Computing Zeta Functions of Surfaces

Kiran S. Kedlaya, Massachusetts Institute of Technology

`kedlaya@math.mit.edu`

AGCT-10 (Arithmetic, Geometry, and Coding Theory), CIRM (Luminy)

September 29, 2005

Maybe this talk should be called...

How to Succeed in Coding Theory Without Really Trying

Acknowledgments: the implementation aspect is a joint project with Tim Abbott and David Roe. Abbott and Roe were supported by MIT's Undergraduate Research Opportunities Program; the speaker is supported by NSF grant DMS-0400747.

Some notation

$\mathbb{F}_q$	a finite field
X	a smooth projective surface over $\mathbb{F}_q$
H	a very ample divisor on X
$\mathcal{L}(H)$	$\{f \in \mathbb{F}_q(X) : \mathrm{div}(f) + H \geq 0\}$ (Riemann-Roch space)
S	$X(\mathbb{F}_q) \setminus H(\mathbb{F}_q)$
$C(X, H)$	the code $\{(f(s))_{s \in S} : f \in \mathcal{L}(H)\}$
δ	the minimum distance of $C(X, H)$

Minimal distance and Néron-Severi

Let $\mathrm{NS}(X)$ be the Néron-Severi group of X (divisors modulo algebraic equivalence); then $\mathrm{NS}(X)$ is finitely generated and $\operatorname{rank}\mathrm{NS}(X) \geq 1$ (the class of H is not torsion).

Voloch's talk: upper bounds on $\operatorname{rank}\mathrm{NS}(X)$ give lower bounds on δ. The best we can hope for is $\operatorname{rank}\mathrm{NS}(X) = 1$. (Note: these bounds depend only on $\mathrm{NS}(X)/\mathrm{NS}(X)_{\mathrm{tors}}$, i.e., divisors modulo numerical equivalence.)

Terminology: $\operatorname{rank}\mathrm{NS}(X)$ = the *Picard number* of X.

Finding low Picard number

Philosophy: a “random” X of general type should have Picard number 1 unless you can “see” extra cycles from its construction. But how to explicitly find such an X?

Our approach: sample X from a simple family, and test for Picard number 1 by partially computing the zeta function of X. We’ll use smooth quintics in $\mathbb{P}^3$, but many other choices are possible.

Picard number and zeta functions

The zeta function of X is

$$Z(X,T) = \exp\left(\frac{T^n}{n}\#X(\mathbb{F}_{q^n})\right).$$

It factors as

$$\prod_{i=0}^{4} P_i(T)^{(-1)^{i+1}},$$

where $P_i(T) \in \mathbb{Z}[T]$, $P_i(0) = 1$, and $P_i(T)$ has all roots in $\mathbb{C}$ on the circle $|T| = q^{-i/2}$.

Picard number and zeta functions (contd.)

From properties of étale cohomology, we have

$$\operatorname{rank} \operatorname{NS}(X) \leq \operatorname{ord}_{T=1/q} P_2(T),$$

with equality conjectured by Tate. In particular,

$$\operatorname{ord}_{T=1/q} P_2(T) = 1 \implies \operatorname{rank} \operatorname{NS}(X) = 1.$$

Picard number and Frobenius matrices

Let $H^i(X)$ denote any Weil cohomology of X, i.e., vector spaces over a field K with $\mathrm{char}(K) = 0$, acted on by linear transformations F_i satisfying the Lefschetz trace formula:

$$P_i(T) = \det(1 - TF_i, H^i(X)) \qquad (i = 0, \dots, 4).$$

Then $\mathrm{ord}_{T=1/q} P_2(T)$ is the multiplicity of q as an eigenvalue of F_2, so we wish to check whether that multiplicity is 1.

A word from our sponsor: p-adic cohomology

The "usual" Weil cohomology is étale cohomology; its computational utility is limited (but cf. Schoof, Edixhoven).

A better choice for us is p-adic (crystalline, Monsky-Washnitzer, rigid) cohomology; this is already known to give good algorithms, e.g., for zeta functions of hyperelliptic curves.

For X lifting to a smooth proper $\tilde{X}$ over $\mathbb{Z}_q$, the p-adic cohomology "is" the algebraic de Rham cohomology of $\tilde{X} \times \mathbb{Q}_q$. (Here $\mathbb{Z}_q = W(\mathbb{F}_q)$ and $\mathbb{Q}_q = \operatorname{Frac} \mathbb{Z}_q$.)

de Rham cohomology: setup

Let X be a smooth surface of degree d in $\mathbb{P}^3_{\mathbb{F}_q}$, given by the equation $P(x_0, x_1, x_2, x_3) = 0$; put $U = \mathbb{P}^3_{\mathbb{F}_q} \setminus X$. Let H be any hyperplane section.

Fix a lift $\tilde{P}(x_0, x_1, x_2, x_3)$ to $\mathbb{Z}_q$, put $\tilde{X} = V(\tilde{P}) \subset \mathbb{P}^3_{\mathbb{Q}_q}$ and $\tilde{U} = \mathbb{P}^3_{\mathbb{Q}_q} \setminus \tilde{X}$.

de Rham cohomology: comparison

Put $H^2_{\mathrm{prim}}(X) = H^2(X)/\operatorname{Span}([H])$. Since $F[H] = q[H]$, we can deduce $\operatorname{rank}\mathrm{NS}(X) = 1$ if we prove that q is not an eigenvalue of F on $H^2_{\mathrm{prim}}(X)$.

We will attempt to do this via the comparison

$$H^3_{\mathrm{dR}}(\tilde{U}) \cong H^2_{\mathrm{prim}}(X)(-1),$$

where (-1) means Frobenius is multiplied by q. We'll compute a p-adic approximation to the matrix A by which Frobenius acts on some basis, and check that $A - q^2 I$ is nonsingular by Gaussian elimination.

The Griffiths-Dwork method

Put $H^3 = H^3_{\mathrm{dR}}(\tilde{U})$ and

$$\Omega = \sum_{i=0}^{3} (-1)^i x_i \, dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_3.$$

Then H^3 is spanned by $A\Omega/\tilde{P}^n$ for all A, n with $\deg(A) + 4 = nd$, modulo relations of the form

$$\frac{\partial A}{\partial x_i} \frac{\Omega}{\tilde{P}^n} - n \frac{\partial \tilde{P}}{\partial x_i} \frac{A\Omega}{\tilde{P}^{n+1}}.$$

Griffiths-Dwork (contd.)

The relations make it routine to:

- find a basis of H^3;
- represent any 3-form in terms of the basis elements.

These make heavy use of Gröbner basis techniques over quotients of $\mathbb{Z}_q$; these are built into MAGMA.

The Frobenius action on cohomology

The Frobenius action on H^3 is induced by a ring map σ sending x_i to x_i^q for $i = 0, 1, 2, 3$, where

$$\sigma(\tilde{P}^{-1}) = \tilde{P}^{-q}(1 - (\tilde{P}^q - \sigma(\tilde{P}))\tilde{P}^{-q})^{-1}$$

is a p-adically convergent power series (in an appropriate “weakly complete ring”).

Upshot: we can’t compute this exactly; instead, we truncate and compute a p-adic approximation.

Frobenius action (contd.)

It is helpful to describe (via crystalline cohomology) a basis of H^3 so that the matrix of F has entries in $\mathbb{Z}_q$. Moreover, the elementary divisors of this matrix are related to the Hodge numbers of X via the Mazur-Ogus theorem.

We must also control the denominators introduced by the reduction process; these look *a priori* like $1/n!$ but are actually more like $p^{-\lfloor \log_p n \rfloor}$. (The proof uses excision in de Rham cohomology.)

Approximate Gaussian elimination

Recall: we wish to verify that a certain square matrix $(F - q^2 I)$ over $\mathbb{Z}_q$ is nonsingular, where each entry only carries a few accurate p-adic digits.

- In the first column, of those entries with positive relative precision, find the one of lowest valuation; break ties in favor of more relative precision. If no such entries exist, FAIL.
- If the matrix is 1×1, SUCCEED. Else, switch the chosen row with the top row, then use it to clear the rest of the first column. Repeat on the submatrix excluding the first row and column.

Implementation details

For $q = p$, we (with Abbott and Roe) have implemented the approximate p-adic calculation of Frobenius in MAGMA on `dwork`, a Sun dual Opteron 246 (2 GHz, 2 GB RAM, 32-bit mode).

Code for this implementation will be made available upon request; it will eventually appear on my web site. (Beware that MAGMA 2.12-10 or later is required.)

An example

Example. *The zero locus in* $\mathbb{P}^3_{\mathbb{F}_2}$ *of the quintic*

$$x_0^5 + x_0^2 x_1^2 x_3 + x_0 x_1 x_2^2 x_3 + x_0 x_1 x_3^3 + x_0 x_2 x_3^3 + x_0 x_3^4 + x_1^5 + x_1^3 x_2 x_3 + x_1^2 x_3^3 + x_2^5 + x_2^3 x_3^2 + x_3^5$$

is a smooth surface of general type with Picard number 1.

This uses the Frobenius matrix mod 2^4, which we compute in 2 CPU-hours. (Mod 2^5 requires 3.5 CPU-hours; mod 2^6 requires 7 CPU-hours.)

An alternate algorithm of Lauder (“deformation”) should be faster but seems hard to implement.

Complements

With more work, one can sometimes show that a given X over $\mathbb{F}_q$ has small *geometric* Picard number. This can be used to exhibit K3 surfaces over $\mathbb{Q}$ of geometric Picard number 1; cf. the dissertation of R. van Luijk. (Beware: over a finite field, if $\dim H^2(X)$ is even, the geometric Picard number is at least 2.)

It should also be easy to compute p-adic cohomology of, and hence find examples of Picard number 1 among, smooth hypersurfaces in toric varieties (e.g., $\mathbb{P}^1 \times \mathbb{P}^2$, weighted projective spaces).

The end