Counting points with the deformation method

Jan Tuitman, KU Leuven,
(joint work with S. Pancratz)

September 26, 2013

Counting points

- $\mathbf{F}_q$ finite field with $q = p^a$ elements,
- $X/\mathbf{F}_q$ smooth hypersurface of degree d in $\mathbf{P}^n_{\mathbf{F}_q}$

Definition

$$Z(X, T) = \exp\left(\sum_{i=1}^{\infty} |X(\mathbf{F}_q^i)| \frac{T^i}{i}\right) \quad (\in \mathbf{Q}(T))$$

Problem

Compute $Z(X, T)$ efficiently.

p-adic cohomology

One can define rigid cohomology spaces $H^*_{\mathrm{rig}}(X)$ over $\mathbf{Q}_q$ with an action of the p-th power Frobenius F_p such that

Theorem

$$Z(X,T) = \prod_{i=0}^{2(n-1)} \det(1 - T\,\mathrm{F}_p^a\,|H^i(X))^{(-1)^i}.$$

Since X is a smooth projective hypersurface, we only have to compute

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

Cohomology of a family

Now we take a **family** of smooth projective hypersurfaces

$$\pi : X \to S,$$

defined over some open subset $S \subset \mathbf{P}^1_{\mathbf{F}_q}$ by $\bar{f} \in \mathbf{F}_q[t][x_0, \dots x_n]$ homogeneous of degree d in the variables $x_0, \dots, x_n$.

The cohomology spaces $H^{n-1}_{\mathrm{rig}}(X_s)$ glue together to form an overconvergent F-isocrystal $H^{n-1}_{\mathrm{rig}}(X/S)$.

More concretely, let $f \in \mathbf{Z}_q[t][x_0, \dots, x_n]$ be a lift of $\bar{f}$ to characteristic 0 and

$$\pi : \mathcal{X} \to \mathcal{S}$$

the corresponding family of hypersurfaces.

The Gauss–Manin connection

Basically, $H^{n-1}_{\mathrm{rig}}(X/S)$ is just the algebraic de Rham cohomology

$$H^{n-1}_{\mathrm{dR}}(\mathcal{X}/\mathcal{S} \otimes \mathbf{Q}_q),$$

which carries a natural Gauss–Manin connection ∇. Let $[e_1, \ldots e_b]$ be a basis of sections of $H^{n-1}_{\mathrm{dR}}(\mathcal{X}/\mathcal{S} \otimes \mathbf{Q}_q)$ and $M(t)$ the matrix of ∇ with respect to this basis:

$$\nabla(e_j) = \sum_{i=1}^{b} M_{ij} e_i \otimes dt.$$

Note that $M \in M_{b\times b}(\mathbf{Q}_q(t))$ can be computed using linear algebra with the Griffiths-Dwork method. Let $r(t) \in \mathbf{Z}_q[t]$ be such that $r(t)M \in M_{b\times b}(\mathbf{Z}_q[t])$.

The Frobenius structure

We denote

$$\mathbf{Q}_q\langle t, \frac{1}{r(t)}\rangle^\dagger = \{\sum_{i,j=0}^{\infty} a_{i,j}\frac{t^i}{r(t)^j} | \exists \rho > 1 \colon \lim_{i+j\to\infty} |a_{i,j}|\rho^{i+j} = 0\}$$

and let σ be the standard p-th power Frobenius lift on this ring.

Theorem

There exists a matrix $\Phi \in M_{b\times b}(\mathbf{Q}_q\langle t, \frac{1}{r(t)}\rangle^\dagger)$ such that if $\hat{\tau} \in \mathcal{S}(\mathbf{Z}_q)$ denotes a Teichmueller lift of $\tau \in S(\mathbf{F}_q)$, then $\Phi(\hat{\tau})$ is the matrix of F_p on $H^{n-1}(X_\tau)$.

The differential equation

Theorem

$$\frac{d\Phi}{dt} + M\Phi = pt^{p-1}\Phi\sigma(M).$$

Suppose that $r(0) \neq 0 \pmod{p}$ and let $C \in M_{b\times b}(\mathbf{Q}_q[[t]])$ be a fundamental matrix of solutions of ∇ at 0:

$$\frac{dC}{dt} + MC = 0, \qquad C(0) = I.$$

Then

$$\Phi = C(t)\Phi(0)\sigma(C^{-1}).$$

When evaluating Φ at $\hat{\tau}$, first convert to an element of $\mathbf{Q}_q\langle t, \frac{1}{r(t)}\rangle^\dagger$, since the power series only converges on the open unit disk.

The deformation method

Lauder(2004) proposes the following algorithm:

- Choose a family X/S for which X_0 is diagonal and X_τ more complicated.
- Compute $\Phi(0)$ using an explicit formula of Dwork.
- Solve for $C(t)$ and compute $\Phi = C\Phi(0)\sigma(C^{-1})$.
- Evaluate $\Phi(\hat{\tau})$ and deduce $Z(X_\tau, T)$.

Why deformation?

- Time complexity $(pad^n)^{\mathcal{O}(1)}$, which is polynomial in the input size for fixed p. AKR and Lauder-Wan have a factor $d^{\mathcal{O}(n^2)}$, so are only polynomial in the input size if n is fixed as well.
- Hubrechts: something similar can be used to lower the space complexity in Kedlaya's algorithm from a^3 to a^2 for (hyper) elliptic curves contained in a family over a small field (for fixed p and g).
- Especially good for big fibres in small families (where big and small refer to the field of definition) and for counting points on a lot of of fibres in the same family.

Our work

- Time complexity:

$$\tilde{O}\left(pa^3 d^{n(\omega+4)} e^{2n} + a^2 \left(d^{n(\omega+2)} e^{n(\omega+1)} + d^{5n} e^{3n}\right)\right),$$

  where ω denotes the least exponent for matrix multiplication, so $2 \leq \omega \leq 2.3727$. This improves Lauder's complexity bound by a factor pd^n.
- We combine all known tricks (Newton Girard identities, Hodge structures, effective convergence bounds for Frobenius structures on connections, effective Christol Dwork bounds) to get the precision bounds to be as low as possible.
- Highly optimised implementation by S.Pancratz in FLINT (starting from a family over $\mathbf{Q}$).

SAGE

Nothing in SAGE yet, what would be needed?

- *LUP* decompositions for large sparse matrices over (for example) $\mathbf{Q}(t)$, to compute the matrix M of ∇.
- For the case when τ is not contained in the prime field, a better implementation of $\mathbf{Q}_q$ is needed. At the moment, things like Teichmueller lifts and σ are about 10^4 times slower in SAGE than in MAGMA.

Both of these problems should be resolved when FLINT 2.4 goes into SAGE.

paper:

'Improvements to the deformation method for counting points on smooth projective hypersurfaces'

http://arxiv.org/abs/1307.1250

code:

https://github.com/SPancratz/deformation