Calculating Automorphic Forms for Unitary Groups in SAGE

David Loeffler

Department of Mathematics
Imperial College, London

SAGE Days 6, November 2007

Aims of this Talk

- Introduce automorphic forms
- Special cases amenable to calculation
- Experimental results calculated using SAGE
- Room for optimization

Outline of talk

Outline

Motivation: Lie Groups

- G connected real Lie group e.g. $S^1 \times S^3$, $GL_2(\mathbb{R})$
- Good classification theory exists
- Γ some discrete subgroup
- Coset space $\Gamma \backslash G$ has G-invariant measure for nice G
- Want to understand $L^2(\Gamma \backslash G)$

K-types

- K maximal compact subgroup
- A K-type is an irreducible representation of K
- Decompose $L^2(\Gamma\backslash G)$ by K-types
- Irreducible constituents correspond to *automorphic forms*

Classical Example: Modular Forms

Definition

Let $\mathbb{H}$ upper half-plane, $\Gamma \subset SL_2(\mathbb{Z})$ discrete subgroup, $k \geq 0$ integer. Then an automorphic form of level Γ and weight k is

$$f : \mathbb{H} \to \mathbb{C} \mid f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

(+ some analytic conditions)

- Automorphic forms for the group SL_2
- Rich arithmetical structure

Outline

Algebraic Groups

- Variety with group structure "compatible" with variety structure
- Two major classes
  - Projective case: Abelian varieties – always commutative
  - Affine case: Linear algebraic groups – always embed in a matrix group
- All groups are extensions of Abelian by linear (Chevalley) (K perfect)

Linear algebraic groups

- Determined up to isogeny by Lie algebra
- Radical = largest solvable subgroup
  - Semisimple if trivial radical
  - Reductive if radical = centre
- Reductive $\Rightarrow$ representations are *completely reducible*
- Strong classification theory for reductive groups over algebraically closed fields
  - Isogenous to a product of tori and simple groups
  - Simple groups up to isogeny:
    - Infinite families A_n, B_n, C_n, D_n
    - Six exceptional cases: E_6, E_7, E_8, F_4 and G_2.

Forms of groups and Galois cohomology

- L subfield of $\mathbb{C}$
- If G, G' isomorphic after base extension, say they are L-forms of each other
- Classified by $H^1(\mathrm{Gal}(\overline{L}/L), \mathrm{Aut}\, G)$.
- Example: SU_2 and SL_2 over $\mathbb{R}$ – drastically different topologically.

Arithmetic Subgroups

- Subgroups $H_1, H_2 \leq G(\mathbb{Q})$ commensurable if intersection has finite index in each
- Arithmetic $=$ commensurable with $G(\mathbb{Z})$
- Special case: congruence subgroups
  - Correspond to open compact subgroups of $G(\mathbb{A}_f)$, $\mathbb{A}_f$ = finite adeles of $\mathbb{Q}$
- Congruence Subgroup Problem: is every arithmetic subgroup a congruence subgroup?
  - True for $SL_n (n \geq 3)$ (Bass–Milnor–Serre)
  - False for SL_2

Outline

Automorphic Forms

- Recall $\mathbb{A} = \prod'_v \mathbb{Q}_v = \mathbb{Q} \times \hat{\mathbb{Z}} \times \mathbb{R}_{>0}$
- $\mathbb{A}_f = \prod'_{v \text{ finite}} \mathbb{Q}_v = \mathbb{Q} \times \hat{\mathbb{Z}}$
- $G(\mathbb{Q})$ discrete in $G(\mathbb{A})$
- $G(\mathbb{A})$ unimodular for G reductive
- Can consider $L^2(G(\mathbb{Q})\backslash G(\mathbb{A})/K_f)$ for $K_f \subset G(\mathbb{A}_f)$.

Equivalent Definition for Compact Groups

- Functions $G(\mathbb{A}_f) \to V$, V a $\overline{\mathbb{Q}}$-representation of G, such that
$$f(\gamma g k) = \gamma \circ f(g) \quad \forall \gamma \in G(\mathbb{Q}), k \in K_f$$
- Analytical hypotheses disappear
- Finite amount of data as
$$G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / K_f$$
is finite

Computing Automorphic Forms

- GL_2 relatively well understood
  - Modular symbols
- GL_3 much more difficult!
  - (Ash, Stevens + Pollack have something)
- G, G' isomorphic over $\overline{\mathbb{Q}} \Rightarrow$ strong relations between automorphic forms (Langlands functoriality)
- Idea: compute on a compact form of GL_3 – a unitary group.

Outline

What Is A Unitary Group?

Definition

E imaginary quadratic extension of $\mathbb{Q}$.

$$U_{n,E} = \left\{ m \in M_{n\times n}(E) \mid m\overline{m}^t = \mathrm{id} \right\}.$$

- $\mathbb{Q}$-points of a reductive algebraic group
- $\mathbb{R}$-points usual unitary group; $U_n(\mathbb{R})$ compact, but $U_n(\mathbb{C}) \cong GL_n(\mathbb{C})$.

U_n As An Adelic Group

- Can make sense of $U_n(\mathbb{Q}_p)$ for any prime p
- Also has *integral structure*: $U_n(\mathbb{Z})$ and $U_n(\mathbb{Z}_p)$ well defined
- For p any prime split in E, $U_n(\mathbb{Q}_p) \cong GL_n(\mathbb{Q}_p)$.

Outline

Double Coset Decompositions

- We know how f transforms by $G(\mathbb{Q})$ on the left and by K on the right $\Rightarrow$ determined by values on

$$G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K.$$

- Must have $f(\mu)$ fixed by $\Gamma = G(\mathbb{Q}) \cap \mu K \mu^{-1}$ (a finite group).
- The map $f \mapsto (f(\mu_1), \ldots, f(\mu_r))$ identifies the space of automorphic forms with

$$\bigoplus_{i=1}^{r} V^{\Gamma_i}.$$

Double Coset Decompositions (2)

- Given $g, h \in G(\mathbb{A}_f)$, can easily determine if g it lies in $G(\mathbb{Q})hK$: the coset $h^{-1}gK$ contains finitely many rational points, corresponding to elements of $G(\mathbb{Q})$ with bounded denominators
- In the unitary group case, this boils down to finding all $\delta \in M_{n\times n}(\mathcal{O}_E)$ with $\delta\bar{\delta}^t = m \cdot \mathrm{id}_n$ for various integers m
- This is a key problem. In practice one enumerates all the n-tuples of elements in $(a_1 \dots a_n) \in \mathcal{O}_E^n$ with $|a_1|^2 + \dots + |a_n|^2 = m$, and searches for sets of n orthogonal vectors.
- Very slow for m large: for $n = 3$ and $E = \mathbb{Q}(\sqrt{-7})$, this takes several days for $m \sim 100$.

The Mass Formula

Definition

The *mass* of the compact open subgroup K is defined as

$$\mathrm{Mass}(K) = \sum_{i=1}^{r} \frac{1}{|\Gamma_i|}$$

where $\mu_1, \ldots, \mu_r$ are double coset representatives and $\Gamma_i = G(\mathbb{Q}) \cap \mu_i K \mu_i^{-1}$.

- Much better behaved than the class number (e.g. if $K' \subset K$, $\mathrm{Mass}(K') = [K : K']\,\mathrm{Mass}(K)$).
- If $G = U_n$, the mass of $K = G(\hat{\mathbb{Z}})$ is given in terms of the special value of an L-function (Gan–Hanke–Yu).

Outline

Hecke Operators

- The spaces of automorphic forms have an action of the Hecke algebra $\mathcal{H}(G, K)$.
- Abstractly this is the algebra of functions $G(\mathbb{A}_f) \to \mathbb{Q}$ which are invariant on both sides by K.
- Splits into a product of local Hecke algebras at each prime ℓ.
- If ℓ is split in E (so $G(\mathbb{Q}_\ell) = GL_n(\mathbb{Q}_\ell)$), the local Hecke algebra is isomorphic to the symmetric polynomials in n variables
- Generators are double cosets of the form $\mathrm{diag}(1, \ldots, 1, \ell, \ldots, \ell)$.

Hecke Cosets

- The double coset $K\eta K$ acts on automorphic forms as follows: if $K\eta K = \bigsqcup_i \eta_i K$, then

$$([K\eta K] \circ f)(g) = \sum_i f(g\eta_i)$$

- If η is one of the basic Hecke operators at a split prime ℓ, then a set of coset representatives $\eta_s \in G(\mathbb{Q}_\ell)$ can be found easily by linear algebra
- One must then express each product $\mu_r \eta_s$ in the form $\gamma \mu_t k$ using the algorithm from before (store γ and discard k)

Some Short Cuts

- Can combine finding Hecke operators with finding the class group
- One-off calculation (independent of weight)
- Can skip parts of the computation using commutativity of the Hecke algebra

Outline

Representations of GL_n

- Irreducibles determined by highest weight
- Explicit models known using geometry of flag varieties (Borel-Weil-Bott theorem)
- SYMMETRICA?
- I coded a horrible combinatorial bodge, and another cleaner (but slower) approach using polynomial rings

Outline

Double cosets

- Used $G = U_{n,E}$ for $n = 3$, $E = \mathbb{Q}(\sqrt{-7})$, $K = G(\hat{\mathbb{Z}})$
- Split primes are those 1, 2 or 4 $\pmod 7$
- No nontrivial roots of unity in $E \Rightarrow |G(\mathbb{Z})| = 2^n n! = 48$
- Mass formula gives $\text{Mass}(K) = \frac{1}{42}$, so missing at least one coset

Nontrivial Double Coset

- The element

$$\mu_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & -1 & 2 \end{pmatrix} \in G(\mathbb{Q}_2)$$

  isn't in $G(\mathbb{Q})K$
- $G(\mathbb{Q}) \cap \mu_2 K \mu_2^{-1}$ has order 336
- $\frac{1}{48} + \frac{1}{336} = \frac{1}{42}$ so finished

Dimensions of Spaces

(Can be found efficiently using classical invariant theory)

		a					
		0	1	2	3	4	5
	0	2	0	1	0	3	0
	1	0	0	0	1	1	2
b	2	1	0	2	1	5	2
	3	0	1	1	4	3	6
	4	3	1	5	3	8	7
	5	0	2	2	6	7	10

The Trivial Representation

- $cl(G) = 2 \Rightarrow$ 2-dimensional space of trivial weight forms
- No central character so $T_{p,p,p}$ acts trivially and $T_p = T_{p,p}$
- Constant function has T_p-eigenvalue $p^2 + p + 1$
- Other eigenform:

p	2	11	23	29	37
a_p	-1	5	41	-25	-1

- For $\mathfrak{p}$ a prime above p we have T_p eigenvalue

$$\lambda_p = \mathfrak{p}^2 + \mathfrak{p}\bar{\mathfrak{p}} + \bar{\mathfrak{p}}^2.$$

Nontrivial Weights

- For $(2,0,0)$ there is a unique form whose $T_{\mathfrak{p}}$ eigenvalue is $\mathfrak{p}^4/\overline{\mathfrak{p}}^2 + \mathfrak{p}\overline{\mathfrak{p}} + \overline{\mathfrak{p}}^2$.
- For $(2,2,0)$ there are two forms. One has $T_{\mathfrak{p}}$ eigenvalue $\mathfrak{p}\overline{\mathfrak{p}}\left(\frac{\mathfrak{p}}{\overline{\mathfrak{p}}}^3 + 1 + \frac{\overline{\mathfrak{p}}}{\mathfrak{p}}^3\right)$. The other is more subtle: $T_{\mathfrak{p}}$ acts as $p + \frac{1}{p^2} a_p$ where a_p is the Hecke eigenvalue of a modular form of weight 7 and level $\Gamma_1(7)$.
- For $(3,1,0)$ there is a unique form whose Hecke eigenvalue of $T_{\mathfrak{p}}$ is given by $p + \frac{1}{\mathfrak{p}\overline{\mathfrak{p}}^3} a_p$ where a_p is the same classical modular eigenvalue as before!
- First geninunely 3-dimensional form turns up at weight $(3,3,0)$

Galois Representations

- To an eigenform f, can associate a system of representations

$$\rho_f : \mathrm{Gal}(\overline{E}/E) \to GL_3(\overline{\mathbb{Q}}_\ell).$$

- Endoscopic forms correspond to direct sums of lower-dimensional representations
- ρ_f conjecturally extends to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to L^G(\overline{\mathbb{Q}}_\ell)$ (the Langlands L-group).
- This is false for U_2!
- Buzzard is working on finding a correct formulation

Computational bottlenecks

- Calculating "r-good matrices" (matrices $m \in GL_n(\mathcal{O}_E)$ with $m\overline{m}^t = r.\mathrm{id}$)
- Finding large symmetric powers of matrices