Overconvergent Modular Symbols in Sage

David Roe
(with Rob Pollack, Rob Harron, Ander Steele and others)

Department of Mathematics
University of Pittsburgh

Towards new development of mathematics via computational algebra systems
RIMS, Kyoto

Outline

Classical Modular Forms

$\mathcal{H}$ – upper half plane: complex numbers $z = x + iy$ with $y > 0$.

$\Gamma_0(N)$ $\subseteq \mathrm{SL}_2(\mathbb{Z})$ consists of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $N \mid c$.
Acts on $\mathcal{H}$ by $\gamma \cdot z = \frac{az+b}{cz+d}$. Example of a *level* Γ.

k – an integer, the *weight*.

$M_k(\Gamma)$ – holomorphic functions $f : \mathcal{H} \to \mathbb{C}$ with
$f(\gamma \cdot z) = (cz + d)^k f(z)$ for $\gamma \in \Gamma$. These are *modular forms*.

Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$, $f(z + 1) = f(z)$. Get a Fourier expansion around $i\infty$: if $q = e^{2\pi i z}$,

$$f(z) = \sum_{n=0}^{\infty} a_n q^n.$$

Note: $a_n = 0$ for $n < 0$ is an additional condition on f.

Examples: Eisenstein Series

For $k > 2$ even, $G_k(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^k} \in M_k(\mathrm{SL}_2(\mathbb{Z}))$.

$$G_k(z) = 2\zeta(k)\left(1 + \frac{2}{\zeta(1-k)}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right),$$

where $\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}$.

- For other Γ, a *cusp* is a Γ-orbit on $\mathbb{Q} \cup \{\infty\}$.
- Basis for Eisenstein series of forms that take value 1 on one cusp and zero on others.
- Cusp forms $S_k(\Gamma) \subset M_k(\Gamma)$ are those vanishing on all cusps.

Examples: Modular Forms from Elliptic Curves

If E is an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Q}$ with *discriminant* $-16(4a^3 + 27b^2)$ and *conductor* N (same prime factors),

$$
\begin{aligned}
a_p &= (p+1) - \#E(\mathbb{F}_p) \text{ if } p \nmid N \\
a_p &= 0 \text{ if } E \text{ has additive reduction} \\
a_p &= 1 \text{ if } E \text{ has split multiplicative reduction} \\
a_p &= -1 \text{ if } E \text{ has non-split multiplicative reduction} \\
a_{p^r} &= a_{p^{r-1}} \cdot a_p - p \cdot a_{p^{r-2}} \text{ if } p \nmid N \\
a_{p^r} &= a_p^r \text{ if } p \mid N \\
a_{mn} &= a_m \cdot a_n \text{ if } (m,n) = 1.
\end{aligned}
$$

$$f_E = \sum_{n=1}^{\infty} a_n q^n \in M_2(\Gamma_0(N)).$$

Hecke Operators

- For fixed k and Γ, the space $M_k(\Gamma)$ is finite dimensional (with explicit dimensions via Riemann-Roch).
- For each $n \geq 1$ there is a linear operator T_n on $M_k(\Gamma)$, and the T_n commute with each other.
- An *eigenform* is a simultaneous eigenvector for these operators (e.g. f_E).

LMFDB

L-functions and Modular Forms Database

Break for demo of `http://beta.lmfdb.org`.

Modular Symbols

For $k > 1$, computation made possible by *modular symbols*.

Δ_0 – $\mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))$: formal sums $\sum_{\alpha \in \mathbb{Q} \cup \{\infty\}} a_\alpha \alpha$ with $\sum_\alpha a_\alpha = 0$.

$S_0(p)$ – $\left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mid (a, p) = 1, p \mid c \text{ and } ad - bc \neq 0 \right\}$.

V – a $\mathbb{Z}$-module (e.g. $\mathbb{C}$ or $\mathrm{Sym}^{k-2}(\mathbb{C})$) with right actions of Γ and $S_0(p)$.

Γ – acts on $\mathrm{Hom}(\Delta_0, V)$ by $(\varphi|\gamma)(D) = \varphi(\gamma D)|\gamma$.

$\mathrm{Smb}_\Gamma(V)$ – $\{\varphi \in \mathrm{Hom}(\Delta_0, V) \mid \varphi = \varphi|\gamma\}$.

T_ℓ – acts by $\varphi|T_\ell = \varphi|\left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix} \right) + \sum_{a=0}^{\ell-1} \varphi|\left(\begin{smallmatrix} 1 & a \\ 0 & \ell \end{smallmatrix} \right)$ for $\ell \nmid N$.

U_q – acts by $\varphi|U_q = \sum_{a=0}^{q-1} \varphi|\left(\begin{smallmatrix} 1 & a \\ 0 & q \end{smallmatrix} \right)$ for $q \mid N$.

Manin Relations

G – $\mathrm{PSL}_2(\mathbb{Z})$

$[\gamma]$ – $\frac{b}{d} - \frac{a}{c} \in \Delta_0$ when $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.

σ – $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, a two-torsion element.

τ – $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, a three-torsion element.

I – the left ideal $\mathbb{Z}[G](1+\sigma) + \mathbb{Z}[G](1+\tau+\tau^2)$.

$\{g_i\}$ – right coset reps for $\Gamma \backslash G$, generate $\mathbb{Z}[G]$ as a free $\mathbb{Z}[\Gamma]$-module.

Using continued fractions, every element of Δ_0 is the sum of elements $[\gamma]$, so get surjective map

$$\mathbb{Z}[G] \to \Delta_0.$$

Manin showed that the kernel is I. Therefore Δ_0 is generated by the g_i, with relations given by I. For instance,

$$g_i(1+\sigma) = g_i + g_i\sigma = g_i + \gamma_{ij} g_j.$$

Modular Symbols to Modular Forms

Theorem (Eichler-Shimura)

$\mathrm{Smb}_\Gamma(\mathrm{Sym}^{k-2}(\mathbb{C})) \cong M_k(\Gamma) \oplus S_k(\Gamma)$ *as Hecke-modules.*

So to compute $M_k(\Gamma)$, we

1. Using Manin relations, write down a basis for $\mathrm{Smb}_\Gamma(\mathrm{Sym}^{k-2}(\mathbb{C}))$.
2. Compute matrices for action of U_q and T_ℓ for small ℓ.
3. Diagonalize to get *systems of Hecke eigenvalues* $\{a_\ell\}$.
4. These systems provide the Fourier coefficients for a basis of eigenforms in $M_k(\Gamma)$.

p-adic Numbers

Fix p prime. Recall:

- v_p – For a, b prime to p, set $v_p\left(p^v \cdot \frac{a}{b}\right) = v$ and $\left|p^v \cdot \frac{a}{b}\right|_p = p^{-v}$.
- $\mathbb{Q}_p$ – Completion of $\mathbb{Q}$ with norm $|\cdot|_p$. Then $\mathbb{Z}_p = \{z \in \mathbb{Q}_p : |z| \leq 1\}$.
- $\mathbb{Z}_p$ – Alternately, $\mathbb{Z}_p = \lim_{\leftarrow m} \mathbb{Z}/p^m\mathbb{Z}$ and $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$.
  - Concretely, of the form $\sum_{m=v}^{\infty} a_m p^m$ with $a_m \in \{0, \ldots, p-1\}$.
  - Computationally, represent as $p^v \cdot u$, where $u \in (\mathbb{Z}/p^m\mathbb{Z})^\times$.

p-adic Distributions

$\mathbf{A}$ – $\left\{f(z) = \sum_{n=0}^{\infty} a_n z^n \in \mathbb{Q}_p[\![z]\!] \;:\; |a_n| \to 0\right\}$; $||f|| = \sup_{z \in \mathbb{Z}_p} |f(z)|$.

$\mathbf{D}$ – $\mathrm{Hom}(\mathbf{A}, \mathbb{Q}_p)$; $||\mu|| = \sup_{0 \neq f \in \mathbf{A}} \frac{|\mu(f)|}{||f||}$.

$\mathbf{A}_k$ – $\mathbf{A}$ with $(\gamma \cdot_k f)(z) = (a + cz)^k \cdot f\left(\frac{b+dz}{a+cz}\right)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S_0(p)$.

$\mathbf{D}_k$ – $\mathbf{D}$ with $(\mu|_k \gamma)(f) = \mu(\gamma \cdot_k f)$.

V_k – $\mathrm{Sym}^k(\mathbb{Q}_p^2) = \mathbb{Q}_p[X, Y]_k$ with
$(P|\gamma)(X, Y) = P(dX - cY, -bX + aY)$.

Moments

The map

$$M : \mathrm{D} \to \prod_{j=0}^{\infty} \mathbb{Q}_p$$
$$\mu \mapsto \left(\mu(z^j)\right) j = 0^{\infty}$$

is injective, with image the bounded sequences.

The map

$$\rho_k : \mathrm{D}_k \to V_k$$
$$\mu \mapsto \int (Y - zX)^k d\mu(z) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \mu(z^j) X^j Y^{k-j}$$

is $S_0(p)$-equivariant.

Computing with Distributions

D^0 – $\{\mu \in \mathrm{D} : \mu(z^j) \in \mathbb{Z}_p$ for all $j\}$.

Fil^m – $\{\mu \in \mathrm{D}^0 : v_p(\mu(z^j)) \geq m - j\}$.

$\mathcal{F}^m$ – $\mathrm{D}^0 / \mathrm{Fil}^m$, a finite $\mathbb{Z}_p$-module.

We will define Hecke operators via the action of $S_0(p)$ and Fil^m is chosen to be stable under this action.

Overconvergent Modular Symbols

- Let N be prime to p and $\Gamma = \Gamma_0(Np) \subset S_0(p)$.
- An overconvergent modular symbol is an element of $\mathrm{Smb}_\Gamma(\mathrm{D}_k)$. Have Hecke operators.
- Approximate by elements of $\mathrm{Smb}_\Gamma(\mathcal{F}_k^m)$, Hecke operators descend.
- The *slope* of an eigensymbol φ is the valuation of the U_p-eigenvalue.
- Specialization map $\rho^* : \mathrm{Smb}_\Gamma(\mathrm{D}_k) \to \mathrm{Smb}_\Gamma(V_k)$ is surjective, isomorphism on the slope $< (k+1)$ piece.

Overconvergent Modular Symbols in Sage

Sage

Break for Sage demo: `https://cloud.sagemath.com`

Application: p-adic L-functions

Classically, $\zeta(1-k)$ *p-adically interpolates* for positive integers k.
Kummer congruences:
if $h \equiv k \pmod{\phi(p^m)}$ then $\frac{B_h}{h} \equiv \frac{B_k}{k} \pmod{p^m}$.

Can do the same for other L-functions. For example, if $f \in S_{k+2}(\Gamma, \bar{\mathbb{Q}})$ is a slope $h < k+1$ eigenform, define the p-adic L-function of f to be the unique distribution μ_f on $\mathbb{Z}_p^\times$ so that if χ is a character of $\mathbb{Z}_p^\times$ with conductor p^n and $0 \leq j \leq k$, then

$$\mu_f(z^j \cdot \chi) = \frac{1}{\alpha^n} \cdot \frac{p^{n(j+1)}}{(-2\pi i)^j} \cdot \frac{j!}{\tau(\chi^{-1})} \cdot \frac{L(f, \chi^{-1}, j+1)}{\Omega_f^\pm}.$$

Here α is the U_p-eigenvalue of f, $\tau(\chi^{-1})$ is a Gauss sum and $\Omega_f^\pm$ are complex periods.

Computation of p-adic L-functions

The classical construction of μ_f involves an integral, the computation of which requires a Riemann sum. The resulting algorithm for computing μ_f is exponential in the desired precision.

Pollack and Stevens show that there is an overconvergent eigensymbol Φ_f, lifting the symbol φ_f, so that

$$\mu_f = \Phi_f(\{\infty\} - \{0\})|_{\mathbb{Z}_p^\times}.$$

The resulting algorithm for computing μ_f is polynomial in the desired precision.

p-adic L-functions in Sage

Sage

Break for Sage demo: `https://cloud.sagemath.com`

Hida Families

Let $\mathcal{W} = \lim_{\leftarrow m} (\mathbb{Z}/\phi(p^m)\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.
Hida constructed families of overconvergent modular forms with varying *weight*. These families

- consisted of *ordinary forms*: slope 0,
- extended over all of weight space $\mathcal{W}$,
- have constant rank over weight space.

These families form a part of the *eigencurve*, a rigid analytic object parameterizing overconvergent modular forms.

Ongoing work: positive slope families

The remainder of the eigencurve corresponds to families of overconvergent forms with *positive slope*. Want to compute power series that give the Hecke eigenvalues as a function of varying *weight*. These power series will be valid only in subsets of weight space (discs and annuli).

Idea

Use overconvergent modular symbols to find eigenvalues at specific weights and interpolate.

Overconvergent modular symbols are crucial since the weights will be *large*.

More details: positive slope families

Solved Problem

Need to match corresponding eigenvalues between different weights. Solution: since eigenvalues vary p-adically, their reduction modulo p is constant over small discs. Can use reductions for varying T_ℓ as a *signature* to match between different weights.

Unsolved Problem

In higher slope, finding eigenvalues at a fixed weight involves iterating $\frac{U_p}{p^h}$. For positive h, we have been unable to avoid devastating precision loss.