Recent developments in point counting

Jan Tuitman, KU Leuven

June 6, 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

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

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 (of genus at most 2).

Theorem

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

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

Some notation

Suppose that $p \neq 2$. A hyperelliptic curve $X/\mathbf{F}_q$ (with a rational Weierstrass point) is a smooth projective curve 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 $\gcd(Q, Q') = 1$.

$\mathbf{Q}_q$ denotes the unique unramified extension of $\mathbf{Q}_p$ of degree n and $\sigma \in Gal(\mathbf{Q}_q/\mathbf{Q}_p)$ the unique lift of the p-th power Frobenius on $\mathbf{F}_q$.

Recall that the rigid cohomology $H^1_{\text{rig}}(X)$ is a finite dimensional $\mathbf{Q}_q$-vector space with a σ-semilinear action of F_p.

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 $[x^0 \frac{dx}{y}, \ldots, x^{2g-1} \frac{dx}{y}]$ of $H^1_{\mathrm{rig}}(X)$ 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 $0 \leq i \leq d_x - 1$.

Recall that $\mathbf{Z}_q$ denotes the ring of integers of $\mathbf{Q}_q$.

Let $\mathcal{Q} \in \mathbf{Z}_q[x]$ be 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* 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. We denote*

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

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 I

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 $\mathcal{U} = \mathcal{X} \setminus \mathcal{D}_{\mathcal{X}}$.*
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 of $\mathcal{U}$, $\mathcal{V}$ and $\mathbb{U} = \mathcal{U} \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$, $\mathbb{V} = \mathcal{V} \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$, $\mathbb{X} = \mathcal{X} \otimes_{\mathbf{Z}_q} \mathbf{Q}_q$ the generic fibres of $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{X}$.

Assumptions II

Assumption

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

Assumption

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

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

then $[b^{\infty}_0, \ldots, b^{\infty}_{d_x - 1}]$ is an integral basis for the function field $\mathbf{Q}_q(x, y)$ of $\mathbb{X}$ over $\mathbf{Q}_q[x^{-1}]$.

An auxiliary polynomial

Proposition

There exists $s \in \mathbf{Z}_q[x,y]$ such that

$$\frac{s}{r} = \frac{1}{\frac{\partial \mathcal{Q}}{\partial y}}$$

as elements of the function field $\mathbf{Q}_q(x,y)$ of $\mathbb{X}$.

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.

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.

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.

Rigid cohomology

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 have

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

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: 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. Since r is separable, its derivative r' is invertible in $\mathbf{Q}_q[x]/(r)$. One checks that v has to satisfy $\left(\frac{rG}{r'} - \ell I\right)v \equiv \frac{u}{r'} \pmod r$ over $\mathbf{Q}_q[x]/(r)$. The finite exponents of Gdx 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

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

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*

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

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*

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

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 $H^1_{\mathrm{rig}}(U)$

Theorem

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

$$
\begin{aligned}
E_0 &= \{ \Big(\sum_{i=0}^{d_x-1} u_i(x) y^i \Big) \frac{dx}{r} &&: u \in \mathbf{Q}_q[x]^{\oplus d_x} \}, \\
E_\infty &= \{ \Big(\sum_{i=0}^{d_x-1} u_i(x, x^{-1}) b_i^\infty \Big) \frac{dx}{r} &&: u \in \mathbf{Q}_q[x, x^{-1}]^{\oplus d_x}, \mathrm{ord}_\infty(u) > \mathrm{ord}_0(W^\infty) - \deg(r) + 1 \}, \\
B_0 &= \{ \sum_{i=0}^{d_x-1} v_i(x) y^i &&: v \in \mathbf{Q}_q[x]^{\oplus d_x} \}, \\
B_\infty &= \{ \sum_{i=0}^{d_x-1} v_i(x, x^{-1}) b_i^\infty &&: v \in \mathbf{Q}_q[x, x^{-1}]^{\oplus d_x}, \mathrm{ord}_\infty(v) > \mathrm{ord}_0(W^\infty) \}.
\end{aligned}
$$

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

- A basis for $H^1_{\text{rig}}(U)$ can now be computed by linear algebra. Any 1-form on $\mathbb{U}$ can be reduced to this basis using the theorems above. We recover $H^1_{\text{rig}}(X)$ inside $H^1_{\text{rig}}(U)$ as the kernel of a *cohomological residue map*.
- We have generalised all the steps in Kedlaya's algorithm (lifting Frobenius, computing in cohomology, bounding the loss of p-adic precision) to much more general curves.
- Our assumptions can be weakened. We need a good lift of the curve and integral bases for the function field $\mathbf{Q}_q(x, y)$ of $\mathbb{X}$ 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:

$$\mathcal{O}(p^{1+\epsilon} d_x^{6+\epsilon} d_y^{4+\epsilon} n^{3+\epsilon}).$$

Note that for d_x fixed this is $\mathcal{O}(p^{1+\epsilon} d_y^{4+\epsilon} n^{3+\epsilon})$ 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`.

We return to the case of hyperelliptic curves.

Let p be an odd prime, take $q = p^n$ and let $X/\mathbf{F}_q$ denote the smooth projective curve defined by

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

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

Kedlaya's algorithm runs in time $\mathcal{O}(p^{1+\epsilon} g^{4+\epsilon} n^{3+\epsilon})$. So the runtime is *polynomial* in g, n but *exponential* in $\log(p)$. In practice the algorithm is therefore restricted to rather small values of p.

Harvey has improved this situation in two ways.

$\mathcal{O}(p^{1/2+\epsilon})$ algorithm

Let ω be a real number such that two $\ell \times \ell$ matrices over a ring R can be multiplied in $\mathcal{O}(\ell^{\omega+\epsilon})$ ring operations in R, for example $\omega = 2.3729$.

Theorem (Harvey, 2007)

Kedlaya's algorithm can be modified to run in time

$$\mathcal{O}(p^{1/2+\epsilon} g^{\omega+5/2+\epsilon} n^{7/2+\epsilon} + \log(p)^{1+\epsilon} g^{8+\epsilon} n^{5+\epsilon}),$$

which in particular is $\mathcal{O}(p^{1/2+\epsilon})$ *for fixed* g, n *(instead of* $\mathcal{O}(p^{1+\epsilon})$*).*

Remark

This algorithm is implemented in SAGE for the case $n = 1$*.*

Hyperelliptic curves over $\mathbf{Q}$

Now let $X/\mathbf{Q}$ denote the smooth projective curve defined by

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

with $Q \in \mathbf{Z}[x]$ a monic squarefree polynomial of degree $2g + 1$ with coefficients bounded in absolute value by B.

For any odd prime not dividing the discriminant of Q, let $X_p/\mathbf{F}_p$ be the hyperelliptic curve that is the reduction of X modulo p.

Average polynomial time algorithm

Theorem (Harvey, 2013)

Kedlaya's algorithm can be modified to return the zeta function of X_p for all odd $p < N$ not dividing the discriminant of Q in time

$$\mathcal{O}(g^{8+\epsilon} N \log^2(N) \log^{1+\epsilon}(BN)).$$

Since the number of primes $p < N$ is asymptotically $N/\log(N)$, the average time spent per prime is

$$\mathcal{O}(g^{8+\epsilon} \log^3(N) \log^{1+\epsilon}(BN)),$$

which in particular is polynomial in the size of the input.

Sketch of Harvey's methods I

Kedlaya:

$$\begin{aligned} F_p(x^i dx/y) &= p x^{ip+p-1} F_p(1/y) dx \\ &= p x^{ip+p-1} y^{-p} \left(1 + \frac{\mathcal{Q}^{\sigma}(x^p) - \mathcal{Q}(x)^p}{y^{2p}}\right)^{-\frac{1}{2}} dx \\ &= p x^{ip+p-1} y^{-p} \sum_{k=0}^{\infty} \binom{-1/2}{k} \frac{\left(\mathcal{Q}^{\sigma}(x^p) - \mathcal{Q}(x)^p\right)^k}{y^{2pk}} \end{aligned}$$

Problem: expanding this modulo p^m we get $\sim pm$ terms.

Sketch of Harvey's methods II

Theorem

Suppose that $p > (2m-1)(2g+1)$ and define:

$$
\begin{aligned}
C_{j,r} &= \text{ the coefficient of } x^r \text{ in } \mathcal{Q}(x)^j, \\
\alpha_j &= \sum_{k=j}^{m-1} (-1)^{k+j} \binom{-1/2}{k} \binom{k}{j} && \text{for } 0 \leq j < m, \\
T_i &= \sum_{j=0}^{m-1} \sum_{r=0}^{(2g+1)j} p C_{j,r}^{\sigma} \alpha_j x^{p(i+r+1)-1} y^{-p(2j+1)+1} \frac{dx}{y} && \text{for } 0 \leq i < 2g.
\end{aligned}
$$

Then modulo p^m we have $F_p(x^i dx/y) \equiv T_i$ in $H^1_{rig}(X)$.

Remark

The number of terms of T_i does not depend on p.

Sketch of Harvey's methods III

Let $U_p^{a,b}$ denote the reduction of $x^{pa-1}y^{-pb-1}dx/y$ in $H^1_{\text{rig}}(X)$. Note that is what remains to be computed.

$U_p^{a,b}$ can be computed by computing a matrix product $M_1^{a,b}M_2^{a,b}\cdots M_p^{a,b}$, where the $M_i^{a,b}$ are matrices of size $\mathcal{O}(g)$ over $\mathbf{Z}_q[x]$.

- Using a baby step - giant step approach to compute the products $M_1^{a,b}M_2^{a,b}\cdots M_p^{a,b}$ yields the $\mathcal{O}(p^{1/2+\epsilon})$ algorithm.
- For a hyperelliptic curve over $\mathbf{Q}$, different products $M_1^{a,b}M_2^{a,b}\cdots M_{p_1}^{a,b}$ and $M_1^{a,b}M_2^{a,b}\cdots M_{p_2}^{a,b}$ for primes $p_1, p_2 < N$ have some overlap. Exploiting this (using accumulating remainder trees) yields the average polynomial time algorithm.