the curve and integral bases for the function field $\mathbf{Q}_q(x, y)$ over $\mathbf{Q}_q[x]$ and $\mathbf{Q}_q[x^{-1}]$, respectively. Therefore, our approach works for just about *any* curve.

The algorithm

Let d_x, d_y be the degrees of $\mathcal{Q}$ in y, x, respectively. Moreover, recall that $q = p^n$ with p prime. The runtime of our algorithm is:

$$\tilde{\mathcal{O}}(p d_x^6 d_y^4 n^3).$$

Note that for d_x fixed this is $\tilde{\mathcal{O}}(p d_y^4 n^3)$ like Kedlaya's algorithm.

We have completed a MAGMA implementation of the algorithm (under the assumptions in this presentation) that is very efficient in practice.

preprint: `http://arxiv.org/abs/1402.6758`.

code: `pcc_p` and `pcc_q` packages at

`https://perswww.kuleuven.be/jan_tuitman`.