Hecke Operators and q-Expansions

William Stein

Department of Mathematics
University of Washington

August 3, 2006 / MSRI Workshop

Outline

Hecke Operators on Modular Symbols

Hecke Operators on Modular Symbols

Let $\Gamma = \Gamma_1(N)$ or $\Gamma_0(N)$.
For any positive integer n, let

$$X_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}) \ : \ a \geq 1, \ ad = n, \text{ and } 0 \leq b < d \right\}.$$

Note that the set X_n is in bijection with the set of subgroups of $\mathbb{Z}^2$ of index n, where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ corresponds to $L = \mathbb{Z} \cdot (a, b) + \mathbb{Z} \cdot (0, d)$, as one can see using Hermite normal form.

Definition (Hecke Operators on Modular Forms)

If f is a modular form of weight k, then

$$T_n(f) = \sum_{g \in X_n} f^{[\gamma]_k}.$$

Definition (Hecke Operators on Modular Symbols)

For a modular symbol $P\{\alpha, \beta\}$ we define

$$T_n(x) = \sum_{g \in X_n} g(P\{\alpha, \beta\}).$$

Compatibility

Definition (Hecke Operators on Modular Forms)

If f is a modular form of weight k, then

$$T_n(f) = \sum_{g \in X_n} f^{[\gamma]_k}.$$

Definition (Hecke Operators on Modular Symbols)

For a modular symbol $P\{\alpha, \beta\}$ we define

$$T_n(x) = \sum_{g \in X_n} g(P\{\alpha, \beta\}).$$

Theorem

We have

$$\langle T_n(f), x \rangle = \langle f, T_n(x) \rangle.$$

This is the integration pairing $\langle (f), P\{\alpha, \beta\} \rangle = \int_\alpha^\beta f(z) P(z, 1)\, dz$

Example: Hecke Operators on Modular Symbols

When $k = 2$ and p is a prime not dividing N, we have

$$T_p(\{\alpha, \beta\}) = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \{\alpha, \beta\} + \sum_{r \bmod p} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} \{\alpha, \beta\}.$$

Example

For example, when $N = 11$ we have

$$\begin{aligned} T_2\{0, 1/5\} &= \{0, 2/5\} + \{0, 1/10\} + \{1/2, 3/5\} \\ &= -2\{0, 1/5\}. \end{aligned}$$

Remark

Computing Hecke operators this way on modular symbols, as I described them last time, is **very slow** since you have to convert everything back and forth to Manin symbols.

Example: Hecke Operator on Modular Symbols

```
sage: set_modsym_print_mode('modular')
sage: M = ModularSymbols(5,4); M.basis()
(X^2*{0,Infinity}, 4*X^2*{-1/2,0} + 4*X*Y*{-1/2,0} + Y^2*{-1/2,0},
  9*X^2*{-1/3,0} + 6*X*Y*{-1/3,0} + Y^2*{-1/3,0}, 16*X^2*{-1/4,0}
     + 8*X*Y*{-1/4,0} + Y^2*{-1/4,0})
sage: t = M.T(2); t
Hecke operator T_2 on Modular Symbols space of dimension 4 for
Gamma_0(5) of weight 4 with sign 0 over Rational Field

sage: print M.0, '|--->', t(M.0)
X^2*{0,Infinity} |---> 9*X^2*{0,Infinity} + X^2*{-1/2,0}+X*Y*{-1/2,0}
  + 1/4*Y^2*{-1/2,0} + 27/4*X^2*{-1/3,0} + 9/2*X*Y*{-1/3,0}
  + 3/4*Y^2*{-1/3,0} - 16*X^2*{-1/4,0} - 8*X*Y*{-1/4,0}-Y^2*{-1/4,0}
sage: print M.1, '|--->', t(M.1)
4*X^2*{-1/2,0} + 4*X*Y*{-1/2,0} + Y^2*{-1/2,0} |---> 2*X^2*{-1/2,0}
  + 2*X*Y*{-1/2,0} + 1/2*Y^2*{-1/2,0} + 9/2*X^2*{-1/3,0}
  + 3*X*Y*{-1/3,0} + 1/2*Y^2*{-1/3,0} + 128*X^2*{-1/4,0}
  + 64*X*Y*{-1/4,0} + 8*Y^2*{-1/4,0}
sage: print M.2, '|--->', t(M.2)
9*X^2*{-1/3,0} + 6*X*Y*{-1/3,0} + Y^2*{-1/3,0} |---> 18*X^2*{-1/2,0}
  + 18*X*Y*{-1/2,0} + 9/2*Y^2*{-1/2,0} - 63/2*X^2*{-1/3,0}
  - 21*X*Y*{-1/3,0} - 7/2*Y^2*{-1/3,0} + 128*X^2*{-1/4,0}
  + 64*X*Y*{-1/4,0} + 8*Y^2*{-1/4,0}
```

Hecke Operators on Manin Symbols

Hecke Operators on Manin Symbols

If S is a subset of $\mathrm{GL}_2(\mathbb{Q})$, let

$$\tilde{S} = \{\tilde{g} : g \in S\},$$

where

$$\tilde{g} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \det(g) \cdot g^{-1}.$$

Also, for any ring R and any subset $S \subset \mathrm{Mat}_2(\mathbb{Z})$, let $R[S]$ denote the free R-module with basis the elements of S, so the elements of $R[S]$ are the finite R-linear combinations of the elements of S.

Definition (Merel's Condition C_n)

An element

$$h = \sum u_M [M] \in \mathbb{C}[\mathrm{Mat}_2(\mathbb{Z})_n]$$

satisfies condition C_n if for every $K \in \mathrm{Mat}_2(\mathbb{Z})_n / \mathrm{SL}_2(\mathbb{Z})$, we have that

$$\sum_{M \in K} u_M([M\infty] - [M0]) = [\infty] - [0] \in \mathbb{C}[P^1(\mathbb{Q})]. \quad (2.1)$$

Definition (Merel's Condition C_n)

An element

$$h = \sum u_M[M] \in \mathbb{C}[\mathrm{Mat}_2(\mathbb{Z})_n]$$

satisfies condition C_n if for every $K \in \mathrm{Mat}_2(\mathbb{Z})_n / \mathrm{SL}_2(\mathbb{Z})$, we have that

$$\sum_{M \in K} u_M([M\infty] - [M0]) = [\infty] - [0] \in \mathbb{C}[P^1(\mathbb{Q})]. \qquad (2.2)$$

Suppose h satisfies condition C_n.

Theorem (Merel)

For any Manin symbol $[P, g] \in M_k(\Gamma)$*,*

$$T_n([P, (u, v)]) = \sum_M u_M[P(aX + bY,\ cX + dY), (u, v)M]. \qquad (2.3)$$

Here (u, v) corresponds to a coset of Γ in $\mathrm{SL}_2(\mathbb{Z})$, and if $(u', v') = (u, v)M \in (\mathbb{Z}/N\mathbb{Z})^2$, and $\gcd(u', v', N) \neq 1$, then we omit the corresponding summand.

Heilbronn Matrices

Proposition (Merel)

The element

$$F_n = \sum_{\substack{a>b\geq 0\\ d>c\geq 0\\ ad-bc=n}} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in \mathbb{Z}[\mathrm{Mat}_2(\mathbb{Z})_n]$$

satisfies condition C_n.

Merel's proof is not too difficult (two pages). He also gives **several other examples** of elements that satisfy condition C_n. They each have $\sim n\log(n)$ terms, which has implications for complexity of computing Hecke operators.

Remark

There is a map $\pi : \mathbb{Z}[\mathrm{Mat}_2(\mathbb{Z})_p] \to \mathbb{Z}[\mathrm{Mat}_2(\mathbb{Z}/N\mathbb{Z})_p]$. For fixed N, if you could compute $\pi(F_p)$ in time polynomial in $\log(p)$, then (I think) you would be able to compute Hecke eigenvalues in extreme generality in polynomial time.

Example: Matrices that Satisfy C_n

```
sage: list(HeilbronnMerel(2))
[[1, 0, 0, 2], [1, 0, 1, 2], [2, 0, 0, 1], [2, 1, 0, 1]]

sage: list(HeilbronnMerel(3))
[[1, 0, 0, 3], [1, 0, 1, 3], [1, 0, 2, 3], [2, 1, 1, 2],
 [3, 0, 0, 1], [3, 1, 0, 1], [3, 2, 0, 1]]

sage: list(HeilbronnMerel(6))

[[1, 0, 0, 6], [1, 0, 1, 6], [1, 0, 2, 6], [1, 0, 3, 6],
 [1, 0, 4, 6], [1, 0, 5, 6], [2, 0, 0, 3], [2, 1, 0, 3],
 [2, 0, 1, 3], [2, 0, 2, 3], [2, 1, 2, 4], [2, 1, 4, 5],
 [3, 0, 0, 2], [3, 1, 0, 2], [3, 2, 0, 2], [3, 0, 1, 2],
 [3, 2, 3, 4], [4, 2, 1, 2], [4, 3, 2, 3], [5, 4, 1, 2],
 [6, 0, 0, 1], [6, 1, 0, 1], [6, 2, 0, 1], [6, 3, 0, 1],
 [6, 4, 0, 1], [6, 5, 0, 1]]
```

Using Hecke Operators to Compute Modular Forms

Linear Functionals

Let $\mathbb{T} \subset \mathrm{End}(S_k(\Gamma))$ be the Hecke algebra.
Gabor explained that there is an isomorphism of vector spaces

$$\Psi : S_k(\Gamma) \xrightarrow{\cong} \mathrm{Hom}(\mathbb{T}, \mathbb{C}) \tag{3.1}$$

that sends $f \in S_k(\Gamma)$ to the homomorphism

$$t \mapsto a_1(t(f)).$$

Definition

For any $\mathbb{C}$-linear map $\varphi : \mathbb{T}_{\mathbb{C}} \to \mathbb{C}$, let

$$f_\varphi = \sum_{n=1}^{\infty} \varphi(T_n) q^n \in \mathbb{C}[[q]].$$

Lemma

The series f_φ is the q-expansion of $\Psi^{-1}(\varphi) \in S_k(\Gamma)$.

Definition

For any $\mathbb{C}$-linear map $\varphi : \mathbb{T}_{\mathbb{C}} \to \mathbb{C}$, let

$$f_\varphi = \sum_{n=1}^{\infty} \varphi(T_n) q^n \in \mathbb{C}[[q]].$$

Lemma

The series f_φ is the q-expansion of $\Psi^{-1}(\varphi) \in S_k(\Gamma)$.

Conclusion: The cusp forms f_φ, as φ varies through a basis of $\mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C})$, form a basis for $S_k(\Gamma)$. In particular:

> We can compute $S_k(\Gamma)$ by computing a basis for $\mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C})$, where we compute $\mathbb{T}$ in any way we want, e.g., using a space that contains an isomorphic copy of $S_k(\Gamma)$.

Example: $S_2(\Gamma_0(11))$

The smallest N with $S_2(\Gamma_0(N)) \neq 0$ is $N = 11$.

```
sage: M = ModularSymbols(11); M.basis()
((1,0), (1,8), (1,9))
sage: S = M.cuspidal_submodule(); S
Dimension 2 subspace of a modular symbols space of level 11
```

We compute a few Hecke operators, then read off a nonzero cusp form, which forms a basis for $S_2(\Gamma_0(11))$:

```
sage: S.T(2).matrix()
[-2  0]
[ 0 -2]
sage: S.T(3).matrix()
[-1  0]
[ 0 -1]
```

Thus

$$f_{0,0} = q - 2q^2 - q^3 + \cdots \in S_2(\Gamma_0(11))$$

forms a basis for $S_2(\Gamma_0(11))$.

Example: $S_2(\Gamma_0(33))$

We compute a basis for $S_2(\Gamma_0(33))$ to precision $O(q^6)$.

```
sage: M = ModularSymbols(33)
sage: S = M.cuspidal_submodule(); S
Dimension 6 subspace of a modular symbols space of level 33
```

Thus $\dim S_2(\Gamma_0(33)) = 3$.

```
sage: R.<q> = PowerSeriesRing(QQ)
sage: a = [S.T(n).matrix()[0,0] for n in range(6)]
sage: f00 = sum(v[n]*q^n for n in range(6)) + O(q^6)
sage: f00
q - q^2 - q^3 + q^4 + O(q^6)
```

This gives us one basis element of $S_2(\Gamma_0(33))$. It remains to find two others. We find

```
sage: a = [S.T(n).matrix()[0,1] for n in range(6)]
sage: f01 = sum(v[n]*q^n for n in range(1,6)) + O(q^6)
sage: f01
-2*q^3 + O(q^6)
```

and

```
sage: a = [S.T(n).matrix()[1,0] for n in range(6)]
```

Computing Eigenforms

1. Use the Atkin-Lehner theory of newforms to write $S_k(N)$ in terms of new subspaces of $S_k(M)$ with $M \mid N$:
$$S_k(N) = \bigoplus_{M|N} \bigoplus_{d|N/M} \alpha_d(S_k(M)_{\text{new}}).$$
2. Compute the new subspace of $V = S_k(M)$ using degeneracy maps, which have an explicit description.
3. Decompose V as a direct sum of simple $\mathbb{T}$-modules (using linear algebra – charpolys, kernels, etc.)
4. Suppose $W \subset V$ is a simple module and fix $x \in W$ nonzero.
5. Define a surjective map $\phi : \mathbb{T}_{\mathbb{Q}} \to W$ given by $t \mapsto tx$.
6. This endows W with an algebra structure (in which x corresponds to 1). In particular, you can choose and fix an isomorphism $W \to K = \mathbb{Q}(a_2, a_3, \ldots)$, given in terms of a power basis.
7. Store either the $T_p(x)$ or $T_n(x)$, depending on the intended application, along with the isomorphism $W \to K$.
8. (One can recover a_n for n composite from the a_p for p prime via arithmetic.)