Algorithmic Treatment of Algebraic Modular Forms

Diamant Symposium
Fall 2015

Sebastian Schönnenbeck
November 27, 2015

Experimental and constructive algebra

RWTH AACHEN UNIVERSITY

A Classical Problem

$V = \mathbb{Q}^n$, $q : V \to \mathbb{Q}$ a positive definite quadratic form.
$L, L' \subset V$ lattices (i.e. $\mathbb{Z}$-submodules in V of rank n)

- L, L' *isometric*, $L \cong L'$, iff $gL = L'$ for some $g \in O(q)$; $\mathrm{class}(L) = \{M \mid M \cong L\}$.
- L, L' in the *same genus*, iff for all p prime there is $g_p \in O(\mathbb{Q}_p \otimes V, \mathbb{Q}_p \otimes q)$ with $g_p(\mathbb{Z}_p \otimes L) = \mathbb{Z}_p \otimes L'$.
- L, L' isometric implies L, L' in the same genus **but** the converse is false.
- The genus of L decomposes into finitely many isometry classes; $\mathrm{genus}(L) = \mathrm{class}(L_1) \sqcup ... \sqcup \mathrm{class}(L_r)$, r the *class number* of L.

Question: How do we find representatives for the isometry classes in a given genus?

Theorem (Eichler, Kneser)

Assume L even (i.e. $q(L) \subset 2\mathbb{Z}$) of rank greater or equal 3, $\det(L)$ squarefree, and $p \nmid \det(L)$ prime. Then every class in the genus of L is represented by a lattice M such that

$$\mathbb{Z}_q \otimes L = \mathbb{Z}_q \otimes M \;\forall\, q \neq p.$$

Strong Approximation and the Kneser Method

Neighbours

L as before. $M, N \in \mathrm{genus}(L)$ are called p-neighbours, $M \overset{p}{-} N$ if

$$[M : M \cap N] = [N : M \cap N] = p.$$

Theorem (Kneser)

For $M \in \mathrm{genus}(L)$ there is an $M' \in \mathrm{class}(M)$ and a chain of lattices $L = L_0, L_1, ..., L_k = M'$ such that

$$L_0 \overset{p}{-} L_1 \overset{p}{-} L_2 \overset{p}{-} ... \overset{p}{-} M'.$$

Neighbouring Graph

The p-neighbouring graph of $\mathrm{genus}(L)$ is the directed weighted graph with vertices the isometry classes in $\mathrm{genus}(L)$ and edges $\mathrm{class}(L_i) \to \mathrm{class}(L_j)$ weighted by the number of p-neighbours of L_i isometric to L_j.

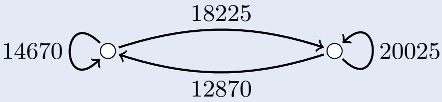
Example

Dimension 16

There are two isometry classes in the set of even unimodular lattices of rank 16:

$$\mathrm{class}(E_8 \perp E_8) \sqcup \mathrm{class}(D_{16}^{+}).$$

The 2-neighbouring graph of this genus is:



Remark

- Note that $18225 + 14670 = 12870 + 20025$, number of neighbours does not depend on the class.
- Note that $\frac{18225}{12870} = \frac{|\mathrm{Aut}(E_8 \perp E_8)|}{|\mathrm{Aut}(D_{16}^{+})|}$.
- The adjacency matrix of the graph acts as a Hecke operator on the space of modular forms generated by the theta series of the two lattices (Eichler, Andrianov, Yoshida).

Algebraic Modular Forms

Notation: $\mathbb{G}$ almost simple algebraic group defined over $\mathbb{Q}$, $\mathbb{G}(\mathbb{R})$ compact, V a f.d. $\mathbb{Q}$-rational representation of $\mathbb{G}$, $\mathbb{A}_f$ the finite adeles of $\mathbb{Q}$.

Definition [Gross '99]

$K \leq \mathbb{G}(\mathbb{A}_f)$ open and compact.

$$M(V,K) := \{f : \mathbb{G}(\mathbb{A}_f) \to V \mid f(gxk) = gf(x) \text{ for all } g \in \mathbb{G}(\mathbb{Q}), x \in \mathbb{G}(\mathbb{A}_f), k \in K\},$$

the space of *algebraic modular forms* of *level* K and *weight* V.

Remark

- $|gKg^{-1} \cap \mathbb{G}(\mathbb{Q})| < \infty$ for all $g \in \mathbb{G}(\mathbb{A}_f)$.
- $|\mathbb{G}(\mathbb{Q})\backslash\mathbb{G}(\mathbb{A}_f)/K| < \infty$.
- Let $\mathbb{G}(\mathbb{A}_f) = \bigsqcup_{i=1}^{r} \mathbb{G}(\mathbb{Q})\gamma_i K$ and $\Gamma_i := \gamma_i K \gamma_i^{-1} \cap \mathbb{G}(\mathbb{Q})$ then

$$M(V,K) \cong_{\mathbb{Q}} \bigoplus_{i=1}^{r} V^{\Gamma_i}.$$

The Hecke Algebra

Definition

$K \leq \mathbb{G}(\mathbb{A}_f)$ open and compact.

$$H_K := \{f : \mathbb{G}(\mathbb{A}_f) \to \mathbb{Q} \mid f \text{ compactly supported and } K\text{-bi-invariant}\}$$

with multiplication by convolution. The *Hecke algebra* of $\mathbb{G}$ with respect to K.

Remark

- H_K has the natural basis $\mathbb{1}_{K\gamma K},\ K\gamma K \in \mathbb{G}(\mathbb{A}_f)/\!\!/K$.
- Let $\gamma_1, \gamma_2 \in \mathbb{G}(\mathbb{A}_f)$ with $K\gamma_i K = \bigsqcup_j \gamma_{i,j} K$. The multiplication in H_K is

$$\mathbb{1}_{K\gamma_1 K}\mathbb{1}_{K\gamma_2 K} = \sum_{j,j'} \mathbb{1}_{\gamma_{1,j}\gamma_{2,j'}K}.$$

- If $K = \prod_p K_p$ is a product of local factors, the Hecke algebra is the restricted tensor product

$$H_K = \otimes_p' H_{K_p}.$$

The Action of the Hecke Algebra

Definition

For $\gamma \in \mathbb{G}(\mathbb{A}_f)$ we define the linear operator $T(\gamma) \in \mathrm{End}_{\mathbb{Q}}(M(V,K))$ via

$$(T(\gamma)f)(x) = \sum_i f(x\gamma_i)$$

where $f \in M(V,K)$ and $K\gamma K = \bigsqcup_i \gamma_i K$.

Remark

- The additive extension of $\mathbb{1}_{K\gamma K} \mapsto T(\gamma)$ defines an algebra homomorphism $H_K \to \mathrm{End}_{\mathbb{Q}}(M(V,K))$.
- $M(V,K)$ is a semi-simple H_K-module.

Integral Forms

What would be "interesting" / computationally well-suited open compact subgroups to consider?

Definition

Let $\mathbb{G} \hookrightarrow \mathrm{GL}_n$ be a faithful representation. An *integral form* $\mathbb{G}_L$ of $\mathbb{G}$ is given by a lattice $L \leq_{\mathbb{Z}} \mathbb{Q}^n$ via

$$\mathbb{G}_L(\mathcal{O}_k) = \mathrm{Stab}_{\mathbb{G}(k)}(\mathcal{O}_k \otimes L), \ \mathbb{G}_L(\mathbb{Z}_p) = \mathrm{Stab}_{\mathbb{G}(\mathbb{Q}_p)}(\mathbb{Z}_p \otimes L)$$

for every finite extension k of $\mathbb{Q}$ and every prime p.

Remark

- $\mathbb{G}(\mathbb{A}_f)$ acts on the integral forms via $(g_p)_p L = L'$ where $\mathbb{Z}_p \otimes L' = g_p(\mathbb{Z}_p \otimes L)$ for all p.
- $\mathrm{Stab}_{\mathbb{G}(\mathbb{A}_f)}(L) = \prod_p \mathbb{G}_L(\mathbb{Z}_p)$ is an open compact subgroup of $\mathbb{G}(\mathbb{A}_f)$.
- $\mathbb{G}_L(\mathbb{Z}_p)$ is a hyperspecial maximal compact subgroup of $\mathbb{G}(\mathbb{Q}_p)$ for all but finitely many p.
- Call L, L' ($\mathbb{G}$-)*isomorphic* if $gL = L'$ for some $g \in \mathbb{G}(\mathbb{Q})$. Say L, L' in the same *genus* if $\gamma L = L'$ for some $\gamma \in \mathbb{G}(\mathbb{A}_f)$.

Some (very informal) remarks on buildings

Associated to $\mathbb{G}(\mathbb{Q}_p)$ there is a so-called *building* $\mathcal{B}$, a simplicial complex with a $\mathbb{G}(\mathbb{Q}_p)$-action and the following properties:

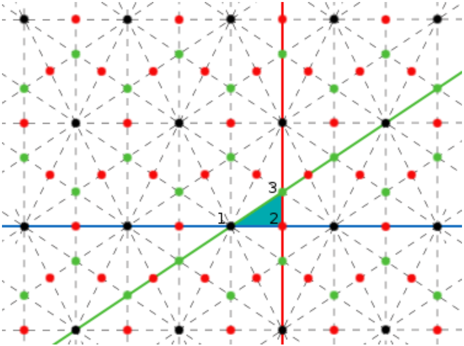
- $\mathcal{B}$ is a union of apartments A which are in bijection with the maximal $\mathbb{Q}_p$-split tori of $\mathbb{G}$.
- Each apartment is an affine Euclidean space.
- Each apartment A corresponding to T comes with an extended affine Weyl group, $\tilde{W} \cong X^\vee(T) \rtimes W_0$, where W_0 is the usual (finite) Weyl group (w.r.t. T).
- The extended affine Weyl group is an extension of an infinite Coxeter group by an abelian group.
- Every compact subgroup fixes a point in $\mathcal{B}$.
- The stabilizers of vertices are always maximal compact subgroups.
- There is a Bruhat decomposition $\mathbb{G}(\mathbb{Q}_p) = \bigsqcup_{w \in \tilde{W}} IwI$ where I is the pointwise stabilizer of a maximal simplex (chamber).

$\rightsquigarrow$ New concept of p-neighbourship (of certain lattices/ integral forms/ open compact subgroups) via closeness in the affine building.

Example: The affine building of type $\tilde{G}_2$

The group G_2 can be realized as the automorphism group of the (8-dim.) octonion algebra $\mathbb{O}$ (Dickson-double of the Hamilton quaternions).
The affine building for $G_2(\mathbb{Q}_p)$ can be realized as follows:

- There are 3 labels for the vertices, $\mathcal{V} = \mathcal{V}_1 \sqcup \mathcal{V}_2 \sqcup \mathcal{V}_3$, corresponding to 3 ($G_2(\mathbb{Q}_p)$-)classes of orders in $\mathbb{O}_p$.
- Hyperspecial vertices correspond to maximal orders.
- Adjacency is given by inclusion ($V_1 \supset V_2 \supset V_3$).
- An apartment in this building looks as follows:



Algorithmic Questions

Aim: Compute the action of $T(\gamma)$ on $M(V, K)$ (where K comes from an integral form $\mathbb{G}_L$).

Approach

- Decompose $\mathbb{G}(\mathbb{A}_f) = \bigsqcup_i \mathbb{G}(\mathbb{Q})\mu_i K$, compute $\Gamma_i = \mu_i K \mu_i^{-1} \cap \mathbb{G}(\mathbb{Q})$ and V^{Γ_i}.
- Decompose $K\gamma K = \bigsqcup_j \gamma_j K$.
- For i, j write $\gamma_j \mu_i$ as $g' \mu_{i'} k$ for some i'.

Aspects to consider

What do we have to know in order to make this work?

- Decide for two integral forms if they are $\mathbb{G}$-isomorphic / compute the stabilizer of a lattice in $\mathbb{G}(\mathbb{Q})$.
- Be able to compute a system of representatives for $\mathrm{genus}(\mathbb{G}_L)$.
- Decompose double cosets into left cosets.

Stabilizers and Isometries

$\mathbb{G} \hookrightarrow \mathrm{GL}_n$, $L, L' < \mathbb{Q}^n$ lattices.

- $\mathbb{G}(\mathbb{Q}) \subset \mathrm{GL}_n(\mathbb{Q})$ compact $\rightsquigarrow$ $\mathbb{G}(\mathbb{Q})$ fixes a definite inner product on $\mathbb{Q}^n$.
- $\mathbb{G}(\mathbb{Q}) \subset O_n(\mathbb{Q}) \rightsquigarrow \mathrm{Stab}_{\mathbb{G}(\mathbb{Q})}(L) \subset \mathrm{Stab}_{O_n(\mathbb{Q})}(L)$.
- $\mathrm{Stab}_{O_n(\mathbb{Q})}(L)$ computable (Plesken-Souvignier-algorithm) and finite $\rightsquigarrow$ Finding $\mathrm{Stab}_{\mathbb{G}(\mathbb{Q})}(L)$ reduced to a finite problem.
- Same idea for isometry testing: Find O_n-isometry $g : L \to L'$ $\rightsquigarrow$ All isometries are given by $g\,\mathrm{Stab}_{O_n(\mathbb{Q})}(L)$ $\rightsquigarrow$ Finite problem.

Example: G_2

The group G_2 can be realized as the automorphism group of the (8-dim.) octonion algebra $\mathbb{O}$ (Dickson-double of the Hamilton quaternions). G_2 fixes the inner product $(x, y) \mapsto x\bar{y}$. $L < \mathbb{O}$ lattice then $\mathrm{Stab}_{G_2}(L)$ is the stabilizer of the multiplication (which can be thought of as an element of $V^* \otimes V^* \otimes V$) in $\mathrm{Stab}_{O_8}(L)$. E.g. L a maximal order then

$$|\mathrm{Stab}_{O_8}(L)| = 696729600, \ |\mathrm{Stab}_{G_2}(L)| = 12096.$$

Genus Enumeration

Question: How do you compute representatives of $\mathrm{genus}(L)$ starting at L?

Almost Strong Approximation

If $\mathbb{G}$ is simply connected and of certain type then there is a finite set Ω of primes such that for all $p \notin \Omega$ the lattice L_p is hyperspecial and we can find representatives of $\mathrm{genus}(L)$ as p-neighbours of L.

Question: How do you know when to stop?

Mass Formula

Let $\mathrm{genus}(L) = \mathrm{class}(L_1) \sqcup \ldots \sqcup \mathrm{class}(L_r)$ and set

$$\mathrm{mass}(\mathrm{genus}(L)) := \sum_{i=1}^{r} \frac{1}{|\,\mathrm{Stab}_{\mathbb{G}}(L_i)|}.$$

Then we can compute $\mathrm{mass}(\mathrm{genus}(L))$ from information only on the local structure of L.

Examples

Some Genera for G_2

Genus	Class Number	Mass Decomposition
max. order	1	$\frac{1}{12096}$
type 2 at 3, max. else	2	$\frac{1}{192}+\frac{1}{432}$
type 2 at 5, max. else	3	$\frac{1}{192}+\frac{1}{48}+\frac{1}{36}$
type 3 at 7, max. else	2	$\frac{1}{216}+\frac{1}{42}$

Some Genera for Sp_4

Compact forms of Sp can be found as unitary groups over (definite) quaternion algebras D, integral forms via $\mathcal{O}_D$-lattices (where $\mathcal{O}_D$ is a maximal order).

Genus Representative	Class Number	Mass Decomposition
$\mathcal{O}_D^2$, $D=\left(\frac{-1,-1}{\mathbb{Q}}\right)$	1	$\frac{1}{1152}$
$\mathcal{O}_D^2$, $D=\left(\frac{-2,-5}{\mathbb{Q}}\right)$	2	$\frac{1}{240}+\frac{1}{72}$
$\mathcal{O}_D^2$, $D=\left(\frac{-2,-13}{\mathbb{Q}}\right)$	4	$\frac{1}{48}+\frac{1}{12}+\frac{2}{8}$
$\mathcal{O}_D^2$, $D=\left(\frac{-1,-23}{\mathbb{Q}}\right)$	16	$\frac{5}{4}+\frac{3}{8}+\frac{3}{12}+\frac{2}{24}+\frac{1}{32}+\frac{1}{48}+\frac{1}{72}$

Coset Decomposition

Aim: Decompose a double coset $K\gamma K$ into left cosets.
First observation: Since $H_K = \otimes'_p H_{K_p}$ we only need to do this locally.
For simplicity assume: $\mathbb{G}$ split at p, K_p "nice".

Structure of p-adic Groups (Bruhat-Tits)

$I \leq K_p \leq \mathbb{G}(\mathbb{Q}_p)$ Iwahori subgroup, $\tilde{W}(= X^\vee \rtimes W_0)$ the extended affine Weyl group.

- $\mathbb{G}(\mathbb{Q}_p) = \bigsqcup_{w \in \tilde{W}} IwI$, $K_p = \bigsqcup_{w \in W_{K_p}} IwI$ for some $W_{K_p} \leq \tilde{W}$.
- H_I is an algebra with basis $T_w,\ w \in \tilde{W}$ and multiplication $T_w T_{w'} = T_{ww'}$ if $l(ww') = l(w) + l(w')$, $T_s^2 = (p-1)T_s + p$ for the simple reflections s.
- $e := [K_p : I]^{-1} \sum_{w \in W_{K_p}} T_w \in H_I$ is an idempotent and $H_{K_p} \cong eH_I e$.

Coset Decomposition

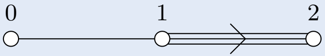
- Bruhat-Tits ('65): Explicit formula to decompose $IwI,\ w \in \tilde{W}$ into I-left cosets.
- Lansky-Pollack (2001): Explicit formula to decompose $K_p w K_p,\ w \in \tilde{W}$ into K_p-left cosets.

Example

G_2

$\mathbb{G}$ of type G_2 (simply connected and adjoint) with extended Dynkin diagram (at split prime p):

$\tilde{G}_2$:



If K open compact, with K_p hyperspecial maximal compact ($W_{K_p} = \langle s_1, s_2 \rangle$), then the local Hecke algebra H_{K_p} is a polynomial ring in two variables generated by the characteristic functions on the double cosets

$$T_1 := K_p s_0 K_p \text{ and } T_2 := K_p s_0 s_1 s_2 s_1 s_0 K_p.$$

T_1 decomposes into $q(q^5 + q^4 + q^3 + q^2 + q + 1)$ left cosets.
T_2 decomposes into $q^5(q^5 + q^4 + q^3 + q^2 + q + 1)$ left cosets.

Sp_4

In the analogous situation for Sp_4 (simply connected but not adjoint) there are also two generators which decompose into $q(q^3 + q^2 + q + 1)$ and $q^3(q^3 + q^2 + q + 1)$ left cosets, respectively.

Venkov's Method

Aim: Give an alternative method to compute neighbouring operators.
Idea: Use a generalization of the following method attributed to Venkov: L, L' two lattices then

$$\mathrm{mass}(\mathrm{genus}(L))\frac{[\mathrm{Stab}_{\mathbb{G}}(L) : \mathrm{Stab}_{\mathbb{G}}(L, L')]}{[\mathrm{Stab}_{\mathbb{G}}(L') : \mathrm{Stab}_{\mathbb{G}}(L, L')]} = \mathrm{mass}(\mathrm{genus}(L')).$$

Now: p prime such that $\mathbb{G}$ is split at p and L_p is hyperspecial,
$\mathrm{genus}(L) = [L_1] \sqcup \ldots \sqcup [L_r]$.

Neighbouring Operator

Set $N_p \in \mathbb{Z}^{r\times r}$ the matrix with

$$(N_p)_{i,j} = \{L' \mid L' p\text{-neighbour of } L_i, L' \cong L_j\}. \quad (1)$$

The neighbouring operator of $\mathrm{genus}(L)$ at p (or the Hecke operator $T(s_0)$ where s_0 is the fundamental reflection at p not fixing L) or just the adjacency matrix of the neighbouring graph.

Fix a lattice $M \leq L$ such that L, L' are p-neighbours iff $L \cap L' \in \mathrm{genus}(M)$ (very often possible).

The Venkov Transfer

Observation

We can write $\mathrm{genus}(M) = [M_1] \sqcup \ldots \sqcup [M_s]$ where each M_i is a sublattice of L_j for some j.

The Transfer Matrix

Set T_M^L the matrix given by

$$(T_M^L)_{i,j} = \{M' \mid M' \leq L_i, M' \cong M_j\}$$

and define T_L^M the other way around.

Remark

- There are often far fewer $M' \in \mathrm{genus}(M), M' \leq L$ than there are p-neighbours of L.
- $(T_M^L)_{i,j} \cdot |\,\mathrm{Stab}_{M_j}\,| = (T_L^M)_{j,i} \cdot |\,\mathrm{Stab}_{L_i}\,|$.

The Neighbouring Operator

Theorem

$T_L^M T_M^L = a \cdot I_r + N_p$ where a is the number of lattices in the genus of M contained in L.

Generalization

We can generalize this method to include other operators and modular forms of arbitrary weight:
Let K_1, K_2 be two open compact subgroups and let $K_2 = \bigsqcup k_i(K_1 \cap K_2)$. Then we get an operator

$$T_2^1 : M(V, K_1) \to M(V, K_2),\ f \mapsto f' \text{ where } f'(x) = \sum_i f(xk_i).$$

This is well-defined and generalizes the T_M^L from above.

Some Remarks

Properties of the operators T_2^1

- T_M^L is the matrix of T_2^1 where K_1 is the stabilizer of L, K_2 is the stabilizer of M and V is the trivial representation.
- T_2^1 and T_1^2 are adjoint to each other with respect to certain scalar products. In particular we can compute T_1^2 if we know T_2^1 (and some other easily obtained information).
- $T_1^2 T_2^1 : M(V, K_1) \to M(V, K_1)$ acts as an element of the Hecke algebra (w.r.t. K_1).
- Under certain conditions we have explicit knowledge of the cosets appearing in $T_1^2 T_2^1$ (e.g. if K_1 and K_2 differ only at one (split) prime and $\mathbb{G}$ is simply connected).
- The local Hecke algebra for simply connected groups of type C_n at hyperspecial primes is generated by n operators of the form $T_1^2 T_2^1$.
- In general these operators do not generate the whole Hecke algebra.