MATHEMATICS OF COMPUTATION
Volume 80, Number 274, April 2011, Pages 1071–1092
S 0025-5718(2010)02423-8
Article electronically published on September 30, 2010

COMPUTING SYSTEMS OF HECKE EIGENVALUES ASSOCIATED TO HILBERT MODULAR FORMS

MATTHEW GREENBERG AND JOHN VOIGHT

Abstract. We utilize effective algorithms for computing in the cohomology of a Shimura curve together with the Jacquet-Langlands correspondence to compute systems of Hecke eigenvalues associated to Hilbert modular forms over a totally real field F.

The design of algorithms for the enumeration of automorphic forms has emerged as a major theme in computational arithmetic geometry. Extensive computations have been carried out for elliptic modular forms and now large databases exist of such forms [5, 35]. As a consequence of the modularity theorem of Wiles and others, these tables enumerate all isogeny classes of elliptic curves over $\mathbb{Q}$ up to a very large conductor. The algorithms employed to list such forms rely heavily on the formalism of modular symbols, introduced by Manin [26] and extensively developed by Cremona [4], Stein [34], and others. For a positive integer N, the space of modular symbols on $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ is defined to be the group $H^1_c(Y_0(N)(\mathbb{C}), \mathbb{C})$ of compactly supported cohomology classes on the open modular curve $Y_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H}$, where $\mathcal{H}$ denotes the upper half-plane. Let $S_2(\Gamma_0(N))$ denote the space of cuspidal modular forms for $\Gamma_0(N)$. By the Eichler-Shimura isomorphism, the space $S_2(\Gamma_0(N))$ embeds into $H^1_c(Y_0(N)(\mathbb{C}), \mathbb{C})$ and the image can be characterized by the action of the Hecke operators. In sum, to compute with the space of modular forms $S_2(\Gamma_0(N))$, one can equivalently compute with the space of modular symbols $H^1_c(Y_0(N)(\mathbb{C}), \mathbb{C})$ together with its Hecke action. This latter space is characterized by a natural isomorphism of Hecke modules

$$H^1_c(Y_0(N)(\mathbb{C}), \mathbb{C}) \cong \mathrm{Hom}_{\Gamma_0(N)}(\mathrm{Div}^0\, \mathbb{P}^1(\mathbb{Q}), \mathbb{C}),$$

where a cohomology class ω is mapped to the linear functional which sends the divisor $s - r \in \mathrm{Div}^0\, \mathbb{P}^1(\mathbb{Q})$ to the integral of ω over the image on $Y_0(N)$ of a path in $\mathcal{H}$ between the cusps r and s.

Modular symbols have proved to be crucial in both computational and theoretical roles. They arise in the study of special values of L-functions of classical modular forms, in the formulation of p-adic measures and p-adic L-functions, as well as in the conjectural constructions of Gross-Stark units [8] and Stark-Heegner points [7]. It is therefore quite inconvenient that a satisfactory formalism of modular symbols is absent in the context of automorphic forms on other Shimura varieties. Consequently, the corresponding theory is not as well understood. From this point of view, alternative methods for the explicit study of Hilbert modular forms are of particular interest.

Received by the editor April 24, 2009 and, in revised form, February 19, 2010.
2010 *Mathematics Subject Classification.* Primary 11F46 11G18.

Let F be a totally real field of degree $n = [F : \mathbb{Q}]$ and let $\mathbb{Z}_F$ denote its ring of integers. Let $S_2(\mathfrak{N})$ denote the Hecke module of (classical) Hilbert modular cusp forms over F of parallel weight 2 and level $\mathfrak{N} \subset \mathbb{Z}_F$. Dembélé [12] and Dembélé and Donnelly [13] have presented methods for computing with the space $S_2(\mathfrak{N})$ under the assumption that n is even. Their strategy is to apply the Jacquet-Langlands correspondence in order to identify systems of Hecke eigenvalues occurring in $S_2(\mathfrak{N})$ inside spaces of automorphic forms on $B^\times$, where B is the quaternion algebra over F ramified precisely at the infinite places of F, whence their assumption that n is even. In this way, Dembélé and his coauthors have convincingly demonstrated that automorphic forms on totally definite quaternion algebras, corresponding to Shimura varieties of dimension zero, are amenable to computation.

Here, we provide an algorithm which permits this computation when n is odd. We locate systems of Hecke eigenvalues in the (degree one) cohomology of a Shimura curve. We explain how a reduction theory for the associated quaternionic unit groups, arising from a presentation of a fundamental domain for the action of this group [38], allows us to compute the Hecke module structure of these cohomology groups in practice. Our methods work without reference to cusps or a canonical moduli interpretation of the Shimura curve, as these features of the classical situation are (in general) absent.

Our main result is as follows.

Theorem. *There exists an algorithm which, given a totally real field F of strict class number 1 and odd degree n, and an ideal $\mathfrak{N}$ of $\mathbb{Z}_F$, computes the system of Hecke eigenvalues associated to Hecke eigenforms in the space $S_2(\mathfrak{N})$ of Hilbert modular forms of parallel weight 2 and level $\mathfrak{N}$.*

In fact, our methods work more generally for fields F of even degree as well (under a hypothesis on $\mathfrak{N}$) and for higher weight k, and therefore overlap with the methods of Dembélé and his coauthors in many cases; see the precise statement in Theorem 3.10 below. This overlap follows from the Jacquet-Langlands correspondence, but it can also be explained by the theory of nonarchimedean uniformization of Shimura curves: one can describe the $\mathbb{C}_\mathfrak{p}$-points of a Shimura curve, for suitable primes $\mathfrak{p}$, as the quotient of the $\mathfrak{p}$-adic upper half-plane $\mathcal{H}_\mathfrak{p}$ by a definite quaternion order of the type considered by Dembélé. (For a discussion of the assumption on the class number of F, see Remark 3.11.) In particular, this theorem answers (in part) a challenge of Elkies [17] to compute modular forms on Shimura curves.

The article is organized as follows. In §§1 and 2, we introduce Hilbert modular forms (§1) and quaternionic modular forms (§2) and the correspondence of Jacquet-Langlands which relates them. In §3, we discuss how systems of Hecke eigenvalues associated to certain Hilbert or quaternionic modular forms may be found in cohomology groups of Shimura curves. The rest of the paper is devoted to explicit computation in these cohomology groups. In §4, we discuss algorithms for representing quaternion algebras and their orders. In §5, we show how the fundamental domain algorithms of the second author allow for computation in the cohomology of Fuchsian groups, and we show how algorithms for solving the word problem in these groups is the key to computing the Hecke action. We conclude by presenting applications and examples of our algorithms.

Beyond applications to the enumeration of automorphic forms, the techniques of this paper hold the promise of applications to Diophantine equations. The first author [19] has proposed a conjectural, p-adic construction of algebraic Stark-Heegner

points on elliptic curves over totally real fields. These points are associated to the data of an embedding of a non-CM quadratic extension K of a totally real field F into a quaternion F-algebra B. Note that such a quaternion algebra cannot be totally definite. We propose to generalize the formalism of overconvergent modular symbols employed in [9] in the case $B = \mathrm{M}_2(\mathbb{Q})$ to the general quaternionic situation in order to allow for the efficient calculation of these points.

1. Hilbert modular forms

We begin by defining the space of classical Hilbert modular cusp forms. Our main reference for standard facts about Hilbert forms is Freitag [18].

Let F be a totally real field of degree $n = [F : \mathbb{Q}]$ with ring of integers $\mathbb{Z}_F$. Throughout, we assume that the strict class number of F is equal to 1 (see Remark 3.11 for comments on this assumption). Let $v_1, \dots, v_n$ be the embeddings of F into $\mathbb{R}$. If $x \in F$, we write x_i to denote $v_i(x)$. Each embedding v_i induces an embedding $v_i : \mathrm{M}_2(F) \hookrightarrow \mathrm{M}_2(\mathbb{R})$. Extending our shorthand to matrices, if $\gamma \in \mathrm{M}_2(F)$ we write γ_i for $v_i(\gamma)$. Let

$$\mathrm{GL}_2^+(F) = \{\gamma \in \mathrm{GL}_2(F) : \det \gamma_i > 0 \text{ for all } i = 1, \dots, n\}.$$

The group $\mathrm{GL}_2^+(F)$ acts on the cartesian product $\mathcal{H}^n$ by the rule

$$\gamma(\tau_1, \dots, \tau_n) = (\gamma_1\tau_1, \dots, \gamma_n\tau_n)$$

where as usual $\mathrm{GL}_2^+(\mathbb{R})$ acts on $\mathcal{H}$ by linear fractional transformations.

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and $\tau \in \mathcal{H}$. We define

$$j(\gamma, \tau) = c\tau + d \in \mathbb{C}. \tag{1.1}$$

For a *weight*

$$k = (k_1, \dots, k_n) \in (2\mathbb{Z}_{>0})^n, \tag{1.2}$$

we define a right *weight k action* of $\mathrm{GL}_2^+(F)$ on the space of complex-valued functions on $\mathcal{H}^n$ by

$$(f \,|_k\, \gamma)(\tau) = f(\gamma\tau) \prod_{i=1}^{n} (\det \gamma_i)^{k_i/2} j(\gamma_i, \tau_i)^{-k_i}$$

for $f : \mathcal{H}^n \to \mathbb{C}$ and $\gamma \in \mathrm{GL}_2^+(F)$. The center $F^\times$ of $\mathrm{GL}_2^+(F)$ acts trivially on such f. Therefore, the weight k action descends to an action of $\mathrm{PGL}_2^+(F) = \mathrm{GL}_2^+(F)/F^\times$.

Now let $\mathfrak{N}$ be a (nonzero) ideal of $\mathbb{Z}_F$. Define

$$\Gamma_0(\mathfrak{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Z}_F) : c \in \mathfrak{N} \right\}.$$

A *Hilbert modular cusp form of weight k and level $\Gamma_0(\mathfrak{N})$* is an analytic function $f : \mathcal{H}^n \to \mathbb{C}$ such that $f \,|_k\, \gamma = f$ for all $\gamma \in \Gamma_0(\mathfrak{N})$ and such that f vanishes at the cusps of $\Gamma_0(\mathfrak{N})$. We write $S_k(\mathfrak{N}) = S_k(\Gamma_0(\mathfrak{N}))$ for the finite-dimensional $\mathbb{C}$-vector space of Hilbert modular forms of weight k and level $\Gamma_0(\mathfrak{N})$. (See Freitag [18, Chapter 1] for proofs and a more detailed exposition.)

The space $S_k(\mathfrak{N})$ is equipped with an action of Hecke operators as follows. Let $\mathfrak{p}$ be a (nonzero) prime ideal of $\mathbb{Z}_F$ with $\mathfrak{p} \nmid \mathfrak{N}$. Write $\mathbb{F}_\mathfrak{p}$ for the residue field of $\mathbb{Z}_F$ at $\mathfrak{p}$. By our assumption that F has strict class number one, there exists a totally

positive element $p \in \mathbb{Z}_F$ which generates the ideal $\mathfrak{p}$. Let $\pi = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. Then there are elements $\gamma_a \in \Gamma = \Gamma_0(\mathfrak{N})$, indexed by $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, such that

$$\Gamma\pi\Gamma = \bigsqcup_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} \Gamma\alpha_a, \tag{1.3}$$

where $\alpha_a = \pi\gamma_a$. If $f \in S_k(\mathfrak{N})$, we define

$$f \mid T_\mathfrak{p} = \sum_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} f \mid_k \alpha_a.$$

Then $f \mid T_\mathfrak{p}$ also belongs to $S_k(\mathfrak{N})$ and the operator $T_\mathfrak{p} : S_k(\mathfrak{N}) \to S_k(\mathfrak{N})$ is called the *Hecke operator* associated to the ideal $\mathfrak{p}$. One verifies directly that $T_\mathfrak{p}$ depends only on $\mathfrak{p}$ and not on our choice of generator p of $\mathfrak{p}$ or on our choice of representatives (1.3) for $\Gamma\backslash\Gamma\pi\Gamma$.

Suppose instead that now $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}_F$ such that $\mathfrak{p}^e \parallel \mathfrak{N}$. Let p and n be totally positive generators of $\mathfrak{p}$ and $\mathfrak{n}$, respectively. Then there exist $x, y \in \mathbb{Z}_F$ such that $xp^e - y(n/p^e) = 1$. The element

$$\pi = \begin{pmatrix} xp^e & y \\ n & p^e \end{pmatrix}$$

with $\det \pi = p^e$ normalizes Γ, and we have $\pi^2 \in F^\times\Gamma$. Setting

$$f \mid W_{\mathfrak{p}^e} = f \mid \pi,$$

we verify that $W_{\mathfrak{p}^e}$ is an involution of $S_2(\mathfrak{N})$, called an *Atkin-Lehner involution*, and this operator depends only on the prime power $\mathfrak{p}^e$ and not on its generator p or the elements x, y.

We conclude this section by defining the space of newforms. Let $\mathfrak{M}$ be an ideal of $\mathbb{Z}_F$ with $\mathfrak{M} \mid \mathfrak{N}$. For any totally positive element $d \mid \mathfrak{N}\mathfrak{M}^{-1}$ we have a map

$$\begin{aligned} h_d : S_k(\Gamma_0(\mathfrak{M})) &\hookrightarrow S_k(\mathfrak{N}) \\ f &\mapsto f \mid \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right). \end{aligned}$$

We say that $f \in S_k(\mathfrak{N})$ is an *oldform* at $\mathfrak{M}$ if f is in the image of h_d for some $d \mid \mathfrak{N}\mathfrak{M}^{-1}$. Let $S_k(\mathfrak{N})^{\mathfrak{M}\text{-old}}$ denote the space of oldforms at $\mathfrak{M}$. Then we can orthogonally decompose the space $S_k(\mathfrak{N})$ as

$$S_k(\mathfrak{N}) = S_k(\mathfrak{N})^{\mathfrak{M}\text{-old}} \oplus S_k(\mathfrak{N})^{\mathfrak{M}\text{-new}}$$

and we say that $f \in S_k(\mathfrak{N})$ is a *newform* at $\mathfrak{M}$ if $f \in S_k(\mathfrak{N})^{\mathfrak{M}\text{-new}}$.

2. Quaternionic modular forms

Our main reference for this section is Hida [23, §2.3]. Let B be a quaternion algebra over F which is split at the real place v_1 and ramified at the real places $v_2, \ldots, v_n$ (and possibly some finite places). Let $\mathfrak{D}$ be the *discriminant* of B, the product of the primes of $\mathbb{Z}_F$ at which B is ramified. Let $\omega(\mathfrak{D})$ denote the number of distinct primes dividing $\mathfrak{D}$. Then since a quaternion algebra is ramified at an even number of places, we have

$$\omega(\mathfrak{D}) \equiv n - 1 \pmod 2. \tag{2.1}$$

We note that the case $\mathfrak{D} = (1)$ is possible in (2.1) if and only if n is odd. For unity of presentation, we assume that $\omega(\mathfrak{D}) + n > 1$ or equivalently that $B \ncong \mathrm{M}_2(\mathbb{Q})$ or that B is a division algebra.

Since B is split at v_1, we may choose an embedding

$$\iota_1 : B \hookrightarrow B \otimes \mathbb{R} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{R}). \tag{2.2}$$

We denote by $\mathrm{nrd} : B \to F$ the *reduced norm* on B, defined by $\mathrm{nrd}(\gamma) = \gamma\overline{\gamma}$ where $\overline{\ } : B \to B$ is the unique *standard involution* (also called *conjugation*) on B. Let $B_+^\times$ denote the subgroup of $B^\times$ consisting of elements with totally positive reduced norm. Since B is ramified at all real places except v_1, an element $\gamma \in B^\times$ has totally positive norm if and only if $v_1(\mathrm{nrd}(\gamma)) > 0$, so that

$$B_+^\times = \{\gamma \in B^\times : v_1(\mathrm{nrd}\,\gamma) = \det \iota_1(\gamma) > 0\}. \tag{2.3}$$

The group $B_+^\times$ acts on $\mathcal{H}$ via v_1; we write simply γ_1 for $\iota_1(\gamma)$. As $F^\times \subset B_+^\times$ acts trivially on $\mathcal{H}$ via ι_1, the action of $B_+^\times$ on $\mathcal{H}$ descends to the quotient $B_+^\times/F^\times$.

For an integer $m \geq 0$, let $P_m = P_m(\mathbb{C})$ be the subspace of $\mathbb{C}[x, y]$ consisting of homogeneous polynomials of degree m. In particular, $P_0 = \mathbb{C}$. For $\gamma \in \mathrm{GL}_2(\mathbb{C})$, let $\bar{\gamma}$ be the adjoint of γ, so that $\gamma\bar{\gamma} = \det\gamma$. Note that this notation is consistent with the bar notation used for conjugation in a quaternion algebra as ι_1 is an isomorphism of algebras with involution: $\iota_1(\bar{\gamma}) = \overline{\iota_1(\gamma)}$. Define a right action of $\mathrm{GL}_2(\mathbb{C})$ on $P_m(\mathbb{C})$ by

$$(q \cdot \gamma)(x, y) = q((x\ y)\bar{\gamma}) = q(dx - cy, -bx + ay)$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$ and $q \in P_m(\mathbb{C})$. For $\ell \in \mathbb{Z}$, define a modified right action $\cdot_\ell$ of $\mathrm{GL}_2(\mathbb{C})$ on $P_m(\mathbb{C})$ by

$$q \cdot_\ell \gamma = (\det\gamma)^\ell\,(q \cdot \gamma).$$

We write $P_m(\ell)(\mathbb{C})$ for the resulting right $\mathrm{GL}_2(\mathbb{C})$-module.

Let k be a weight as in (1.2) and let $w_i = k_i - 2$ for $i = 2, \ldots, n$. Define the right $\mathrm{GL}_2(\mathbb{C})^{n-1}$-module

$$W(\mathbb{C}) = P_{w_2}(-w_2/2)(\mathbb{C}) \otimes \cdots \otimes P_{w_n}(-w_n/2)(\mathbb{C}). \tag{2.4}$$

For the ramified real places $v_2, \ldots, v_n$ of F, we choose splittings

$$\iota_i : B \hookrightarrow B \otimes_F \mathbb{C} \cong M_2(\mathbb{C}). \tag{2.5}$$

We abbreviate as above $\gamma_i = \iota_i(\gamma)$ for $\gamma \in B$. Then $W(\mathbb{C})$ becomes a right $B^\times$-module via $\gamma \mapsto (\gamma_2, \ldots, \gamma_n) \in \mathrm{GL}_2(\mathbb{C})^{n-1}$. We write $(x, \gamma) \mapsto x^\gamma$ for this action. We define a *weight k action* of $B_+^\times$ on the space of $W(\mathbb{C})$-valued functions on $\mathcal{H}$ by

$$(f\,|_k\,\gamma)(\tau) = (\det\gamma_1)^{k_1/2} j(\gamma_1, \tau)^{-k_1} f(\gamma_1\tau)^\gamma$$

for $f : \mathcal{H} \to W(\mathbb{C})$ and $\gamma \in B_+^\times$, where j is defined as in (1.1). Note that the center $F^\times \subset B_+^\times$ again acts trivially, so the action descends to $B_+^\times/F^\times$. We endow $W(\mathbb{C})$ with an analytic structure via a choice of the linear isomorphism $W(\mathbb{C}) \cong \mathbb{C}^{(k_2-1)\cdots(k_n-1)}$; the resulting analytic structure does not depend on this choice.

Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ which is prime to $\mathfrak{D}$ and let $\mathcal{O}_0(\mathfrak{N})$ be an Eichler order in B of level $\mathfrak{N}$. We denote by $\mathcal{O}_0(\mathfrak{N})_+^\times \subset B_+^\times$ the units of $\mathcal{O}_0(\mathfrak{N})$ with totally positive reduced norm, as in (2.3), and we let $\Gamma_0^{\mathfrak{D}}(\mathfrak{N}) = \mathcal{O}_0(\mathfrak{N})_+^\times/\mathbb{Z}_{F,+}^\times$, where $\mathbb{Z}_{F,+}^\times$ denotes the units of $\mathbb{Z}_F$ with totally positive norm. A *quaternionic modular form of weight k and level $\mathcal{O}_0(\mathfrak{N})$* is an analytic function $f : \mathcal{H} \to W(\mathbb{C})$ such that $f\,|_k\,\gamma = f$ for all $\gamma \in \mathcal{O}_0(\mathfrak{N})_+^\times$. We write $S_k^{\mathfrak{D}}(\mathfrak{N})$ for the finite-dimensional $\mathbb{C}$-vector space of quaternionic modular forms of weight k and level $\mathcal{O}_0(\mathfrak{N})$.

Spaces of quaternion modular forms can be equipped with the action of Hecke operators. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$ with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$. Since F has strict class

number 1, by strong approximation [37, Theorème III.4.3] there exists $\pi \in \mathcal{O}_0(\mathfrak{N})$ such that $\operatorname{nrd}\pi$ is a totally positive generator for the ideal $\mathfrak{p}$. It follows that there are elements $\gamma_a \in \Gamma = \Gamma_0(\mathfrak{N})$, indexed by $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, such that

$$\Gamma\pi\Gamma = \bigsqcup_{a\in\mathbb{P}^1(\mathbb{F}_\mathfrak{p})} \Gamma\alpha_a, \tag{2.6}$$

where $\alpha_a = \pi\gamma_a$. We define the *Hecke operator* $T_\mathfrak{p} : S_k(\mathfrak{N}) \to S_k(\mathfrak{N})$ by the rule

$$f \mid T_\mathfrak{p} = \sum_{a\in\mathbb{P}^1(\mathbb{F}_\mathfrak{p})} f \mid_k \alpha_a. \tag{2.7}$$

The space $S_k^\mathfrak{D}(\mathfrak{N})$ also admits an action of Atkin-Lehner operators. Now suppose that $\mathfrak{p}^e \subset \mathbb{Z}_F$ is a prime power with $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$. (Recall that $e = 1$ if $\mathfrak{p} \mid \mathfrak{D}$ and that $\mathfrak{D}$ and $\mathfrak{N}$ are coprime.) Then there exists an element $\pi \in \mathcal{O}_0(\mathfrak{N})$ whose reduced norm is a totally positive generator of $\mathfrak{p}^e$ and such that π generates the unique two-sided ideal of $\mathcal{O}_0(\mathfrak{N})$ with norm $\mathfrak{p}^e$. The element π normalizes $\mathcal{O}_0(\mathfrak{N})$ and $\pi^2 \in \mathcal{O}_0(\mathfrak{N}) \subset \mathcal{O}_0(\mathfrak{N})^\times F^\times$ (see Vignéras [37, Chapitre II, Corollaire 1.7] for the case $\mathfrak{p} \mid \mathfrak{D}$ and the paragraph following [37, Chapitre II, Lemme 2.4] if $\mathfrak{p} \mid \mathfrak{N}$). Thus, we define the *Atkin-Lehner involution* $W_{\mathfrak{p}^e} : S_k(\mathfrak{N}) \to S_k(\mathfrak{N})$ by

$$f \mid W_{\mathfrak{p}^e} = f \mid_k \pi \tag{2.8}$$

for $f \in S_k(\mathfrak{N})$. As above, this definition is independent of the choice of π and so only depends on the ideal $\mathfrak{p}^e$.

The following fundamental result, the Jacquet-Langlands correspondence, relates these two spaces of Hilbert and quaternionic modular forms.

Theorem 2.9. *There is a vector space isomorphism*

$$S_k^\mathfrak{D}(\mathfrak{N}) \xrightarrow{\sim} S_k(\mathfrak{D}\mathfrak{N})^{\mathfrak{D}\text{-}new}$$

which is equivariant for the actions of the Hecke operators $T_\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ and the Atkin-Lehner involutions $W_{\mathfrak{p}^e}$ with $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$.

A useful reference for the Jacquet-Langlands correspondence is Hida [20, Proposition 2.12], where Theorem 2.9 is deduced from the representation theoretic results of Jacquet-Langlands.

In particular, when $n = [F : \mathbb{Q}]$ is odd, we may take $\mathfrak{D} = (1)$ to obtain an isomorphism $S_k^{(1)}(\mathfrak{N}) \xrightarrow{\sim} S_k(\mathfrak{N})$.

3. Quaternionic modular forms and the cohomology of Shimura curves

In this section, we relate the spaces $S_k^\mathfrak{D}(\mathfrak{N})$ of quaternionic modular forms, together with their Hecke action, to the cohomology of Shimura curves. As above, let $\Gamma = \Gamma_0^\mathfrak{D}(\mathfrak{N}) = \mathcal{O}_0(\mathfrak{N})_+^\times/\mathbb{Z}_F^\times$. The action of Γ on $\mathcal{H}$ is properly discontinuous. Therefore, the quotient $\Gamma\backslash\mathcal{H}$ has a unique complex structure such that the natural projection $\mathcal{H} \to \Gamma\backslash\mathcal{H}$ is analytic. Since B is, by assumption, a division algebra, $\Gamma\backslash\mathcal{H}$ has the structure of a compact Riemann surface. By the theory of canonical models due to Shimura [31] and Deligne [10], this Riemann surface is the locus of complex points of the *Shimura curve* $X = X_0^\mathfrak{D}(\mathfrak{N})$ which is defined over F, under our assumption that F has strict class number 1.

Define the right $\mathrm{GL}_2(\mathbb{C})^n = \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})^{n-1}$-module

$$V(\mathbb{C}) = \bigotimes_{i=1}^{n} P_{w_i}(-w_i/2)(\mathbb{C}) = P_{w_1}(-w_1/2)(\mathbb{C}) \otimes W(\mathbb{C}).$$

The group $B^\times$ acts on $V(\mathbb{C})$ via the embedding $B^\times \hookrightarrow \mathrm{GL}_2(\mathbb{C})^n$ given by $\gamma \mapsto (\gamma_1, \dots, \gamma_n)$ arising from (2.2) and (2.5). As $F^\times$ acts trivially on $P_{w_1}(-w_1/2)(\mathbb{C})$ via ι_1 and on $W(\mathbb{C})$ via $(\iota_2, \dots, \iota_n)$, the action of $\mathcal{O}_0(\mathfrak{N})_+^\times \subset B^\times$ on $V(\mathbb{C})$ descends to a right action of Γ on $V(\mathbb{C})$.

It is convenient to identify $V(\mathbb{C})$ with the subspace of the algebra $\mathbb{C}[x_1, y_1, \dots, x_n, y_n]$ consisting of those polynomials q which are homogeneous in (x_i, y_i) of degree w_i. Under this identification, the action of $B^\times$ on $V(\mathbb{C})$ takes the form

$$q^\gamma(x_1, y_1, \dots, x_n, y_n) = \prod_{i=1}^{n} (\det \gamma_i)^{-w_i/2} q((x_1\ y_1)\bar{\gamma}_1, \dots (x_n\ y_n)\bar{\gamma}_n).$$

Let $V = V(\mathbb{C})$. We now consider the cohomology group $H^1(\Gamma, V)$. We represent elements of $H^1(\Gamma, V)$ by (equivalence classes of) crossed homomorphisms. Recall that a *crossed homomorphism* (or 1-*cocycle*) $f : \Gamma \to V$ is a map that satisfies the property

$$f(\gamma\delta) = f(\gamma)^\delta + f(\delta) \tag{3.1}$$

for all $\gamma, \delta \in \Gamma$. A crossed homomorphism f is *principal* (or a 1-*coboundary*) if there is an element $g \in V$ such that

$$f(\gamma) = g^\gamma - g \tag{3.2}$$

for all $\gamma \in \Gamma$. Let $Z^1(\Gamma, V)$ and $B^1(\Gamma, V)$ denote the spaces of crossed homomorphisms and principal crossed homomorphisms from Γ into V, respectively. Then

$$H^1(\Gamma, V) = Z^1(\Gamma, V)/B^1(\Gamma, V).$$

We now define (for a third time) the action of the Hecke operators, this time in cohomology. Let $f : \Gamma \to V$ be a crossed homomorphism, and let $\gamma \in \Gamma$. Recall the definition of Hecke operators (2.6)–(2.7). There are elements $\delta_a \in \Gamma$ for $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ and a unique permutation γ^* of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ such that

$$\alpha_a \gamma = \delta_a \alpha_{\gamma^* a} \tag{3.3}$$

for all a. Define $f \mid T_\mathfrak{p} : \Gamma \to V$ by

$$(f \mid T_\mathfrak{p})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} f(\delta_a)^{\alpha_a}. \tag{3.4}$$

It is a standard calculation [32, §8.3] that $f \mid T_\mathfrak{p}$ is a crossed homomorphism and that $T_\mathfrak{p}$ preserves 1-coboundaries. Moreover, $f \mid T_\mathfrak{p}$ does not depend on our choice of the coset representatives α_a. Therefore, $T_\mathfrak{p}$ yields a well-defined operator

$$T_\mathfrak{p} : H^1(\Gamma, V) \to H^1(\Gamma, V).$$

Remark 3.5. One may in a natural way extend this definition to compute the action of any Hecke operator $T_\mathfrak{a}$ for $\mathfrak{a} \subset \mathbb{Z}_F$ an ideal with $(\mathfrak{a}, \mathfrak{D}\mathfrak{N}) = 1$.

We now define an operator corresponding to complex conjugation. Let $\mu \in \mathcal{O}_0(\mathfrak{N})^\times$ be an element such that $v(\mathrm{nrd}\,\mu) < 0$; such an element exists again by

strong approximation. Then μ normalizes Γ and $\mu^2 \in \Gamma$. If $f \in Z^1(\Gamma, V)$, then the map $f \mid W_\infty$ defined by

$$(f \mid W_\infty)(\gamma) = f(\mu\gamma\mu^{-1})^\mu \tag{3.6}$$

is also a crossed homomorphism which is principal if f is principal, so it induces a linear operator

$$W_\infty : H^1(\Gamma, V) \to H^1(\Gamma, V).$$

Since $\mu^2 \in \Gamma$ and $\mathbb{Z}_{F,+}^*$ acts trivially on V, the endomorphism W_∞ has order two. Therefore, $H^1(\Gamma, V)$ decomposes into eigenspaces for W_∞ with eigenvalues $+1$ and -1, which we denote

$$H^1(\Gamma, V) = H^1(\Gamma, V)^+ \oplus H^1(\Gamma, V)^-.$$

It is not hard to see that $T_\mathfrak{p}$ commutes with W_∞. Therefore, $T_\mathfrak{p}$ perserves the $\pm$-eigenspaces of $H^1(\Gamma, V)$.

The group $H^1(\Gamma, V)$ also admits an action of Atkin-Lehner involutions. Letting $\mathfrak{p}$, e, and π be as in the definition of the Atkin-Lehner involutions (2.8) in §2, we define the involution $W_{\mathfrak{p}^e}$ on $H^1(\Gamma, V)$ by

$$(f \mid W_{\mathfrak{p}^e})(\gamma) = f(\pi\gamma\pi^{-1})^\pi. \tag{3.7}$$

We conclude this section by relating the space of quaternionic modular forms to cohomology using the *Eichler-Shimura isomorphism* (in analogy with the classical case $B = \mathrm{M}_2(\mathbb{Q})$ [32, §8.2]). We choose a base point $\tau \in \mathcal{H}$, and for $f \in S_k^\mathfrak{D}(\mathfrak{N})$ we define a map

$$\mathrm{ES}(f) : \Gamma \to V$$

by the rule

$$\mathrm{ES}(f)(\gamma) = \int_{\gamma_1^{-1}\tau}^{\tau} f(z)(zx_1 + y_1)^{w_1} dz \in V(\mathbb{C}).$$

A standard calculation [32, §8.2] shows that $\mathrm{ES}(f)$ is a crossed homomorphism which depends on the choice of base point τ only up to 1-coboundaries. Therefore, ES descends to a homomorphism

$$\mathrm{ES} : S_k(\Gamma) \to H^1(\Gamma, V).$$

Let

$$\mathrm{ES}^\pm : S_k(\Gamma) \to H^1(\Gamma, V)^\pm$$

be the composition of ES with projection to the $\pm$-subspace, respectively.

Theorem 3.8 ([27, §4])**.** *The maps $ES^\pm$ are isomorphisms (of $\mathbb{C}$-vector spaces) which are equivariant with respect to the action of the Hecke operators $T_\mathfrak{p}$ for $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ and $W_{\mathfrak{p}^e}$ for $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$.*

In sum, to compute the systems of Hecke eigenvalues occurring in spaces of Hilbert modular forms, combining the Jacquet-Langlands correspondence (Theorem 2.9) and the Eichler-Shimura isomorphism (Theorem 3.8), it suffices to enumerate those systems occurring in the Hecke module $H^1(\Gamma, V(\mathbb{C}))^+$.

Let $\mathfrak{N} \subset \mathbb{Z}_F$ be an ideal. Suppose that $\mathfrak{N}$ admits a factorization $\mathfrak{N} = \mathfrak{D}\mathfrak{M}$ such that

$$\mathfrak{D} \text{ is squarefree, } \mathfrak{D} \text{ is coprime to } \mathfrak{M}, \text{ and } \omega(\mathfrak{D}) \equiv n - 1 \pmod 2. \tag{3.9}$$

Then there is a quaternion F-algebra B ramified precisely at primes dividing $\mathfrak{D}$ and at the infinite places $v_2, \ldots, v_n$ of F. The goal of the second part of this paper

is to prove the following theorem which describes how spaces of automorphic forms discussed in the first part of this paper can be computed in practice.

Theorem 3.10. *There exists an explicit algorithm which, given a totally real field F of strict class number 1, an ideal $\mathfrak{N} \subset \mathbb{Z}_F$, a factorization $\mathfrak{N} = \mathfrak{D}\mathfrak{M}$ as in (3.9), and a weight $k \in (2\mathbb{Z}_{>0})^n$, computes the systems of eigenvalues for the Hecke operators $T_\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{M}$ and the Atkin-Lehner involutions $W_{\mathfrak{p}^e}$ with $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{M}$ which occur in the space of Hilbert modular cusp forms $S_k(\mathfrak{N})^{\mathfrak{D}\text{-}new}$.*

By this we mean that we will exhibit an explicit finite procedure which takes as input the field F, the ideals $\mathfrak{D}$ and $\mathfrak{M}$, and the integer k, and produces as output a set of sequences $(a_\mathfrak{p})_\mathfrak{p}$ with $a_\mathfrak{p} \in \overline{\mathbb{Q}}$ which are the Hecke eigenvalues of the finite set of $\mathfrak{D}$-newforms in $S_2(\mathfrak{N})$. The algorithm will produce the eigenvalues $a_\mathfrak{p}$ in any desired ordering of the primes $\mathfrak{p}$.

Remark 3.11. Generalizations of these techniques will apply when the strict class number of F is greater than 1. In this case, the canonical model X for the Shimura curve associated to B is the disjoint union of components defined over the strict class field of F and indexed by the strict ideal class group of $\mathbb{Z}_F$. The Hecke operators and Atkin-Lehner involutions then permute these components nontrivially and one must take account of this additional combinatorial data when doing computations. Because of this additional difficulty (see also Remark 5.4 below), we leave this natural extension as a future project.

We note, however, that it is a folklore conjecture that if one orders totally real fields by their discriminant, then a (substantial) positive proportion of fields will have strict class number 1. For this reason, we are content to consider a situation which is already quite common.

4. Algorithms for quaternion algebras

We refer to work of Kirschmer and the second author [25] as a reference for algorithms for quaternion algebras. We will follow the notation and conventions therein.

To even begin to work with the algorithm implied by Theorem 3.10 we must first find a representative quaternion algebra $B = \left(\frac{a,b}{F}\right)$ with discriminant $\mathfrak{D}$ which is ramified at all but one real place. From the point of view of effective computability, one can simply enumerate elements $a, b \in \mathbb{Z}_F \setminus \{0\}$ and then compute the discriminant of the corresponding algebra [40] until an appropriate representative is found. (Since such an algebra exists, this algorithm always terminates after a finite amount of time.) In practice, it is much more efficient to compute as follows.

Algorithm 4.1. *This algorithm takes as input a discriminant ideal $\mathfrak{D} \subset \mathbb{Z}_F$, the product of distinct prime ideals with $\omega(\mathfrak{D}) \equiv n - 1 \pmod 2$, and returns $a, b \in \mathbb{Z}_F$ such that the quaternion algebra $B = \left(\frac{a,b}{F}\right)$ has discriminant $\mathfrak{D}$.*

1. *Find $a \in \mathfrak{D}$ such that $v(a) > 0$ for at most one real place v_1 of F and such that $a\mathbb{Z}_F = \mathfrak{D}\mathfrak{b}$ with $\mathfrak{D} + \mathfrak{b} = \mathbb{Z}_F$ and $\mathfrak{b}$ odd.*

2. *Find* $t \in \mathbb{Z}_F/8a\mathbb{Z}_F$ *such that the following hold:*
   - *For all primes* $\mathfrak{p} \mid \mathfrak{D}$*, we have* $\left(\frac{t}{\mathfrak{p}}\right) = -1$*;*
   - *For all primes* $\mathfrak{q} \mid \mathfrak{b}$*, we have* $\left(\frac{t}{\mathfrak{q}}\right) = 1$*; and*
   - *For all prime powers* $\mathfrak{r}^e \parallel 8\mathbb{Z}_F$ *with* $\mathfrak{r} \nmid \mathfrak{D}$*, we have* $t \equiv 1 \pmod{\mathfrak{r}^e}$.
3. *Find* $m \in \mathbb{Z}_F$ *such that* $b = t + 8am \in \mathbb{Z}_F$ *is prime and such that* $v(b) < 0$ *for all* $v \neq v_1$ *and either* $v_1(a) > 0$ *or* $v_1(b) > 0$.

Since our theorem does not depend on the correctness of this algorithm, we leave it to the reader to verify that the algebra $B = \left(\frac{a,b}{F}\right)$ output by this algorithm has indeed the correct set of ramified places.

Remark 4.2. When possible, it is often helpful in practice to have $a\mathbb{Z}_F = \mathfrak{D}$, though this requires the computation of a generator for the ideal $\mathfrak{D}$ with the correct real signs; for example, if $\mathfrak{D} = \mathbb{Z}_F$ and there exists a unit $u \in \mathbb{Z}_F^\times$ such that $v(u) > 0$ for a unique real place $v = v_1$ and such that $u \equiv 1 \pmod 8$, then we may simply take $B = \left(\frac{-1,u}{F}\right)$.

One may wish to alternate between Steps 2 and 3 in searching for b. Finally, we note that in Step 2 one may find the element t by either deterministic or probabilistic means.

Given this representative algebra B, there are algorithms [40] to compute a maximal order $\mathcal{O} \subset B$, which is represented in bits by a pseudobasis. Furthermore, given a prime $\mathfrak{p} \nmid \mathfrak{D}$ there exists an algorithm to compute an embedding $\iota_\mathfrak{p} : \mathcal{O} \hookrightarrow \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$ where $\mathbb{Z}_{F,\mathfrak{p}}$ denotes the completion of F at $\mathfrak{p}$. As a consequence, one can compute an Eichler order $\mathcal{O}_0(\mathfrak{N}) \subset \mathcal{O}$ for any level $\mathfrak{N} \subset \mathbb{Z}_F$.

5. Computing in the cohomology of a Shimura curve

In this section, we show how to compute explicitly in the first cohomology group of a Shimura curve, equipped with its Hecke module structure. Throughout, we abbreviate $\Gamma = \Gamma_0^\mathfrak{D}(\mathfrak{N})$ and $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$ as above.

In the choices of embeddings $\iota_1, \dots, \iota_n$ in (2.3) and (2.5), we may assume, without loss of generality, that their image is contained in $\mathrm{M}_2(K)$ with $K \hookrightarrow \mathbb{C}$ a number field containing F; in other words, we may take K to be any Galois number field containing F which splits B. In particular, we note then that the image of $\iota_1(B)$ is contained in $K \cap \mathbb{R}$. So throughout, we may work with the coefficient module

$$V(K) = \bigotimes_{i=1}^{n} P_{w_i}(K)(-w_i/2)$$

since obviously $V(K) \otimes_K \mathbb{C} = V(\mathbb{C})$. The K-vector space $V(K)$ is then equipped with an action of Γ via ι which can be represented using exact arithmetic over K.

Remark 5.1. In fact, one can take the image of ι to be contained in $\mathrm{M}_2(\mathbb{Z}_K)$ for an appropriate choice of K, where $\mathbb{Z}_K$ denotes the ring of integers of K. Therefore, one could alternatively work with $V(\mathbb{Z}_K)$ as a $\mathbb{Z}_K$-module and thereby recover from this integral stucture more information about the structure of this module. In the case where $k = (2, 2, \dots, 2)$, we may work already with the coefficient module $\mathbb{Z}$, and we do so in Algorithm 5.9 below.

The first main ingredient we will use is an algorithm of the second author [38].

Proposition 5.2. *There exists an algorithm which, given Γ, returns a finite presentation for Γ with a minimal set of generators and a solution to the word problem for the computed presentation.*

Remark 5.3. One must choose a point $p \in \mathcal{H}$ with trivial stabilizer $\Gamma_p = \{1\}$ in the above algorithm, but a random choice of a point in any compact domain will have trivial stabilizer with probability 1. The algorithm also yields a fundmental domain $\mathcal{F}$ for Γ which is, in fact, a hyperbolic polygon. For each element γ of our minimal set of generators, $\mathcal{F}$ and $\gamma\mathcal{F}$ share a single side. In other words, there is a unique side s of $\mathcal{F}$ such that γs is also a side of $\mathcal{F}$. We say that γ is a *side pairing element* for s and γs.

Remark 5.4. The algorithms of the second author [38] concern the computation of a fundamental domain for $\mathcal{O}_1^\times/\{\pm 1\}$ acting on $\mathcal{H}$, where $\mathcal{O}_1^\times$ denotes the subgroup of $\mathcal{O}^\times$ consisting of elements of reduced norm 1. Since we have assumed that F has strict class number 1, the natural inclusion $\mathcal{O}_1^\times \hookrightarrow \mathcal{O}_+^\times$ induces an isomorphism

$$\mathcal{O}_1^\times/\{\pm 1\} \xrightarrow{\sim} \mathcal{O}_+^\times/\mathbb{Z}_F^\times = \Gamma.$$

Indeed, if $\gamma \in \mathcal{O}_0(\mathfrak{N})_+^\times$, then $\operatorname{nrd}\gamma \in \mathbb{Z}_{F,+}^\times = \mathbb{Z}_F^{\times 2}$ so if $\operatorname{nrd}\gamma = u^2$, then γ/u maps to γ in the above map.

Let G denote a set of generators for Γ and R a set of relations in the generators G, computed as in Proposition 5.2. We identify $Z^1(\Gamma, V(K))$ with its image under the inclusion

$$\begin{aligned} j_G : Z^1(\Gamma, V(K)) &\to \bigoplus_{g\in G} V(K) \\ f &\mapsto (f(g))_{g\in G}. \end{aligned}$$

It follows that $Z^1(\Gamma, V(K))$ consists of those $f \in \bigoplus_{g\in G} V(K)$ which satisfy $f(r) = 0$ for $r \in R$; these become linear relations written out using the crossed homomorphism property (3.1), and so an explicit K-basis for $Z^1(\Gamma, V(K))$ can be computed using linear algebra. The space of principal crossed homomorphisms (3.2) is obtained similarly, where a basis is obtained from any basis for $V(K)$. We obtain from this a K-basis for the quotient

$$H^1(\Gamma, V(K)) = Z^1(\Gamma, V(K))/B^1(\Gamma, V(K))$$

and an explicit K-linear map $Z^1(\Gamma, V(K)) \to H^1(\Gamma, V(K))$.

We first decompose the space $H^1(\Gamma, V(K))$ into $\pm$-eigenspaces for complex conjugation W_∞ as in (3.6). An element $\mu \in \mathcal{O}^\times$ with $v_1(\operatorname{nrd}(\mu)) < 0$ can be found simply by enumeration of elements in $\mathcal{O}$. Given such an element μ, we can then find a K-basis for the subspace $H^1(\Gamma, V(K))^+$ by linear algebra.

Remark 5.5. This exhaustive search in practice benefits substantially from the methods of Kirschmer and the second author [25] using the absolute reduced norm on $\mathcal{O}$, which gives the structure of a lattice on $\mathcal{O}$ so that an LLL-lattice reduction can be performed.

Next, we compute explicitly the action of the Hecke operators on the K-vector space $H^1(\Gamma, V)^+$. Let $\mathfrak{p} \subset \mathbb{Z}_F$ be an ideal with $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ and let $\pi \in \mathcal{O}$ be such that $\operatorname{nrd}\pi$ is a totally positive generator of $\mathfrak{p}$. We need to compute explicitly a coset

decomposition as in (2.6). Now the set $\mathcal{O}(\mathfrak{p}) = \mathcal{O}^\times \pi \mathcal{O}^\times$ is in natural bijection with the set of elements whose reduced norm generates $\mathfrak{p}$; associating to such an element the left ideal that it generates gives a bijection between the set $\mathcal{O}^\times \backslash \mathcal{O}(\mathfrak{p})$ and the set of left ideals of reduced norm $\mathfrak{p}$, and in particular shows that the decomposition (2.6) is independent of π. But this set of left ideals in turn is in bijection [25, Lemma 6.2] with the set $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$: explicitly, given a splitting $\iota_\mathfrak{p} : \mathcal{O} \hookrightarrow \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$, the left ideal corresponding to a point $a = (x : y) \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is

$$I_a := \mathcal{O}\iota_\mathfrak{p}^{-1} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \mathcal{O}\mathfrak{p}. \tag{5.6}$$

For $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, we let $\alpha_a \in \mathcal{O}$ be such that $\mathcal{O}\alpha_a = I_a$ and $\operatorname{nrd} \alpha_a = \operatorname{nrd} \pi$. We have shown that

$$\mathcal{O}(\mathfrak{p}) = \mathcal{O}^\times \pi \mathcal{O}^\times = \bigsqcup_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} \mathcal{O}^\times \alpha_a.$$

To compute the α_a, we use the following proposition [25].

Proposition 5.7. *There exists an (explicit) algorithm which, given a left $\mathcal{O}$-ideal I, returns $\alpha \in \mathcal{O}$ such that $\mathcal{O}\alpha = I$.*

If $v_1(\operatorname{nrd} \alpha_a)$ happens to be negative, then replace α_a by $\mu\alpha_a$. An intersection with $\mathcal{O}_+^\times$ then yields the decomposition (2.6).

Next, in order to use equation (3.4) to compute $(f \mid T_\mathfrak{p})(\gamma)$ for all $\gamma \in G$, we need to compute the permutations $a \mapsto \gamma^* a$ of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p}) = \mathbb{F}_\mathfrak{p} \cup \{\infty\}$.

Algorithm 5.8. *Given $\gamma \in \Gamma$, this algorithm returns the permutation $a \mapsto \gamma^* a$.*

1. *Let $\beta = \iota_\mathfrak{p}(\alpha_a \gamma) \in \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$ and let β_{ij} denote the ijth entry of β for $i, j = 1, 2$.*
2. *If $\operatorname{ord}_\mathfrak{p}(\beta_{11}) \leq 0$, then return $\beta_{12}/\beta_{11} \bmod \mathfrak{p}$.*
3. *If $\operatorname{ord}_\mathfrak{p}(\beta_{12}) = 0$ or $\operatorname{ord}_\mathfrak{p}(\beta_{21}) > 0$, then return ∞.*
4. *Otherwise, return $\beta_{22}/\beta_{21} \bmod \mathfrak{p}$.*

The proof that this algorithm gives correct output is straightforward.

Having computed the permutation γ^*, for each $a \in \mathbb{P}^1(\mathbb{F}_p)$ we compute $\delta_a = \alpha_a \gamma \alpha_{\gamma^* a}^{-1} \in \Gamma$ as in (3.3). By Proposition 5.2, we can write δ_a as a word in the generators G for Γ, and using the crossed homomorphism property (3.1) for each $f \in Z^1(\Gamma, V(K))^+$ we compute $f \mid T_\mathfrak{p} \in Z^1(\Gamma, V(K))^+$ by computing $(f \mid T_\mathfrak{p})(\gamma) \in V(K)$ for $\gamma \in G$.

Finally, we compute the Atkin-Lehner involutions $W_{\mathfrak{p}^e}$ for $\mathfrak{p}^e \parallel \mathfrak{D}\mathfrak{N}$ as in (3.7). We compute an element $\pi \in \mathcal{O}$ with totally positive reduced norm such that π generates the unique two-sided ideal I of $\mathcal{O}_0(\mathfrak{N})$ of norm $\mathfrak{p}^e$. The ideal I can be computed easily [25], and a generator π can be computed again using Proposition 5.7.

We then decompose the space $H^1(\Gamma, V(K))$ under the action of the Hecke operators into Hecke irreducible subspaces for each operator $T_\mathfrak{p}$, and from this we compute the systems of Hecke eigenvalues using straightforward linear algebra over K. (Very often it turns out in practice that a single operator $T_\mathfrak{p}$ is enough to break up the space into Hecke irreducible subspaces.)

For concreteness, we summarize the algorithm in the simplest case of parallel weight $k = (2, 2, \ldots, 2)$. Here, we may work more simply with the coefficient module $\mathbb{Q}$ (or $\mathbb{Z}$), since the Γ-action is trivial. Moreover, the output of the computation of a fundamental domain provided by Proposition 5.2 is a minimal set of generators and relations with the following properties [38, §5]: each generator $g \in G$ is labelled either elliptic or hyperbolic, and each relation becomes trivial in the free abelian quotient.

Algorithm 5.9. *Let $\mathfrak{p} \subset \mathbb{Z}_F$ be coprime to $\mathfrak{D}$. This algorithm computes the matrix of the Hecke operator $T_\mathfrak{p}$ acting on $H^1(\Gamma, \mathbb{Z})^+$.*

1. *Compute a minimal set of generators for Γ using Proposition 5.2, and let G denote the set of nonelliptic generators. Let $H = \bigoplus_{\gamma \in G} \mathbb{Z}\gamma$.*
2. *Compute an element μ as in (3.6) and decompose H into $\pm$-eigenspaces $H^\pm$ for W_∞.*
3. *Compute α_a for $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ as in (3.3) by Proposition 5.7.*
4. *For each $\gamma \in G$, compute the permutation γ^* of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ using Algorithm 5.8.*
5. *Initialize T to be the zero matrix acting on H, with rows and columns indexed by G.*
6. *For each $\gamma \in G$ and each $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, let $\delta_a := \alpha_a \gamma \alpha_{\gamma^*(a)}^{-1} \in \Gamma$. Write δ_a as a word in G using Proposition 5.2, and add to the column indexed by γ the image of $\delta_a \in H$.*
7. *Compute the action T^+ of the matrix T on H^+ and return T^+.*

We note that Step 1 is performed as a precomputation step as it does not depend on the ideal $\mathfrak{p}$.

6. Higher level and relation to homology

In this section, we consider two topics which may be skipped on a first reading. The first considers a simplification if one fixes the quaternion algebra and varies the level $\mathfrak{N}$. The second considers the relationship between our cohomological method and the well-known method of modular symbols.

Higher level. Let $\mathcal{O}(1)$ be a maximal order of B which contains $\mathcal{O}_0(\mathfrak{N})$ and let $\Gamma(1) = \mathcal{O}(1)_+^\times / \mathbb{Z}_F^\times$. From Shapiro's lemma, we have an isomorphism

$$H^1(\Gamma(1), \mathrm{Coind}_\Gamma^{\Gamma(1)} V(K) \cong H^1(\Gamma, V(K))$$

for any $K[\Gamma]$-module V where $\mathrm{Coind}_\Gamma^{\Gamma(1)} V$ denotes the coinduced module V from Γ to $\Gamma(1)$. In particular, if one fixes $\mathfrak{D}$ and wishes to compute systems of Hecke eigenvalues for varying level $\mathfrak{N}$, one can vary the coefficient module instead of the group and so the fundamental domain algorithm need only be called once to compute a presentation for $\Gamma(1)$.

To compute the action of $\Gamma(1)$ on the coinduced module, we first need to enumerate the set of cosets $\Gamma\backslash\Gamma(1)$. We use a set of side pairing elements [38] for $\Gamma(1)$, which are computed as part of the algorithm to compute a presentation for Γ. (Side pairing elements are defined in Remark 5.3.)

Algorithm 6.1. *Let $\mathfrak{N}$ be a level and let G be a set of side pairing elements for $\Gamma(1)$. This algorithm computes representatives $\alpha \in \Gamma(1)$ such that $\Gamma\backslash\Gamma(1) = \bigsqcup \Gamma\alpha$.*

1. *Initialize $\mathcal{F} := \{1\}$ and $A := \{\}$. Let $G^{\pm} := G \cup G^{-1}$.*
2. *Let*

$$\mathcal{F} := \{g\gamma : g \in G,\ \gamma \in \mathcal{F},\ g\gamma\alpha^{-1} \notin \Gamma \text{ for all } \alpha \in A\}$$

and let $A := A \cup \mathcal{F}$. If $\mathcal{F} = \emptyset$, then return A; else, return to Step 2.

Proof of correctness. Consider the (left) Cayley graph of Γ on the set $G^{\pm}$; this is the graph with vertices indexed by the elements of Γ and directed edges $\gamma \to \delta$ if $\delta = g\gamma$ for some $g \in G^{\pm}$. Then the set $\Gamma\backslash\Gamma(1)$ is in bijection with the set of vertices of this graph under the relation which identifies two vertices if they are in the same coset modulo Γ. Since the set $G^{\pm}$ generates Γ, this graph is connected and Step 2 is simply an algorithmic way to traverse the finite quotient graph. □

Remark 6.2. Although it is tempting to try to obtain a set of generators for Γ from the above algorithm, we note that a presentation for Γ may be arbitrarily more complicated than that of $\Gamma(1)$ and may require many more elements than the number of cosets (due to the presence of elliptic elements). For this reason, it is more efficient to work with the induced module than to compute separately a fundamental domain for Γ.

To compute the Hecke operators as in §5 using this simplification, the same analysis applies and the only modification required is to ensure that the elements α_a arising in (3.3) satisfy $\lambda_a \in \mathcal{O}_0(\mathfrak{N})$; this can be obtained by simply multiplying by the appropriate element $\alpha \in \Gamma\backslash\Gamma(1)$, and in order to do this efficiently one can use a simple table lookup.

Homology. We now relate the cohomological approach taken above to the method using homology. Although the relationship between these two approaches is intuitively clear as the two spaces are dual, this alternative perspective also provides a link to the theory of modular symbols, which we briefly review now. Let $S_2(N)$ denote the $\mathbb{C}$-vector space of classical modular cusp forms of level N and weight 2. Integration defines a nondegenerate Hecke-equivariant pairing between $S_2(N)$ and the homology group $H_1(X_0(N), \mathbb{Z})$ of the modular curve $X_0(N)$. Let $\mathcal{S}_2(N)$ denote the space of cuspidal modular symbols, i.e., the linear combination of paths in the completed upper half-plane $\mathcal{H}^*$ whose endpoints are cusps and whose images in $X_0(N)$ are a linear combination of loops. Manin showed that there is a canonical isomorphism

$$\mathcal{S}_2(N) \cong H_1(X_0(N), \mathbb{Z}).$$

If $SL_2(\mathbb{Z}) = \bigsqcup_i \Gamma_0(N)\gamma_i$, then the set of symbols $\gamma_i\{0, \infty\} = \{\gamma_i(0), \gamma_i(\infty)\}$ generate the space $\mathcal{S}_2(N)$. We have an explicit description of the action of the Hecke operators on the space $\mathcal{S}_2(N)$, and the *Manin trick* provides an algorithm for writing an arbitrary modular symbol as a $\mathbb{Z}$-linear combination of the symbols $\gamma_i\{0, \infty\}$.

The Shimura curves $X = X_0^{\mathfrak{D}}(\mathfrak{N})$ do not have cusps, and so this method does not generalize directly. Consider instead the sides of a fundamental domain D for

$\Gamma = \Gamma_0^{\mathfrak{D}}(\mathfrak{N})$, and let G be the corresponding set of side pairing elements and R the set of minimal relations among them [38]. The side pairing gives an explicit characterization of the gluing relations which describe X as a Riemann surface, hence one obtains a complete description for the homology group $H_1(X, \mathbb{Z})$. Let V be the set of midpoints of sides of D. Then for each $v \in V$, there is a unique $\gamma \in G$ such that $w = \gamma v \in V$, and the path from v to γv in $\mathcal{H}$, which we denote by $p(\gamma) = \{v, \gamma v\}$, projects to a loop on X. Each relation $r = \gamma_1\gamma_2 \cdots \gamma_t = 1$ from R induces the relation in the homology group $H_1(X, \mathbb{Z})$:

$$\begin{aligned} 0 &= p(1) = p(\gamma_1 \cdots \gamma_t) \\ &= \{v, \gamma_1 v\} + \{\gamma_1 v, \gamma_1\gamma_2 v\} + \cdots + \{\gamma_1 \cdots \gamma_{t-1} v, \gamma_1 \cdots \gamma_{t-1}\gamma_t v\} \\ &= \{v, \gamma_1 v\} + \{v, \gamma_2 v\} + \cdots + \{v, \gamma_t v\} = p(\gamma_1) + p(\gamma_2) + \cdots + p(\gamma_t). \end{aligned} \tag{6.3}$$

In particular, if $\gamma \in G$ is an elliptic element, then $p(\gamma) = 0$ in $H^1(X, \mathbb{Q})$. Let $\mathcal{S}_2^{\mathfrak{D}}(\mathfrak{N})$ be the $\mathbb{Q}$-vector space generated by $p(\gamma)$ for $\gamma \in G$ modulo the relations (6.3) with $r \in R$. It follows that

$$H_1(X, \mathbb{Q}) \cong H_1(\Gamma, \mathbb{Q}) \cong \mathcal{S}_2^{\mathfrak{D}}(\mathfrak{N})$$

and we call $\mathcal{S}_2^{\mathfrak{D}}(\mathfrak{N})$ the space of *Dirichlet-modular symbols* for X (relative to D).

The Hecke operators act in an analogous way, as follows. If α_a for $a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ is a set of representatives as in (3.3), then α_a acts on the path $p(\gamma) = \{v, \gamma v\}$ by $\alpha_a\{v, \gamma v\} = \{\alpha_a v, \alpha_a\gamma v\}$; if $\alpha_a\gamma = \delta_a\alpha_{\gamma^* a} = \delta_a\alpha_b$ as before, then in homology we obtain

$$\begin{aligned} \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} \{\alpha_a v, \alpha_a\gamma v\} &= \sum_a \{\alpha_a v, \delta_a\alpha_b v\} = \sum_a \left(\{\alpha_a v, v\} + \{v, \delta_a v\} + \{\delta_a v, \delta_a\alpha_b v\}\right) \\ &= \sum_a \{v, \delta_a v\} + \sum_a \left(\{\alpha_a v, v\} + \delta_a\{v, \alpha_b v\}\right) \\ &= \sum_a \{v, \delta_a v\} + \sum_a \left(-\{v, \alpha_a v\} + \{v, \alpha_b v\}\right) = \sum_a \{v, \delta_a v\}. \end{aligned}$$

Thus, the action of the Hecke operators indeed agrees with that in cohomology, and so one could also rephrase our methods in terms of Dirichlet-modular symbols.

The analogue of the Manin trick in our context is played by the solution to the word problem in Γ. When $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, the Manin trick arises directly from the Euclidean algorithm; therefore, our methods may be seen in this light as a generalization of the Euclidean algorithm to the group Γ. Already this point of view has been taken by Cremona [3] and his students, who generalized methods of modular symbols to the case of $SL_2(\mathbb{Z}_K)$ for K an imaginary quadratic field. We point out that idea analogy between fundamental domain algorithms for Fuchsian groups and continued fraction algorithms goes back at least to Eichler [16]. It seems likely therefore that many other results which follow from the theory of modular symbols should hold in the context of Shimura curves and Hilbert modular varieties as well.

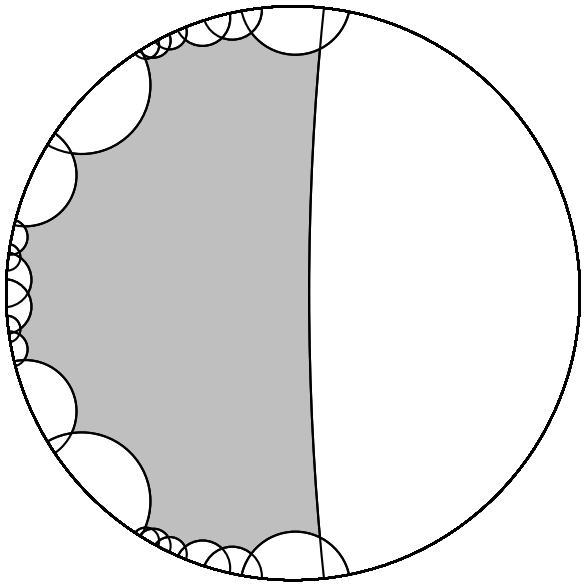

FIGURE 7.1: A fundamental domain for $X(1)$ for $d_F = 1101$

7. Cubic fields

In this section, we tabulate some examples computed with the algorithms illustrated above. We perform our calculations in Magma [1].

First example. We first consider the cubic field F with $d_F = 1101 = 3 \cdot 367$ and primitive element w satisfying $w^3 - w^2 - 9w + 12 = 0$. The field F has Galois group S_3 and strict class number 1. The Shimura curve $X(1) = X_0^{(1)}(1)$ associated to F has signature $(1; 2^2, 3^5)$; according to tables of the second author [39], this is the cubic field of strict class number 1 with smallest discriminant such that the corresponding Shimura curve has genus ≥ 1.

We first compute the representative quaternion algebra

$$B = \left(\frac{-1, -w^2 + w + 1}{F}\right)$$

with discriminant $\mathfrak{D} = (1)$ and a maximal order $\mathcal{O}$, generated as a $\mathbb{Z}_F$-algebra by α and the element

$$\frac{1}{4}\big((-8w + 14) + (-2w + 4)\alpha + (-w + 2)\beta\big).$$

We then compute a fundamental domain for $\Gamma(1) = \Gamma_0^{(1)}(1)$, shown in Figure 7.1.

We may take $\mu = \beta$ as an element to represent complex conjugation; indeed, $\beta^2 = -w^2 + w + 1 \in \mathbb{Z}_F^*$ is a unit. Since the spaces $H^1(\Gamma, \mathbb{Z})^{\pm}$ are one-dimensional, the Hecke operators $T_{\mathfrak{p}}$ act by scalar multiplication, and the eigenvalues are listed in Table 7.2: for each prime $\mathfrak{p}$ of $\mathbb{Z}_F$ with $N(\mathfrak{p}) < 50$, we list a generator π of $\mathfrak{p}$ and the eigenvalue $a(\mathfrak{p})$ of $T_{\mathfrak{p}}$.

TABLE 7.2: Hecke eigenvalues for the group $\Gamma(1)$ for $d_F = 1101$

$N\mathfrak{p}$	π	$a(\mathfrak{p})$	$\#E(\mathbb{F}_\mathfrak{p})$
2	$w-2$	0	3
3	$w-3$	-3	7
3	$w-1$	-1	5
4	w^2+w-7	-3	8
19	$w+1$	-6	26
23	w^2-2w-1	6	18
31	$2w^2-19$	3	29
31	w^2-5	0	32
31	$3w-5$	4	28
41	w^2+2w-7	0	42
43	w^2-11	9	35
47	$3w-7$	-9	57

The curve $X(1)$ has modular Jacobian E and we have $\#E(\mathbb{F}_\mathfrak{p}) = N\mathfrak{p}+1-a(\mathfrak{p})$, so we list these values in Table 7.2 as well. By the reduction theory of Carayol [2], we know that E is an elliptic curve over F with everywhere good reduction. (Compare this result with calculations of Dembélé and Donnelly [13].) We note that since the $a(\mathfrak{p})$ for the primes $\mathfrak{p}$ with $N\mathfrak{p} = 31$ are not equal, the curve E does not arise as the base change of a curve defined over $\mathbb{Q}$.

To find a candidate curve E, we begin by searching for a curve over F with everywhere good reduction. We follow the methods of Cremona and Lingham [6].

Remark 7.1. One possible alternative approach to find an equation for the curve E would be to use the data computed above to give congruence conditions on a minimal Weierstrass model for E,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^4 + a_6$$

with $a_i \in \mathbb{Z}_F$. For example, by a coordinate change for y, without loss of generality, we may assume that a_1, a_3 are chosen from representatives of the set $\mathbb{Z}_F/2\mathbb{Z}_F$, and since the reduction of E modulo the prime $\mathfrak{p}$ with $N\mathfrak{p} = 2$ is supersingular, and a Weierstrass model for such a curve is of the form $y^2 + y = f(x)$, we may assume that $a_1 \equiv 0 \pmod{w-2}$ and $a_3 \equiv 1 \pmod{w-2}$, leaving 4 possibilities each for a_1, a_3. In a similar way, we obtain further congruences. In our case, this approach fails to find a model, but we expect it will be useful in many cases.

Remark 7.2. When F is a real quadratic field, there are methods of Dembélé [11] which apply to find an equation for the curve E by computing the real periods of E.

In our situation, where F has (strict) class number 1, we conclude (see Cremona and Lingman [6, Propositions 3.2–3.3]) that there exists $w \in \mathbb{Z}_F^*/\mathbb{Z}_F^{*6}$ and an integral point on the elliptic curve $E_w : y^2 = x^3 - 1728w$ such that E has j-invariant $j = x^3/w = 1728 + y^2/w$. In our situation, we need not provably enumerate all such curves and we are content to find as many such integral points as we can. Indeed, we find for the unit $w = -1506w^2 + 6150w - 5651 \in \mathbb{Z}_F^*$ that the curve E_w has rank 3 and we find an integral point

$$(-11w^2 - 24w + 144, -445w^2 + 1245w - 132) \in E_w(F);$$

this point corresponds to a curve with j-invariant

$$(-2w^2-4w+7)^9(2w^2+w-17)^3(w-2)^{18}(w-3)^6 = -1805w^2-867w+14820$$

where we note that the first two terms are units and recall that $N(w-2)=2$, $N(w-3)=-3$. We then find an appropriate quadratic twist of this curve which has conductor $(1)=\mathbb{Z}_F$ as follows:

$$A : y^2+w(w+1)xy+(w+1)y = x^3+w^2x^2+a_4x+a_6$$

where

$$a_4 = -13967140935029686 4w^2 - 23568148183993846 8w + 623672370161912822$$

and

$$\begin{aligned} a_6 = {} & 1107260540564019301821064 63w^2 + 1868390950879773446683567 26w \\ & - 4944231842528186971355327 43. \end{aligned}$$

We verify that $\#A(\mathbb{F}_\mathfrak{p}) = N(\mathfrak{p})+1-a(\mathfrak{p})$ in agreement with the above table, so this strongly suggests that the Jacobian $E=J(1)$ of $X(1)$ is isogenous to A (and probably isomorphic to A).

To prove that, in fact, E is isogeneous to A, we use the method of Faltings and Serre. (For an exposition of this method, see Schütt [29, §5] and Dieulefait, Guerberoff, and Pacetti [14, §4], and the references contained therein.)

Let $\rho_E, \rho_A : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{Z}_2)$ be the 2-adic Galois representations associated to the 2-adic Tate modules of E and A, respectively, and let $\overline{\rho}_E, \overline{\rho}_A : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{F}_2)$ be their reductions modulo 2. We will show that we have an isomorphism $\overline{\rho}_E \cong \overline{\rho}_A$ of absolutely irreducible representations and then lift this to an isomorphism $\rho_E \cong \rho_A$ by comparing traces of ρ_E and ρ_A. It then follows from work of Faltings that E is isogeneous to A.

First we show that the representations $\overline{\rho}_E$ and $\overline{\rho}_A$ are absolutely irreducible and isomorphic. (It is automatic that they have the same determinant, the cyclotomic character.) For E, it is clear from Table 7.2 that the image of $\overline{\rho}_E$ contains elements of both even and odd order and so must be all of the group $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. For A, we verify that the 2-division polynomial is irreducible, and adjoining a root of this polynomial to F we obtain a field which is more simply given by the polynomial

$$x^3+(w+1)x^2+(w^2+w-5)x+(w^2+w-7)$$

and with relative discriminant $4\mathbb{Z}_F$; the splitting field L of this polynomial indeed has Galois group isomorphic to S_3.

At the same time, the field cut out by $\overline{\rho}_E$ is an S_3-extension of F which is unramified away from 2. We may enumerate all such fields using class field theory, as follows. Any such extension has a unique quadratic subextension which is also unramified away from 2 and by Kummer theory is given by adjoining the square root of a 2-unit $\alpha \in \mathbb{Z}_F$. Since $2\mathbb{Z}_F = \mathfrak{p}_2\mathfrak{p}_2'$ with $\mathfrak{p}_2 = (w-2)\mathbb{Z}_F$, $\mathfrak{p}_2' = (w^2+w-7)\mathbb{Z}_F$ (of inertial degrees $1,2$, respectively), we see that there are $31 = 2^{3+2}-1$ possibilities for α. Now for each quadratic extension K, we look for a cyclic cubic extension which is unramified away from 2 and which generates a Galois field over F. By class field theory, we compute the complete list, and in fact we find a unique such field and thereby recover the field L. The field L arises from the quadratic subfield $K = F(\sqrt{u})$, where $u = -19w^2-32w+85 \in \mathbb{Z}_F^*$; the class group of K is trivial,

but the ray class group modulo $\mathfrak{p}_2 = (w-2)\mathbb{Z}_F$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We have therefore indeed shown that $\overline{\rho}_E$ and $\overline{\rho}_A$ are isomorphic.

Next, we lift this isomorphism to one between ρ_E and ρ_A. Following Faltings and Serre, we must first compute all quadratic extensions M of L which are unramified away from 2. We find that the 2-unit group of $\mathbb{Z}_L$ modulo squares has rank 16 over $\mathbb{Z}/2\mathbb{Z}$; in other words, we have 16 independent quadratic characters of L. To each odd ideal $\mathfrak{A}$ of $\mathbb{Z}_L$, we associate the corresponding vector $v(\mathfrak{A}) = (\chi(\mathfrak{A}))_\chi \in \{\pm 1\}^{16}$ of values of these 16 characters. Then for each $v \in \{\pm 1\}^{16}$, we need to find an odd ideal $\mathfrak{A}$ of $\mathbb{Z}_L$ such that $v(\mathfrak{A}) = v$ and then verify that $\rho_A(\mathrm{Frob}_\mathfrak{a}) = \rho_E(\mathrm{Frob}_\mathfrak{a})$, where $\mathfrak{a} = \mathbb{Z}_F \cap \mathfrak{A}$. For this, it is enough to verify that $\operatorname{tr}\rho_A(\mathrm{Frob}_\mathfrak{a}) = \operatorname{tr}\rho_E(\mathrm{Frob}_\mathfrak{a})$. Moreover, by multiplicativity, thinking of $\{\pm 1\}^{16}$ as an $\mathbb{F}_2$-vector space in a natural way, it is enough to verify this for a set of odd primes $\mathfrak{P}$ of $\mathbb{Z}_L$ such that the values $v(\mathfrak{P})$ span $\{\pm 1\}^{16}$. We find that the set of primes $\mathfrak{P}$ of $\mathbb{Z}_L$ which lie above primes $\mathfrak{p}$ of $\mathbb{Z}_F$ of norm at most 239 will suffice for this purpose, and for this set we indeed verify that the Hecke eigenvalues agree. (In other words, we verify that $\#E(\mathbb{F}_\mathfrak{p}) = \#A(\mathbb{F}_\mathfrak{p})$ for enough primes $\mathfrak{p}$ of $\mathbb{Z}_F$ to ensure that in fact equality holds for all odd primes $\mathfrak{p}$ of $\mathbb{Z}_F$, whence $\rho_J \cong \rho_A$.) Therefore, E is isogeneous to A, and we have explicitly identified the isogeny class of the Jacobian of the Shimura curve $X(1)$ over F.

Second example. As a second example, we consider the Galois cubic field with $d_F = 1369 = 37^2$, so that F is the (unique totally real) cubic field in $\mathbb{Q}(\zeta_{37})$. The field F is generated by an element w satisfying $w^3 - w^2 - 12w - 11$. Here, the associated Shimura curve of level and discriminant 1 has signature $(1; 2^3, 3^3)$. Computing as above, we obtain the Hecke eigenvalues listed in Table 7.3.

TABLE 7.3: Hecke eigenvalues for the group $\Gamma(1)$ for $d_F = 1369$

$N\mathfrak{p}$	$a(\mathfrak{p})$	$\#E(\mathbb{F}_p)$
8	-5	14
11	-2	14
23	-4	28
27	0	28
29	9	21
31	-10	42
37	-11	49
43	2	42
47	6	42

Let E denote the Jacobian of the Shimura curve $X(1)$ under consideration. Since $\#E(\mathbb{F}_p)$ is always divisible by 7, it is reasonable to believe that E has a nontrivial 7-torsion point. A quick search for F-rational points on $X_1(7)$ (using the Tate model) yields a curve A with minimal model

$$A : y^2 + (w^2+w+1)xy = x^3 + (-w-1)x^2 + (256w^2 + 850w + 641)x + (5048w^2 + 16881w + 12777)$$

with $\#A(\mathbb{F}_p)$ as above. Since $A[7](F)$ is nontrivial, an argument of Skinner and Wiles [33] shows that, in fact, A is isogenous to E.

We note that the eigenvalue $a(\mathfrak{p})$ does not depend on the choice of prime $\mathfrak{p}$ above p, which suggests that E should come as a base change from a curve defined over $\mathbb{Q}$. Indeed, it can be shown by Galois descent (arising from the functoriality of the Shimura-Deligne canonical model) that the curve $X(1)$ has field of moduli equal to $\mathbb{Q}$. Looking at the curves of conductor 1369 in Cremona's tables [4], we find that A is, in fact, the base change to F of the curve

$$\texttt{1369b1} : y^2 + xy = x^3 - x^2 + 3166x - 59359.$$

Third example. We conclude with a third example for which the dimension of the space of cuspforms is greater than 1. The first cubic field F for which this occurs has $d_F = 961 = 31^2$, and the signature of the corresponding Shimura curve $X(1)$ is $(2; 2^4, 3)$. Since this field F is Galois, by Galois descent the corresponding L-function is a base change from $\mathbb{Q}$. We list the characteristic polynomial $\chi(T_\mathfrak{p})$ of Hecke operators $T_\mathfrak{p}$ in Table 7.4.

TABLE 7.4: Hecke eigenvalues for the group $\Gamma(1)$ for $d_F = 961$

$N\mathfrak{p}$	$\chi(T_\mathfrak{p})$
2	$x^2 + 2x - 1$
23	$x^2 + 8x + 16$
27	$x^2 - 4x - 28$
29	$x^2 + 8x + 8$
31	$x^2 + 20x + 100$
47	$x^2 - 8x - 16$

We see that $\mathbb{Q}(T_\mathfrak{p}) = \mathbb{Q}(\sqrt{5})$, so the Jacobian J of $X(1)$ is an abelian surface with real multiplication by $\mathbb{Q}(\sqrt{5})$. Computing via modular symbols the space of newforms for the classical modular group $\Gamma_0(961)$, we find that these characteristic polynomials indeed match a newform with q-expansion

$$q + wq^2 + wq^3 + (-2w - 1)q^4 + \cdots - 4q^{23} + \cdots - (2w + 6)q^{29} + \dots$$

where $w^2 + 2w - 1 = 0$. It is interesting to note that there are six 2-dimensional (irreducible) new Hecke eigenspaces for $\Gamma_0(961)$ and only one of the corresponding forms corresponds to an abelian surface which acquires everywhere good reduction over F.

Comments. Combining the above methods with those of Dembélé and Donnelly, one can systematically enumerate Hilbert modular forms over a wide variety of totally real fields and conductors. This project has been initiated by Donnelly and the second author [15], and we refer to this upcoming work for many, many more examples for fields up to degree 6.

We conclude with a few comments on the efficiency of our algorithms. Unfortunately, we have no provable assessment of the running time of our method. In practice, the computation of a fundamental domain seems to be the most time-consuming step (and unpredictably so), taking on the order of minutes on a standard PC for cubic and quintic fields of small discriminant; but this step should be considered a precomputation step as it need be done only once for each field F. The computation of a single Hecke operator takes on the order of seconds (for the examples above) to a few minutes (for quintic fields), the most onerous step being

the principalization step (Proposition 5.7) and the bookkeeping involved in working with the induced module; with further careful optimization, we believe that this running time can be substantially lowered.

Acknowledgments

The authors gratefully acknowledge the hospitality of the Magma group at the University of Sydney for their hospitality and would like to thank Lassina Dembélé, Steve Donnelly, Benjamin Linowitz, and Ron Livné for their helpful comments.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput., **24** (3–4), 1997, 235–265. MR1484478

[2] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Compositio Math. **59** (1986), no. 2, 151–230. MR860139 (88a:11058)

[3] J. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), no. 3, 275–324. MR743014 (85j:11063)

[4] J. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068)

[5] J. Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, 11–29. MR2282912 (2007k:11087)

[6] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Exp. Math. **16** (2007), no. 3, 303–312. MR2367320 (2008k:11057)

[7] H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*, Ann. of Math. **154** (2001), 589-639. MR1884617 (2003j:11067)

[8] H. Darmon and S. Dasgupta, *Elliptic units for real quadratic fields*, Ann. of Math. (2) **163** (2006) no. 1, 301–346. MR2195136 (2007a:11079)

[9] H. Darmon and R. Pollack, *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel J. Math. 153 (2006), 319-354. MR2254648 (2007k:11077)

[10] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, Lecture Notes in Math. **244**, no. 389, 123–165. MR0498581 (58:16675)

[11] L. Dembélé, *An algorithm for modular elliptic curves over real quadratic fields*, Experiment. Math. **17** (2008), no. 4, 427–438. MR2484426 (2010a:11119)

[12] L. Dembélé, *Quaternionic Manin symbols, Brandt matrices and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057. MR2291849 (2008g:11078)

[13] L. Dembélé and S. Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic Number Theory (Banff, 2008), Alfred van der Poorten and Andreas Stein, eds., Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, 371–386. MR2467859 (2010d:11149)

[14] L. Dieulefait, L. Guerberoff, A. Pacetti, *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79** (2010), 1145–1170.

[15] S. Donnelly and J. Voight, *Tables of Hilbert modular forms and elliptic curves over totally real fields*, in preparation.

[16] M. Eichler, *Grenzkreisgruppen und kettenbruchartige Algorithmen*, Acta Arith. **11** (1965), 169–180. MR0228436 (37:4016)

[17] N. D. Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), J. P. Buhler, ed., Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, 1–47. MR1726059 (2001a:11099)

[18] E. Freitag, *Hilbert Modular Forms*, Springer-Verlag, Berlin, 1990. MR1050763 (91c:11025)

[19] M. Greenberg, *Stark-Heegner points and the cohomology of quaternionic Shimura varieties*, Duke. J. Math., **147** (2009), no. 3, 541–575. MR2510743 (2010f:11097)

[20] H. Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, American Journal of Mathematics **103** (1981), no. 4 727-776. MR623136 (82k:10029)

[21] H. Hida, *On p-adic Hecke algebras for* GL_2 *over totally real fields*, Ann. of Math. **128** (1988), 295-384. MR960949 (89m:11046)

[22] H. Hida, *p-adic automorphic forms on Shimura varieties*, Springer-Verlag, Berlin, 2004. MR2055355 (2005e:11054)
[23] H. Hida, *Hilbert modular forms and Iwasawa theory*, Oxford Science Publications, Oxford, 2006. MR2243770 (2007h:11055)
[24] H. Jacquet and R.P. Langlands, Automorphic forms on GL(2), *Lect. Notes in Math.*, vol. 114, Springer-Verlag, Berlin, 1970. MR0401654 (53:5481)
[25] M. Kirschmer and J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, submitted.
[26] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, *Math. USSR-Izv.* **6** (1972), 19–64. MR0314846 (47:3396)
[27] Y. Matsushima and G. Shimura, *On the cohomology groups attached to certain vector-valued differential forms on the product of the upper half-planes*, Ann. of Math. **78** (1963), no. 3 417-449. MR0155340 (27:5274)
[28] T. Saito, *Hilbert Modular forms and p-adic Hodge theory*, Compos. Math. **145** (2009), no. 5, 1681–1113. MR2551990
[29] M. Schütt, *On the modularity of three Calabi-Yau threefolds with bad reduction at 11*, Canad. Math. Bull. **49** (2006), no. 2, 296-312. MR2226253 (2007d:11041)
[30] G. Shimura, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. **45** (1978), no. 3, 637–679. MR507462 (80a:10043)
[31] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159. MR0204426 (34:4268)
[32] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, Princeton University Press, Princeton, 1994. MR1291394 (95e:11048)
[33] C. Skinner and A. Wiles, *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math., no. 89 (1999), 5–126. MR1793414 (2002b:11072)
[34] W. Stein, *Modular forms, a computational approach*, with an appendix by P. E. Gunnells, Grad. Studies in Math., vol. 79, Amer. Math. Soc., Providence, RI, 2007. MR2289048 (2008d:11037)
[35] W. Stein and M. Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, 267–275. MR2041090 (2005h:11113)
[36] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), no. 2, 265–280. MR1016264 (90m:11176)
[37] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980. MR580949 (82i:12016)
[38] J. Voight, *Computing fundamental domains for Fuchsian groups*, J. Théorie Nombres Bordeaux **21** (2009), no. 2, 469–491. MR2541438
[39] J. Voight, *Shimura curves of genus at most two*, Math. Comp. **78** (2009), 1155–1172. MR2476577
[40] J. Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, submitted.

University of Calgary, 2500 University Drive NW, Calgary, AB, T2N 1N4, Canada
E-mail address: mgreenbe@math.ucalgary.ca

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, Vermont 05401
E-mail address: jvoight@gmail.com