Computing Hilbert modular forms over fields with nontrivial class group

L. Dembélé and Steve Donnelly

May 21, 2008

Outline

- Hilbert modular forms
- Modularity conjecture
- Brandt modules
- Algorithm
- Examples

Notations

- Let F be a totally real number field of even degree g.
- Let v_i, $i = 1, \ldots, g$, be all the real embeddings of F. And, for every $a \in F$, let $a_i = v_i(a)$ be the image of a under v_i.
- We let $\mathcal{O}_F$ be the ring of integers of F.
- Let $\mathfrak{N}$ be an integral ideal of F.
- Let $\mathfrak{N}_i$, $i = 1, \ldots, h^+$, be a complete set of representatives of the narrow class group $\mathrm{Cl}^+(F)$.
- For each ideal $\mathfrak{N}_i$, we define the group

$$\Gamma_0(\mathfrak{N}, \mathfrak{N}_i) = \left\{ \gamma \in \begin{pmatrix} \mathcal{O}_F & \mathfrak{N}_i^{-1} \\ \mathfrak{N}\mathfrak{N}_i & \mathcal{O}_F \end{pmatrix} : \det(\gamma) \in \mathcal{O}_F^\times, \det(\gamma) \gg 0 \right\}.$$

- Let $\mathfrak{H} = \{x + iy \in \mathbb{C} : y > 0\}$ be the Poincaré upper half-plane.

Definition

A **classical Hilbert modular form** *of level* $\Gamma_0(\mathfrak{N}, \mathfrak{N}_i)$ *and parallel weight 2 is a holomorphic function* $f : \mathfrak{H}^g \to \mathbb{C}$ *given by a power series*

$$f(z) = \sum_{\substack{\mu=0, \\ \mu \gg 0}} a_\mu^{(i)} e^{2\pi i(\mu_1 z_1 + \cdots + \mu_g z_g)}$$

such that

$$f\left(\frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \ldots, \frac{a_g z_g + b_g}{c_g z_g + d_g}\right) = \left(\prod_{i=1}^{g} \det(\gamma_i)^{-1}(c_i z_i + d_i)^2\right) \times f(z_1, \cdots, z_g),$$

for all $\gamma \in \Gamma(\mathfrak{N}, \mathfrak{N}_i)$.

Hilbert modular forms

Definition

The space of **Hilbert modular forms** *is given by*

$$M_2(\mathfrak{N}) = \bigoplus_{i=1}^{h^+} M_2(\Gamma_0(\mathfrak{N}, \mathfrak{N}_i)).$$

In other words, a **Hilbert modular form** *of parallel weight 2 and level $\mathfrak{N}$ is an h^+-tuple of classical Hilbert modular forms.*

Let $f = (f_1, \ldots, f_{h^+})$ be a Hilbert modular form. We say that f is a **cusp form** *if $a_0^{(i)} = 0$ for all $i = 1, \ldots, g$.*

We denote the space of cusp forms by $S_2(\mathfrak{N})$.

Hilbert modular forms

Definition

Let $f = (f_1, \ldots, f_{h^+})$ be a Hilbert cusp form of parallel weight 2 and level $\mathfrak{N}$.

Let $\mathfrak{m}$ be an integral ideal, and $\mathfrak{N}_i$ be the unique representative such that $\mathfrak{m} = (\mu)\mathfrak{N}_i^{-1}$. **Then $a_\mu^{(i)}$ only depends on $\mathfrak{m}$.**

We call it the **Fourier coefficient** *of f at $\mathfrak{m}$ and denote it by* **$a_{\mathfrak{m}}(f)$.**

The **L-series** *attached to f is defined by*

$$L(f, s) := \sum_{\mathfrak{m} \subseteq \mathcal{O}_F} \frac{a_{\mathfrak{m}}(f)}{\mathrm{N}(\mathfrak{m})^s}.$$

This converges for $\mathrm{Re}(s)$ large enough.

Hilbert modular forms

There is a commuting family of diagonalizable operators called the **Hecke operators** which acts on the space of Hilbert modular forms $M_2(\mathfrak{N})$.

We say that a cusp form f is a **newform** if it is a common eigenvector of the Hecke operators and $a_{(1)}(f) = 1$.

This theorem explains in parts the interest of number theorists into modular forms.

Theorem (Shimura)

Let f be a newform. Then the coefficients $a_{\mathfrak{m}}(f)$ are **algebraic integers.** *More specifically, $\mathbb{Q}(a_{\mathfrak{m}}(f), \mathfrak{m} \subseteq \mathcal{O}_F)$ is a number field, and $L(f, s)$ admits an Euler product.*

Modularity over totally real number fields

Let A be an abelian variety over F.

As in the classical setting, we can define the L-series of A again by counting points.

We say that A is **modular** if there exists an integral ideal $\mathfrak{N}$ in F and a newform f of level $\mathfrak{N}$ and parallel weight 2 such that $L(A, s) = L(f, s)$.

Conjecture (Shimura-Taniyama)

Let A/F be an abelian variety (of GL_2-type). Then, there exists an integral ideal $\mathfrak{N}$ and a newform f of level $\mathfrak{n}$ and weight $(2, 2)$ such that

$$L(A, s) = L(f, s).$$

Modularity over totally real number fields

In the classical setting, this is now a theorem of Khare-Wintenberger et al.

The totally real case is very less understood. Hence the need to experiment.

Experimentation was crucial in the understanding of the classical case.

Brandt modules

- We let B be a division quaternion algebra over F such that $B \otimes \mathbb{R} \cong \mathbb{H}^g$, where $\mathbb{H}$ is the Hamilton quaternion algebra, and such that the completion of B at any finite prime $\mathfrak{p}$ is the matrix algebra.
- We choose a maximal order R of B.
- Let $\mathrm{Cl}(R)$ denote a complete set of representatives of all the right ideal classes of R (**appropriately chosen**).
- For any $\mathfrak{a} \in \mathrm{Cl}(R)$, we let $R_{\mathfrak{a}}$ be the left order of $\mathfrak{a}$.
- We fix an isomorphism $R \otimes (\mathcal{O}_F/\mathfrak{N}) \cong M_2(\mathcal{O}_F/\mathfrak{N})$.

Brandt modules

Let $M_2^{R_{\mathfrak{a}}}(\mathfrak{N}) := \mathbb{Z}[\Gamma_{\mathfrak{a}} \backslash \mathbf{P}^1(\mathcal{O}_F/\mathfrak{N})]$, where $\Gamma_{\mathfrak{a}} = R_{\mathfrak{a}}^{\times}/\mathcal{O}_F^{\times}$ is a finite group.

For each $\mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(R)$ and any prime $\mathfrak{p}$ in $\mathcal{O}_F$, put

$$\Theta^{(S)}(\mathfrak{p};\, \mathfrak{a},\, \mathfrak{b}) := R_{\mathfrak{a}}^{\times} \backslash \left\{ u \in \mathfrak{a}\mathfrak{b}^{-1} : \frac{(\mathrm{nr}(u))}{\mathrm{nr}(\mathfrak{a})\mathrm{nr}(\mathfrak{b})^{-1}} = \mathfrak{p} \right\},$$

where $R_{\mathfrak{a}}^{\times}$ acts by multiplication on the left.

We define the linear map $T_{\mathfrak{a},\,\mathfrak{b}}(\mathfrak{p}) : M_2^{R_{\mathfrak{b}}}(\mathfrak{N}) \to M_2^{R_{\mathfrak{a}}}(\mathfrak{N})$ by

$$T_{\mathfrak{a},\,\mathfrak{b}}(\mathfrak{p}) f(x) = \sum_{u \in \Theta^{(S)}(\mathfrak{p};\, \mathfrak{a},\, \mathfrak{b})} f(ux).$$

Brandt modules

Theorem (Shimizu, Jacquet-Langlands)

There is an isomorphism of Hecke modules

$$M_2(\mathfrak{N}) \simeq \bigoplus_{\mathfrak{a}\in \mathrm{Cl}(R)} M_2^{R_{\mathfrak{a}}}(\mathfrak{N}),$$

where the action of the Hecke operator $T(\mathfrak{p})$ on the right is given by the collection of linear maps $(T_{\mathfrak{a},\mathfrak{b}}(\mathfrak{p}))$ for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(R)$.

Precomputations

1. Find a set of prime ideals S not dividing $\mathfrak{N}$ that generate $\mathrm{Cl}^+(F)$.
2. Find a presentation of the quaternion algebra B/F ramified at precisely the infinite places, and compute a maximal order R of B.
3. Compute a complete set $\mathrm{Cl}(R)$ of representatives $\mathfrak{a}$ for the right ideal classes of R such that the primes dividing $\mathrm{nr}(\mathfrak{a})$ belong to S.
4. For each representative $\mathfrak{a} \in \mathrm{Cl}(R)$, compute its left order $R_\mathfrak{a}$, and compute the unit group $\Gamma_\mathfrak{a} = R_\mathfrak{a}^\times / \mathcal{O}_F^\times$.
5. Compute the sets $\Theta^{(S)}(\mathfrak{p};\ \mathfrak{a},\ \mathfrak{b})$, for all primes $\mathfrak{p}$ with $N\mathfrak{p} \leq b$ and all $\mathfrak{a},\ \mathfrak{b} \in \mathrm{Cl}(R)$.

Algorithm

1. Compute a splitting isomorphisms
$$(R \otimes \mathcal{O}_F/\mathfrak{N})^\times \cong \mathbf{GL}_2(\mathcal{O}_F/\mathfrak{N}).$$
2. For each $\mathfrak{a} \in \mathrm{Cl}(R)$, compute $M_2^{R_\mathfrak{a}}(\mathfrak{N})$ as the module
$$M_2^{R_\mathfrak{a}}(\mathfrak{N}) = \mathbb{Z}[\Gamma_\mathfrak{a} \backslash \mathbf{P}^1(\mathcal{O}_F/\mathfrak{N})].$$
3. Combine the results of step (2), forming the direct sum
$$M_2(\mathfrak{N}) = \bigoplus_{\mathfrak{a} \in \mathrm{Cl}(R)} M_2^{R_\mathfrak{a}}(\mathfrak{N}).$$
4. For every prime $\mathfrak{p}$, compute the Brandt matrix of $T_\mathfrak{p}$ acting on $M_2(\mathfrak{N})$.

Brandt modules

Remark

- *The main improvement to the current algorithm lies in the precomputation phase.*
- *An improvement of the lattice enumeration process led to a substantial speed up in this phase.*
- *The complexity of this phase depends only on the base field F.*
- *The main part of the algorithm is essentially linear algebra.*

Example: $\mathbb{Q}(\sqrt{10})$

Theorem

Let F be the real quadratic field $\mathbb{Q}(\sqrt{10})$ and $H = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ its Hilbert class field. Then, we have the followings:

- **a)** *Up to isogeny, there is a unique modular abelian variety A over F with everywhere good reduction; and it is a simple abelian surface with real multiplication by $\mathbb{Z}[\sqrt{2}]$.*
- **b)** *The abelian surface A is of the form $A = \mathrm{Res}_{H/F}(E)$, where E is an elliptic curve with everywhere good reduction over H.*

Example: $\mathbb{Q}(\sqrt{10})$

Ideas of the proof:

- We compute all the Hilbert newforms of level 1 and weight $(2, 2)$ and weight $(2, 2, 2, 2)$ over F and H respectively. Then we obtained the tables below.
- We observe that all the form on H are base change from F.
- We then search for the corresponding motives.
- Finally, we prove that the motives we found are modular.

Example: $\mathbb{Q}(\sqrt{10})$

The Hilbert class field of F is $H := \mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\alpha)$, where the minimal polynomial of α is $x^4 - 2x^3 - 5x^2 + 6x - 1$. We consider the integral basis

$$\begin{aligned} \alpha_1 &:= 1, \\ \alpha_2 &:= \frac{1}{3}(2\alpha^3 - 3\alpha^2 - 10\alpha + 7), \\ \alpha_3 &:= \frac{1}{3}(-2\alpha^3 + 3\alpha^2 + 13\alpha - 7), \\ \alpha_4 &:= \frac{1}{3}(-\alpha^3 + 3\alpha^2 + 5\alpha - 8). \end{aligned}$$

Then E/H is given by

	a_1	a_2	a_3	a_4	a_6
E :	$[0, 0, 1, 0]$	$[1, 0, 1, -1]$	$[0, 1, 0, 0]$	$[-15, -44, -21, -26]$	$[-91, -123, -48, -97]$

Example: $\mathbb{Q}(\sqrt{10})$

$N(\mathfrak{p})$	$\mathfrak{p}$	f_1	f_2	f_3
2	$(2, \omega_{40})$	-3	3	$-\sqrt{2}$
3	$(3, \omega_{40}+4)$	-4	4	$\sqrt{2}$
3	$(3, \omega_{40}+2)$	-4	4	$\sqrt{2}$
5	$(5, \omega_{40})$	-6	6	$-2\sqrt{2}$
13	$(13, \omega_{40}+6)$	-14	14	0
13	$(13, \omega_{40}+7)$	-14	14	0
31	$(31, \omega_{40}+14)$	32	32	4
31	$(31, \omega_{40}+17)$	32	32	4
37	$(37, \omega_{40}+11)$	-38	38	$6\sqrt{2}$
37	$(37, \omega_{40}+26)$	-38	38	$6\sqrt{2}$

Table: Hilbert modular forms of level 1 and weight $(2,2)$ over $\mathbb{Q}(\sqrt{10})$.

Example: $\mathbb{Q}(\sqrt{10})$

$N(\mathfrak{p})$	$\mathfrak{p}$	f_1	f_2
4	$[0, 0, 1, 0]$	5	-2
9	$[1, 1, -1, 0]$	10	-4
9	$[0, 1, -1, 1]$	10	-4
25	$[1, -2, 0, 0]$	26	-2
31	$[1, 1, 1, -1]$	32	4
31	$[1, -1, -1, -1]$	32	4
31	$[1, 1, -1, 1]$	32	4
31	$[-3, 2, -1, 0]$	32	4

Table: Hilbert modular forms of level 1 and weight $(2, 2, 2, 2)$ over the Hilbert class field H of $\mathbb{Q}(\sqrt{10})$.

Example: $\mathbb{Q}(\sqrt{257})$

$N(\mathfrak{p})$	$\mathfrak{p}$	EIS1	257A	257B	257C	EIS2
2	$(2, \omega_{257})$	3	-1	$\frac{1+\sqrt{13}}{2}$	$\frac{1+\sqrt{-3}}{2}$	$\frac{-3+3\sqrt{-3}}{2}$
2	$(2, 1-\omega_{257})$	3	-1	$\frac{1-\sqrt{13}}{2}$	$\frac{1-\sqrt{-3}}{2}$	$\frac{-3-3\sqrt{-3}}{2}$
9	(3)	10	4	-4	4	10
11	$(11, 4+\omega_{257})$	12	0	1	0	$-6+6\sqrt{-3}$
11	$(11, 5-\omega_{257})$	12	0	1	0	$-6-6\sqrt{-3}$
13	$(13, 9+\omega_{257})$	14	2	$\sqrt{13}$	$-1+\sqrt{-3}$	$-7-7\sqrt{-3}$
13	$(13, 10-\omega_{257})$	14	2	$-\sqrt{13}$	$-1-\sqrt{-3}$	$-7+7\sqrt{-3}$
17	$(17, 11+\omega_{257})$	18	4	$4+\sqrt{13}$	$-2-2\sqrt{-3}$	$-9+9\sqrt{-3}$
17	$(17, 12-\omega_{257})$	18	4	$4-\sqrt{13}$	$-2+2\sqrt{-3}$	$-9-9\sqrt{-3}$

Table: Hilbert modular forms of level 1 and weight $(2, 2)$ over $\mathbb{Q}(\sqrt{257})$.

Example $\mathbb{Q}(\sqrt{257})$

$N(\mathfrak{p})$	$\mathfrak{p}$	257D
2	$(2, \omega_{257})$	β
2	$(2, 1-\omega_{257})$	$(\beta^3+\beta^2+4\beta-3)/3$
9	(3)	-4
11	$(11, 4+\omega_{257})$	$(-\beta^3-4\beta^2-4\beta-9)/12$
11	$(11, 5-\omega_{257})$	$(\beta^3+4\beta^2+4\beta-3)/12$
13	$(13, 9+\omega_{257})$	$(-7\beta^3-4\beta^2-28\beta+21)/12$
13	$(13, 10-\omega_{257})$	$(-\beta^3-4\beta^2-28\beta-9)/12$
17	$(17, 11+\omega_{257})$	$(-\beta^3-4\beta^2+4\beta-9)/4$
17	$(17, 12-\omega_{257})$	$(11\beta^3+20\beta^2+44\beta-33)/12$

Table: Hilbert modular forms of level 1 and weight $(2,2)$ over $\mathbb{Q}(\sqrt{257})$ (cont'd). (Here the minimal polynomial of β is given by $x^4+x^3+4x^2-3x+9$.)

Example: $\mathbb{Q}(\sqrt{401})$

In this case $h_F = h_F^+ = 5$.

Our algorithm gives the dimensions $\dim M_2(1) = 125$ and $\dim S_2(1) = 120$.

The forms that are base change come from the space of classical modular forms $S_2(401, (\frac{401}{}))$, which has dimension 32.

Thus the dimension of the subspace of newforms that are not base change is $120 - 32/2 = 104$.