HECKE OPERATORS FOR ARITHMETIC GROUPS VIA CELL COMPLEXES

MARK MCCONNELL

The subject of this talk is the cohomology of locally symmetric spaces for SL_n, and the conjectural connection between this cohomology and Galois representations. To remind you what sort of conjectures these are, I'll start by describing the story for SL_2, where the results are known. Of course I can tell only a small part of that story. Some names associated to this section are Hecke, Weil, Eichler and Shimura.

Background for SL_2

Let $\mathfrak{h}$ be the upper half-plane in $\mathbf{C}$. Let

$$\Gamma = \Gamma_0(N) = \left\{ A \in \mathrm{SL}_2(\mathbf{Z}) |\, A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mathrm{mod} N \right\}.$$

Let $f \neq 0$ be a cusp form of weight 2 for Γ. This implies $f(z)\,dz$ descends to a holomorphic differential form on $\Gamma\backslash\mathfrak{h}$, giving a cohomology class $\omega \in H^1(\Gamma\backslash\mathfrak{h};\mathbf{C})$.

For $n \in \mathbf{Z}$, we have *Hecke correspondences* $T(n)$ on $\Gamma\backslash\mathfrak{h}$; we'll recall their definition below. Now assume that f is an eigenform for all the $T(n)$. (What's important for later in the talk is that the cohomology class ω be an eigenclass.) In a coordinate chart $q = e^{2\pi i z}$ around infinity, $f = \sum_{n=1}^{\infty} a_n q^n$ with $a_1 \neq 0$, and we multiply through by a scalar so that $a_1 = 1$. It turns out that the a_n are the eigenvalues for $T(n)$ for all n. For simplicity, assume all the a_n lie in $\mathbf{Q}$.

At this point, several ideas which seem to have no *a priori* connection come together in a surprising way.

First, define the *L-function*

$$L(s,f) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

This converges for s in an appropriate right half-plane. It has an analytic continuation to $s \in \mathbf{C}$, a functional equation, and—importantly

Date: June 5, 2008.

for our purposes—an *Euler product*

$$L(s,f) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p \mid N} (1 - a_p p^{-s})^{-1}.$$

Second, in the Jacobian of the modular curve $\overline{\Gamma \backslash \mathfrak{h}}$, there is an elliptic curve E, cut out by the Hecke operators in an appropriate sense, and defined over $\mathbf{Q}$. If $p \nmid N$, the zeta function

$$\exp\left(\sum_{n=1}^{\infty} \left(\#E(\mathbf{F}_{p^n}) \frac{T^n}{n} \right) \right)$$

has the form

$$\frac{1 - a_p T + pT^2}{(1-T)(1-pT)}.$$

The numerator is the same polynomial as in the Euler factor of the L-function, with $T = p^{-s}$. We call this the *Hecke polynomial*.

Third, for a prime $l \nmid N$, the *Tate module* is

$$\lim_{\substack{\leftarrow \\ r}} \{x \in E(\overline{\mathbf{Q}}) \mid l^r x = 0\}.$$

The Tate module is isomorphic to $\mathbf{Z}_l \times \mathbf{Z}_l$ (in each direction, it's an inverse limit of $\mathbf{Z}/l^r\mathbf{Z}$). Consider $G_{\mathbf{Q}}$, the Galois group of $\overline{\mathbf{Q}}/\mathbf{Q}$. The Galois group acts on $E(\overline{\mathbf{Q}})$, hence on the Tate module, so there is a *Galois representation*

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l).$$

Let Frob_p be the *geometric Frobenius element* in $G_{\mathbf{Q}}$. It is defined up to conjugacy and is characterized by saying: if $F/\mathbf{Q}$ is a finite Galois extension, unramified at p, then ${\mathrm{Frob}_p}^{-1}$ acts on the corresponding extension of $\mathbf{F}_p$ by $x \mapsto x^p$.

The main result is

Theorem. *If $p \nmid lN$, the characteristic polynomial of $\rho({\mathrm{Frob}_p}^{-1})$ is exactly the Hecke polynomial $1 - a_p T + pT^2$.*

In particular, the characteristic polynomial is *independent of l*. The elliptic curve E gives rise to a motive over $\mathbf{Q}$. The Galois representations are the *l-adic realizations of the motive.* The motive is the "l-adic cohomology without the l".

Conjectures for SL_n

For $n > 2$ there is no obvious analogue of the elliptic curve E, and no obvious candidate for a motive. The topological space that's the analogue of $\Gamma\backslash\mathfrak{h}$ is no longer an algebraic variety; in fact, its real dimension is just as likely to be odd as to be even. Nevertheless, we can state conjectures, part of the world of the Langlands program, that generalize the story we've told so far.

Let $X = \mathrm{SL}_n(\mathbf{R})/\mathrm{SO}_n(\mathbf{R})$, the *symmetric space* for SL_n. When $n = 2$, $X = \mathfrak{h}$.

Let $\Gamma \subseteq \mathrm{SL}_n(\mathbf{Z})$ be a congruence subgroup of level N. Usually it will be $\Gamma_0(N)$, the subgroup of $\mathrm{SL}_n(\mathbf{Z})$ consisting of matrices congruent to

$$\begin{pmatrix} * & \dots & * & * \\ \vdots & \ddots & \vdots & \vdots \\ & \dots & * & * \\ 0 & \dots & 0 & * \end{pmatrix}$$

mod N.

For $n = 2$, we took a cusp form f of weight 2 and turned it into a cuspidal cohomology class ω on $\Gamma\backslash\mathfrak{h}$. For general n, the analogue is to connect cuspidal automorphic representations Π of GL_n with cuspidal cohomology classes. We'll consider cohomology $H^i(\Gamma\backslash X; V)$ with coefficients in a module V that we'll describe as we go along. In this talk V will at least be defined over $\mathbf{R}$ or $\mathbf{C}$, so we can use the language of de Rham cohomology. A *cuspidal differential form* is a differential form with coefficients in V satisfying certain vanishing conditions as you out to infinity (toward the "cusps") in $\Gamma\backslash X$; it is rapidly decreasing, and appropriate integrals vanish over the parabolic subgroup associated to each cusp. A *cuspidal cohomlogy class* ω is one supported on a cuspidal differential form on $\Gamma\backslash X$.

The cuspidal cohomology is one basic building block of the cohomology of $\Gamma\backslash X$. Much of the rest of the cohomology is not cuspidal, but comes from cuspidal cohomology of other groups. Often Eisenstein classes connect the cohomology on the big space with the cuspidal part from lower-rank groups. This is not the whole story (for instance, ghost classes are not completely understood).

For the sake of time, I won't define automorphic representations. However, standard conjectures would attach a motive to each cuspidal automorphic representation Π of GL_n over a number field, as long as the infinity type of the representation is algebraic. For simplicity, take the number field to be $\mathbf{Q}$. One knows that if Π arises from a cuspidal cohomology class where V is a rational representation, then it satisfies this algebraicity condition.

There is an algebra $\mathcal{H}(N)$ of *Hecke correspondences* given by double cosets $\Gamma A\Gamma$, where $A \in M_n(\mathbf{Z})$, with $\det A$ relatively prime to N and satisfying the same congruence conditions as Γ. The Hecke algebra is commutative, and is generated as a polynomial ring by

$$T(p,k) = \Gamma \cdot \operatorname{diag}(1,\dots,1,\underbrace{p,\dots,p}_{k}) \cdot \Gamma$$

for primes $p \nmid N$ and all $k = 1,\dots,n$. (When $p \mid N$, the generators must be modified slightly. Also note that $T(p,0)$ is the identity double coset.) The Hecke algebra acts on $H^i(\Gamma\backslash X; V)$ whenever Γ and the A's all act on V.

Let ω be a cohomology class that is a Hecke eigenclass. Let $a(p,k)$ be the eigenvalue for $T(p,k)$. Define the *Hecke polynomial* $P(\omega,p)$ to be

$$\sum_{k=0}^{n} (-1)^k p^{k(k-1)/2} a(p,k) T^k.$$

We now come to the main point of the talk.

Conjecture. *Let ω be a cohomology class that is a Hecke eigenclass, and use the other notation above. Then there is a number field F with ring of integers B, such that for any prime l and prime λ of B lying over l, there is a continuous semi-simple Galois representation*

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_n(B_\lambda),$$

unramified outside lN, and such that, for any prime $p \nmid lN$, the characteristic polynomial of $\rho(\mathrm{Frob}_p{}^{-1})$ is the Hecke polynomial $P(\omega,p)$.

We say that ρ, if it exists, is *attached to ω*.

Computational tests of the conjecture.

For the rest of the talk, I'll describe joint work I've been doing with Avner Ash and Paul Gunnells. Over the years, Ash and his collaborators have proved special cases of conjectures like this one and/or have tested them computationally. He and his collaborators (including me) have worked on the torsion case, where V is defined over a finite field of characteristic l. This has the flavor of Serre's conjecture, and the Serre-Deligne theorem for modular forms, where the modular forms and Galois representations are mod l.

Today, however, I'll talk about a recent project with Ash and Gunnells in characteristic 0, the first computational work of this type for GL_4. Here $\Gamma = \Gamma_0(N)$ and $V = \mathbf{C}$, constant complex coefficients.

Our approach is to compute $H^i(\Gamma\backslash X; \mathbf{C})$ by machine, and to compute the $T(p,k)$ on H^i for as many p as we can until the computations become too cumbersome. For GL_4, the cuspidal cohomology lies only in H^4 and H^5, and each of these is dual to the other, so we focus our computations on H^5.

Say that ρ *seems to be attached to* ω if the condition with the Hecke polynomial is satisfied at all the p you have computed before your machine ran out of memory. This is not as great a limitation as it may sound. Often the $T(2,k)$ are enough to suggest persuasively what the Galois representation is.

We decompose H^i into Hecke eigenspaces for these operators. On each eigenspace, we compute the Hecke polynomials and factor them. That tells us how ${\mathrm{Frob}_p}^{-1}$ acts on the eigenspace. In a typical example, if a Hecke polynomial (degree 4) factors as (linear)(linear)(quadratic), it strongly suggests that this is not a cuspidal eigenspace. Rather, it comes from an SL_2 symmetric space lying out along one of the cusps. The quadratic terms will be the Hecke polynomial for some newform of weight 2 or 4. The two linear terms are twists by a power of the cyclotomic character. In a similar way, the cusp forms for SL_3 computed by Ash, Grayson and Green in 1984 appear.

We have carried out these GL_4 computations for $\Gamma_0(N)$, mostly for prime N, and for all prime $N \leq 191$. We have found cusp forms for level 61, 73, and 79. To the best of our knowledge, these are the first concretely constructed cusp forms for GL_4. However, they are not "native" to GL_4. Ash calls a cusp form *autochthonous* if it is not a functiorial lift from a lower rank group. The cusp forms we found turned out to be functorial liftings from holomorphic Siegel modular forms of weight 3 on $\mathrm{GSp}_4(\mathbf{Q})$. We've found there are no autochthonous cusp forms for GL_4 up to prime level 191. But we're still looking!

Performing the computations

... the well-rounded retract. There is a Γ-equivariant deformation retraction of X onto a lower-dimensional subspace W. $\Gamma\backslash W$ is compact. Best of all, the retraction is defined in a natural, geometric way, and it makes W is a locally finite cell complex. Thus $\Gamma\backslash W$ is a finite cell complex. All the cohomology computations can be done explicitly using the cell structure.

... $\mathbf{C}$ is really $\mathbf{F}_{12379}$

... my programs. v mod 12379. Store i, v packed in one 64-bit int. Our matrices are very sparse. The largest matrix so far is 700,000 $\times$ 2.4 million. This was on Linux with 4G of RAM. Initially there are around 100 entries per column. Unlike the RSA challenge matrices, the sparsity is uniform throughout. A sparse vector is a linked list of columns. Lisp, vs Python and C. Let ∂^i be one of the matrices in a cochain complex computing the cohomology. Row- and column-reduce ∂^i simultaneously, obtaining $\partial^i = PDQ$ where P and Q are invertible over $\mathbf{Z}$ and D is diagonal (Smith normal form). Dump P and Q to disk as you go as a list of elementary matrices, since they would be dense if you tried to hold them directly. Markowitz pivoting. When memory fills up, Gaussian earthworm: dump the matrix to disk, read it in one column at a time, and only column-reduce (stop keeping track of Q). In a chain complex, have to use Q of the left-hand matrix to change bases in its right-hand neighbor before reducing the right-hand one.

... my programs work also over $\mathbf{Z}$. Current size record is 8400×33000, but that was three years ago, on a 1G machine, and under Windows (a serious hindrance to memory-heavy computation!) In practice, fill-in stopped me before integer explosion. In the size record just mentioned, the size of the intermediate entries was never more than four digits. Disk-based divide-and-conquer Hermite normal form was helpful but didn't solve the problem. I will be geting back to this. Dumas-Saunders-Villard techniques; need to figure out how to do that while preserving the change-of-basis matrices.

... how to compute Hecke. Well known for $n = 2$: modular symbols. For $n = 3$, Ash and Lee Rudolph have an algorithm generalizing modular symbols; $\dim X = 5$, and the dim of the modular symbol is 3. When $n \geq 4$, it's harder because cuspidal cohomology no longer lives in the top degree of the cohomology. Gunnells has the algorithm that works here.