Computing zeta functions of surfaces using p-adic cohomology

AMS Western Section Meeting
San Francisco State University April 30, 2006

Timothy G. Abbott
Kiran S. Kedlaya
David Roe
MIT
Kedlaya: `kedlaya@mit.edu`

Reference: Bounding Picard numbers of surfaces using p-adic cohomology, arXiv: math.NT/0601508.

Kedlaya is supported by NSF grant DMS-0400727. Abbott and Roe were supported by MIT's UROP (Undergraduate Research Opportunities Program) office.

Overview: zeta functions of surfaces

Let X be a smooth projective surface over a finite field $\mathbb{F}_q$. Its zeta function

$$\zeta_X(T) = \prod_{x \in X} (1 - T^{\deg(x)})^{-1} = \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right)$$

factors as

$$\zeta_X(T) = \frac{P_1(T) P_3(T)}{(1-T)(1-q^2T)P_2(T)}$$

where each $P_i(T) \in \mathbb{Z}[T]$ has $P_i(0) = 1$ and all $\mathbb{C}$-roots of absolute value $q^{-i/2}$. Also, if $P_i(r) = 0$, then $P_{4-i}(q^{-2}/r)) = 0$.

Problem: describe an algorithm (given a class of X's) that given X, finds P_1, P_2, P_3. Usually P_1, P_3 are easy, and P_2 is the hard part.

Motivation: Goppa codes

Goppa recipe for error-correcting codes over $\mathbb{F}_q$: take an ample divisor H on X, and form subspace of $\prod_{x \in X \setminus H} \mathbb{F}_q$ given by

$$\{(f(x))_{x \in X \setminus H} : f \in \Gamma(X, \mathcal{O}(-H))\}.$$

Traditionally X is a *curve* with many $\mathbb{F}_q$-points.

Voloch-Zarzar: take X to be a *surface*; get good examples of LDPC (low-density parity check) codes. (The perp space has many short vectors coming from curves on X.)

To control minimum distance, must control Picard number (arithmetic Néron-Severi rank) of X, which is $\leq \operatorname{ord}_{T=1/q} P_2(T)$ (equality under Tate's conjecture).

Weil cohomologies

There are various ways to attach vector spaces $H^i(X)$ equipped with a linear endomorphism F such that

$$P_i(T) = \det(1 - FT, H^i(X)),$$

whence

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{4} (-1)^i \operatorname{Trace}(F^n, H^i(X)).$$

For theorems, one usually uses étale (ℓ-adic) cohomology; but this theory is not practical for algorithms (except on curves of low genus).

We instead use p-adic (crystalline) cohomology, which can be computed explicitly (à la Dwork, Monsky-Washnitzer).

Smooth surfaces in $\mathbb{P}^3$

Let $Q(x, y, z, w)$ be a nonsingular homogeneous polynomial over $\mathbb{F}_p$ and take $X = V(Q)$; then $P_1(T) = P_3(T) = 1$, so the problem is to find P_2.

The p-adic H^2 here is described by a recipe of Griffiths...

The action of Frobenius

...

An example: degree 4 over $\mathbb{F}_3$

Over $\mathbb{F}_3$, take

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

In `Magma`, we compute a Frobenius matrix modulo 3^3, obtaining

$$\begin{aligned}3P_2(T/3) \equiv\ & 3T^{21} + 5T^{20} + 6T^{19} + 7T^{18} + 5T^{17} \\ & + 4T^{16} + 2T^{15} - T^{14} - 3T^{13} - 5T^{12} \\ & - 5T^{11} - 5T^{10} - 5T^{9} - 3T^{8} - T^{7} \\ & + 2T^{6} + 4T^{5} + 5T^{4} + 7T^{3} + 6T^{2} \\ & + 5T + 3 \pmod{3^2}.\end{aligned}$$

This requires 731 CPU-seconds and 53 MB on `dwork`, a Sun workstation with dual Opteron 246 CPUs running at 2 GHz (currently in 32-bit mode) with 2GB of RAM.

An example: degree 4 over $\mathbb{F}_3$ (contd.)

Note that $3P_2(T/3) \in \mathbb{Z}[T]$ by Hodge-Newton polygon comparison, and has $\mathbb{C}$-roots on the unit circle. This *apparently* implies

$$
\begin{aligned}
3P_2(T/3) = {} & 3T^{21} + 5T^{20} + 6T^{19} + 7T^{18} + 5T^{17} \\
& + 4T^{16} + 2T^{15} - T^{14} - 3T^{13} - 5T^{12} \\
& - 5T^{11} - 5T^{10} - 5T^{9} - 3T^{8} - T^{7} \\
& + 2T^{6} + 4T^{5} + 5T^{4} + 7T^{3} + 6T^{2} \\
& + 5T + 3;
\end{aligned}
$$

this is checked by `Maple` code by Andre Wibisono, using floating-point arithmetic. (To fix this, Wibisono is rewriting in `SAGE/Singular` using the real root finding library, which uses only rational numbers.)

Variations

de Jong has C code doing the analogous calculation for surfaces in weighted projective spaces. Still needed: precision estimates.

In progress (with Po-Ning Chen et al.): nondegenerate hypersurfaces in toric varieties. (For curves in toric surfaces, see Castryck-Denef-Vercauteren.)