Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

An introduction to computing modular forms using modular symbols

WILLIAM A. STEIN

ABSTRACT. We explain how weight-two modular forms on $\Gamma_0(N)$ are related to modular symbols, and how to use this to explicitly compute spaces of modular forms.

Introduction

The definition of the spaces of modular forms as functions on the upper half plane satisfying a certain equation is very abstract. The definition of the Hecke operators even more so. Nevertheless, one wishes to carry out explicit investigations involving these objects.

We are fortunate that we now have methods available that allow us to transform the vector space of cusp forms of given weight and level into a concrete object, which can be explicitly computed. We have the work of Atkin–Lehner, Birch, Swinnerton-Dyer, Manin, Mazur, Merel, and many others to thank for this (see, e.g., [Birch and Kuyk 1975; Cremona 1997; Mazur 1973; Merel 1994]). For example, we can use the Eichler–Selberg trace formula, as extended in [Hijikata 1974], to compute characteristic polynomials of Hecke operators. Then the method described in [Wada 1971] gives a basis for certain spaces of modular forms. Alternatively, we can compute Θ-series using Brandt matrices and quaternion algebras as in [Kohel 2001; Pizer 1980], or we can use a closely related geometric method that involves the module of enhanced supersingular elliptic curves [Mestre 1986]. Another related method of Birch [1991] is very fast, but gives only a piece of the full space of modular forms. The power of the modular symbols approach was demonstrated by Cremona in his book [1997], where he systematically computes a large table of invariants of all elliptic curves of conductor up to 1000 (his online tables [Cremona undated] go well beyond 100,000).

Though the above methods are each beautiful and well suited to certain applications, we will only discuss the modular symbols method further, as it has many advantages. We will primarily discuss the theory in this summary paper, leaving an explicit description of the objects involved for other papers. Nonetheless, there is a definite gap between the theory on the one hand, and an efficient running machine implementation on the other. To implement the algorithms hinted at below requires making absolutely everything completely explicit, then finding intelligent and efficient ways of performing the necessary manipulations. This is a nontrivial and tedious task, with room for error at every step. Fortunately, Sage [2008] has extensive capabilities for computing with modular forms and includes Cremona's programs; we will give a few examples below. See also the author's MAGMA [Bosma et al. 1997] package for computing with modular forms and modular symbols.

In this paper we will focus exclusively on the case of weight-2 modular forms for $\Gamma_0(N)$. The methods explained here extend to modular forms of integer weight greater than 2; for more details see [Stein 2007; Merel 1994].

Section 1 contains a brief summary of basic facts about modular forms, Hecke operators, and integral homology. Section 2 introduces modular symbols, and describes how to compute with them. Section 3 outlines an algorithm for constructing cusp forms using modular symbols in conjunction with Atkin–Lehner theory.

This paper assumes some familiarity with algebraic curves, Riemann surfaces, and homology groups of compact surfaces. A few basic facts about modular forms are recalled, but only briefly. In particular, only a roundabout attempt is made to motivate why one might be interested in modular forms; for this, see many of the references in the bibliography. No prior exposure to modular symbols is assumed.

1. Modular forms and Hecke operators

All of the objects we will consider arise from the modular group $\mathrm{SL}_2(\mathbf{Z})$ of two-by-two integer matrices with determinant equal to one. This group acts via linear fractional transformations on the complex upper half plane $\mathfrak{h}$, and also on the extended upper half plane

$$\mathfrak{h}^* = \mathfrak{h} \cup \mathbf{P}^1(\mathbf{Q}) = \mathfrak{h} \cup \mathbf{Q} \cup \{\infty\}.$$

See [Shimura 1971, § 1.3–1.5] for a careful description of the topology on $\mathfrak{h}^*$. A basis of neighborhoods for $\alpha \in \mathbf{Q}$ is given by the sets $\{\alpha\} \cup D$, where D is a disc in $\mathfrak{h}$ that is tangent to the real line at α. Let N be a positive integer and consider the group $\Gamma_0(N)$ of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ such that $N \mid c$. This group acts on $\mathfrak{h}^*$ by linear fractional transformations, and the quotient $\Gamma_0(N)\backslash\mathfrak{h}^*$ is a Riemann

surface, which we denote by $X_0(N)$. Shimura showed [1971, §6.7] that $X_0(N)$ has a canonical structure of algebraic curve over $\mathbf{Q}$.

A *cusp form* is a function f on $\mathfrak{h}$ such that $f(z)dz$ is a holomorphic differential on $X_0(N)$. Equivalently, a cusp form is a holomorphic function f on $\mathfrak{h}$ such that

(a) the expression $f(z)dz$ is invariant under replacing z by $\gamma(z)$ for each $\gamma \in \Gamma_0(N)$, and
(b) $f(z)$ is holomorphic at each element of $\mathbf{P}^1(\mathbf{Q})$, and moreover $f(z)$ tends to 0 as z tends to any element of $\mathbf{P}^1(\mathbf{Q})$.

The space of cusp forms on $\Gamma_0(N)$ is a finite dimensional complex vector space, of dimension equal to the genus g of $X_0(N)$. Viewed topologically, as a 2-dimensional real manifold, $X_0(N)(\mathbf{C})$ is a g-holed torus.

Condition (b) in the definition of $f(z)$ means that $f(z)$ has a Fourier expansion about each element of $\mathbf{P}^1(\mathbf{Q})$. Thus, at ∞ we have

$$\begin{aligned} f(z) &= a_1 e^{2\pi i z} + a_2 e^{2\pi i 2z} + a_3 e^{2\pi i 3z} + \cdots \\ &= a_1 q + a_2 q^2 + a_3 q^3 + \cdots, \end{aligned}$$

where, for brevity, we write $q = q(z) = e^{2\pi i z}$.

EXAMPLE 1.1. Let E be the elliptic curve defined by the equation $y^2 + xy = x^3 + x^2 - 4x - 5$. For $p \neq 3, 13$, let $a_p = p + 1 - \#\tilde{E}(\mathbf{F}_p)$, where $\tilde{E}$ is the reduction of E mod p, and let $a_3 = -11$, $a_{13} = 1$. For n composite, define a_n using the relations at the end of Section 3. Then

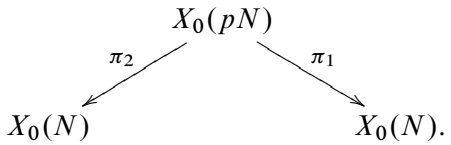
$$f = q + a_2 q^2 + a_3 q^3 + a_4 q^4 + a_5 q^5 + \cdots = q + q^2 - 11q^3 + 2q^5 + \cdots$$

is the q-expansion of a modular form on $\Gamma_0(39)$. The Shimura–Taniyama conjecture, which is now a theorem (see [Breuil et al. 2001]) asserts that any q-expansion constructed as above from an elliptic curve over $\mathbf{Q}$ is a modular form. We define the above elliptic curve and compute the associated modular form f using Sage as follows:

```
sage: E = EllipticCurve([1,1,0,-4,-5]); E
Elliptic Curve defined by y^2 + x*y  = x^3 + x^2 - 4*x - 5
over Rational Field
sage: E.q_eigenform(10)
q + q^2 - q^3 - q^4 + 2*q^5 - q^6 - 4*q^7 - 3*q^8 + q^9 + O(q^10)
```

The Hecke operators are a family of *commuting* endomorphisms of $S_2(N)$, which are defined as follows. The complex points of the open subcurve $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{h}$ are in bijection with pairs (E, C), where E is an elliptic curve over $\mathbf{C}$ and C is a cyclic subgroup of $E(\mathbf{C})$ of order N. If $p \nmid N$ then there are two natural maps π_1 and π_2 from $Y_0(pN)$ to $Y_0(N)$; the first, π_1, sends (E, C)

to (E, C'), where C' is the unique cyclic subgroup of C of order N, and the second, π_2, sends a point $(E, C) \in Y_0(N)(\mathbf{C})$ to $(E/D, C/D)$, where D is the unique cyclic subgroup of C of order p. These maps extend in a unique way to maps from $X_0(pN)$ to $X_0(N)$:



The p-th *Hecke operator* T_p is $(\pi_1)_* \circ (\pi_2)^*$; it acts on most objects attached to $X_0(N)$, such as divisors and cusp forms. There is a Hecke operator T_n for every positive integer n, but we will not need to consider those with n composite.

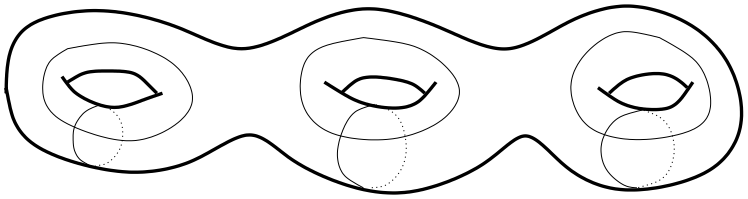
EXAMPLE 1.2. There is a basis of $S_2(39)$ so that

$$T_2 = \begin{pmatrix} 0 & 2 & -1 \\ 1 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix} \text{ and } T_5 = \begin{pmatrix} 1 & -1 & -1 \\ -2 & 2 & -2 \\ -3 & -1 & -1 \end{pmatrix}.$$

Notice that these matrices commute, and that 1 is an eigenvalue of T_2, and 2 is an eigenvalue of T_5. We compute each of the above matrices and verify that they commute using Sage as follows:

```
sage: S = CuspForms(39)
sage: T2 = S.hecke_matrix(2); T2
[ 0  2 -1]
[ 1 -2  1]
[ 0 -1  1]
sage: T5 = S.hecke_matrix(5); T5
[ 1 -1 -1]
[-2  2 -2]
[-3 -1 -1]
sage: T2*T5 == T5*T2
True
```

The first homology group $H_1(X_0(N), \mathbf{Z})$ is the group of singular 1-cycles modulo homology relations. Recall that topologically $X_0(N)$ is a g-holed torus, where g is the genus of $X_0(N)$. The group $H_1(X_0(N), \mathbf{Z})$ is thus a free abelian group of rank $2g$ (see, e.g., [Greenberg and Harper 1981, Ex. 19.30]), with two generators corresponding to each hole, as illustrated in the case $N = 39$ in Diagram 1.



$$H_1(X_0(39), \mathbf{Z}) \cong \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$$

Figure 1. The homology of $X_0(39)$.

The Hecke operators T_p act on $H_1(X_0(N), \mathbf{Z})$, and integration defines a non-degenerate Hecke-equivariant pairing

$$\langle\ ,\ \rangle : S_2(N) \times H_1(X_0(N), \mathbf{Z}) \to \mathbf{C}.$$

Explicitly, for a path x,

$$\langle f, x \rangle = 2\pi i \int_x f(z)dz,$$

where the integral may be viewed as a complex line integral along an appropriate piece of the preimage of x in the upper half plane. The pairing is Hecke equivariant in the sense that for every prime p, we have $\langle f T_p, x \rangle = \langle f, T_p x \rangle$. As we will see, modular symbols allow us to make explicit the action of the Hecke operators on $H_1(X_0(N), \mathbf{Z})$; the above pairing then translates this into a wealth of information about cusp forms.

For a more detailed survey of the basic facts about modular curves and modular forms, we urge the reader to consult the book [Diamond and Shurman 2005] along with the survey paper [Diamond and Im 1995]. For a discussion of how to draw a picture of the ring generated by the Hecke operators, see [Ribet and Stein 2001, § 3.8].

2. Modular symbols

The modular symbols formalism provides a presentation of $H_1(X_0(N), \mathbf{Z})$ in terms of paths between elements of $\mathbf{P}^1(\mathbf{Q})$. Furthermore, a trick due to Manin gives an explicit finite list of generators and relations for the space of modular symbols.

The *modular symbol* defined by a pair $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q})$ is denoted $\{\alpha, \beta\}$. As illustrated in Figure 2, this modular symbol should be viewed as the homology class, relative to the cusps, of a geodesic path from α to β in $\mathfrak{h}^*$. The homology group relative to the cusps is a slight enlargement of the usual homology group,

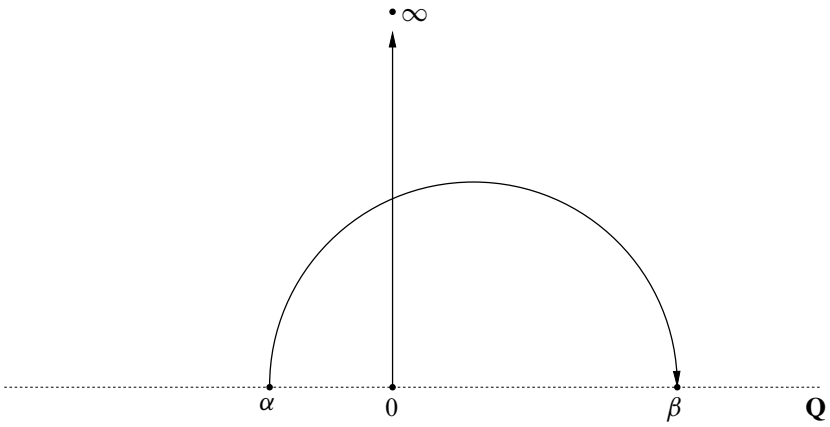


Figure 2. The modular symbols $\{\alpha, \beta\}$ and $\{0, \infty\}$.

in that we allow paths with endpoints in $\mathbf{P}^1(\mathbf{Q})$ instead of restricting to closed loops.

Motivated by this picture, we declare that modular symbols satisfy the following homology relations: if $\alpha, \beta, \gamma \in \mathbf{Q} \cup \{\infty\}$, then

$$\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0.$$

Furthermore, we quotient out by any torsion, so, e.g., $\{\alpha, \alpha\} = 0$ and $\{\alpha, \beta\} = -\{\beta, \alpha\}$.

Denote by $\mathcal{M}_2$ the free abelian group with basis the set of symbols $\{\alpha, \beta\}$ modulo the three-term homology relations above and modulo any torsion. There is a left action of $\mathrm{GL}_2(\mathbf{Q})$ on $\mathcal{M}_2$, whereby a matrix g acts by

$$g\{\alpha, \beta\} = \{g(\alpha), g(\beta)\},$$

and g acts on α and β by a linear fractional transformation. The space $\mathcal{M}_2(N)$ of *modular symbols for* $\Gamma_0(N)$ is the quotient of $\mathcal{M}_2$ by the submodule generated by the infinitely many elements of the form $x - g(x)$, for x in $\mathcal{M}_2$ and g in $\Gamma_0(N)$, and modulo any torsion. A *modular symbol for* $\Gamma_0(N)$ is an element of this space. We frequently denote the equivalence class that defines a modular symbol by giving a representative element.

Manin [1972] proved there is a natural injection $H_1(X_0(N), \mathbf{Z}) \to \mathcal{M}_2(N)$. The image of $H_1(X_0(N), \mathbf{Z})$ in $\mathcal{M}_2(N)$ can be identified as follows. Let $\mathcal{B}_2(N)$ denote the free abelian group whose basis is the finite set $\Gamma_0(N)\backslash\mathbf{P}^1(\mathbf{Q})$. The *boundary map* $\delta : \mathcal{M}_2(N) \to \mathcal{B}_2(N)$ sends $\{\alpha, \beta\}$ to $[\beta]-[\alpha]$, where $[\beta]$ denotes the basis element of $\mathcal{B}_2(N)$ corresponding to $\beta \in \mathbf{P}^1(\mathbf{Q})$. The kernel $\mathcal{S}_2(N)$ of δ is the subspace of *cuspidal* modular symbols. An element of $\mathcal{S}_2(N)$ can

be thought of as a linear combination of paths in $\mathfrak{h}^*$ whose endpoints are cusps, and whose images in $X_0(N)$ are a linear combination of loops. We thus obtain a map $\varphi : \mathcal{S}_2(N) \to H_1(X_0(N), \mathbf{Z})$.

THEOREM 2.1. The map φ given above defines a canonical isomorphism

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

2.1. Manin's trick. In this section, we describe a trick of Manin that shows that the space of modular symbols can be computed.

By reducing modulo N, one sees that the group $\Gamma_0(N)$ has finite index in $\mathrm{SL}_2(\mathbf{Z})$. Let $r_0, r_1, \ldots, r_m$ be distinct right coset representatives for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbf{Z})$, so that

$$\mathrm{SL}_2(\mathbf{Z}) = \Gamma_0(N)r_o \cup \Gamma_0(N)r_1 \cup \cdots \cup \Gamma_0(N)r_m,$$

where the union is disjoint. For example, when N is prime, a list of coset representatives is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ N-1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

In general, the right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbf{Z})$ are in bijection with the elements of $\mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$ (see [Cremona 1997, § 2.2] for complete details).

The following trick of Manin [1972, § 1.5] (see also [Cremona 1997, § 2.1.6]) allows us to write every modular symbol as a $\mathbf{Z}$-linear combination of symbols of the form $r_i\{0, \infty\}$. In particular, the finitely many symbols $r_i\{0, \infty\}$ generate $\mathcal{M}_2(N)$.

Because of the relation $\{\alpha, \beta\} = \{0, \beta\} - \{0, \alpha\}$, it suffices to consider modular symbols of the form $\{0, b/a\}$, where the rational number b/a is in lowest terms. Expand b/a as a continued fraction and consider the successive convergents in lowest terms:

$$\frac{b_{-2}}{a_{-2}} = \frac{0}{1}, \quad \frac{b_{-1}}{a_{-1}} = \frac{1}{0}, \quad \frac{b_0}{a_0} = \frac{b_0}{1}, \ldots, \quad \frac{b_{n-1}}{a_{n-1}}, \quad \frac{b_n}{a_n} = \frac{b}{a}$$

where the first two are added formally. Then

$$b_k a_{k-1} - b_{k-1} a_k = (-1)^{k-1},$$

so that

$$g_k = \begin{pmatrix} b_k & (-1)^{k-1} b_{k-1} \\ a_k & (-1)^{k-1} a_{k-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

Hence

$$\left\{ \frac{b_{k-1}}{a_{k-1}}, \frac{b_k}{a_k} \right\} = g_k\{0, \infty\} = r_i\{0, \infty\},$$

for some i, is of the required special form.

EXAMPLE 2.2. Let $N = 11$, and consider the modular symbol $\{0, 4/7\}$. We have

$$\frac{4}{7} = 0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}},$$

so the partial convergents are

$$\frac{b_{-2}}{a_{-2}} = \frac{0}{1}, \quad \frac{b_{-1}}{a_{-1}} = \frac{1}{0}, \quad \frac{b_0}{a_0} = \frac{0}{1}, \quad \frac{b_1}{a_1} = \frac{1}{1}, \quad \frac{b_2}{a_2} = \frac{1}{2}, \quad \frac{b_3}{a_3} = \frac{4}{7}.$$

Thus

$$\begin{aligned}\{0, 4/7\} &= \{0, \infty\} + \{\infty, 0\} + \{0, 1\} + \{1, 1/2\} + \{1/2, 4/7\} \\ &= \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \{0, \infty\} + \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix} \{0, \infty\} \\ &= 2 \cdot \left[\begin{pmatrix} 1 & 4 \\ 1 & 5 \end{pmatrix} \{0, \infty\} \right].\end{aligned}$$

2.2. Manin symbols. As above, fix coset representatives $r_0, \ldots, r_m$ for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbf{Z})$. Denote the modular symbol $r_i\{0, \infty\}$ by $[r_i]$. The symbols $[r_0]$, $\ldots, [r_m]$ are called *Manin symbols*, and they are equipped with a right action of $\mathrm{SL}_2(\mathbf{Z})$, which is given by $[r_i]g = [r_j]$, where $\Gamma_0(N)r_j = \Gamma_0(N)r_i g$. Recall that $\mathrm{SL}_2(\mathbf{Z})$ is generated by the two matrices $\sigma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ (see Theorem 2 of [Serre 1973, VII.1.2]).

THEOREM 2.3 (MANIN). The Manin symbols $[r_0], \ldots, [r_m]$ satisfy the relations

$$[r_i] + [r_i]\sigma = 0,$$
$$[r_i] + [r_i]\tau + [r_i]\tau^2 = 0.$$

Furthermore, these relations generate all relations (modulo torsion relations).

This theorem, proved in [Manin 1972, § 1.7], provides a finite presentation for the space of modular symbols.

2.3. Hecke operators on modular symbols. When p is a prime not dividing N, define

$$T_p\{\alpha, \beta\} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \{\alpha, \beta\} + \sum_{r \bmod p} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} \{\alpha, \beta\}.$$

As mentioned before, this definition is compatible with the integration pairing $\langle , \rangle$ of Section 1, in the sense that $\langle f T_p, x \rangle = \langle f, T_p x \rangle$. When $p \mid N$, the definition is the same, except that the matrix $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is dropped.

For example, when $N = 11$ we have

$$T_2\{0, 1/5\} = \{0, 2/5\} + \{0, 1/10\} + \{1/2, 3/5\} = -2\{0, 1/5\}.$$

L. Merel [1994] gave a description of the action of T_p directly on Manin symbols $[r_i]$ (see also [Cremona 1997, § 2.4]). For example, when $p = 2$ and N is odd, we have

$$T_2([r_i]) = [r_i]\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix} + [r_i]\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix} + [r_i]\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix} + [r_i]\begin{pmatrix}1 & 0\\ 1 & 2\end{pmatrix}.$$

3. Computing the space of modular forms

In this section we describe how to use modular symbols to construct a basis of $S_2(N)$ consisting of modular forms that are eigenvectors for every element of the ring $\mathbf{T}'$ generated by the Hecke operator T_p, with $p \nmid N$. Such eigenvectors are called *eigenforms*.

Suppose M is a positive integer that divides N. As explained in [Lang 1995, VIII.1–2], for each divisor d of N/M there is a natural *degeneracy map* $\beta_{M,d}$: $S_2(M) \to S_2(N)$ given by $\beta_{M,d}(f(q)) = f(q^d)$. The *new subspace* of $S_2(N)$, denoted $S_2(N)^{\text{new}}$, is the orthogonal complement with respect to the Petersson inner product of the images of all maps $\beta_{M,d}$, with M and d as above.

The theory of Atkin and Lehner [1970] asserts that, as a $\mathbf{T}'$-module, $S_2(N)$ is built up as follows:

$$S_2(N) \quad = \bigoplus_{M|N,\ d|N/M} \beta_{M,d}(S_2(M)^{\text{new}}).$$

To compute $S_2(N)$ it thus suffices to compute $S_2(M)^{\text{new}}$ for each positive divisor M of N.

We now turn to the problem of computing $S_2(N)^{\text{new}}$. Atkin and Lehner [1970] also proved that $S_2(N)^{\text{new}}$ is spanned by eigenforms, each of which occurs with multiplicity one in $S_2(N)^{\text{new}}$. Moreover, if $f \in S_2(N)^{\text{new}}$ is an eigenform then the coefficient of q in the q-expansion of f is nonzero, so it is possible to normalize f so that coefficient of q is 1. With f so normalized, if $T_p(f) = a_p f$, then the p-th Fourier coefficient of f is a_p. If $f = \sum_{n=1}^{\infty} a_n q^n$ is a normalized eigenvector for all T_p, then the a_n, with n composite, are determined by the a_p, with p prime, by the following formulas: $a_{nm} = a_n a_m$ when n and m are relatively prime, and $a_{p^r} = a_{p^{r-1}} a_p - p a_{p^{r-2}}$ for $p \nmid N$ prime. When $p \mid N$, $a_{p^r} = a_p^r$. We conclude that in order to compute $S_2(N)^{\text{new}}$, it suffices to compute all systems of eigenvalues $\{a_2, a_3, a_5, \ldots\}$ of the Hecke operators $T_2, T_3, T_5, \ldots$ acting on $S_2(N)^{\text{new}}$. Given a system of eigenvalues, the corresponding eigenform is $f = \sum_{n=1}^{\infty} a_n q^n$, where the a_n, for n composite, are determined by the recurrence given above.

In light of the pairing $\langle\ ,\ \rangle$ introduced in Section 1, computing the above systems of eigenvalues $\{a_2, a_3, a_5, \ldots\}$ amounts to computing the systems of

eigenvalues of the Hecke operators T_p on the subspace V of $\mathcal{S}_2(N)$ that corresponds to the new subspace of $S_2(N)$. For each proper divisor M of N and each divisors d of N/M, let $\phi_{M,d} : \mathcal{S}_2(N) \to \mathcal{S}_2(M)$ be the map sending x to $\left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)x$. Then V is the intersection of the kernels of all maps $\phi_{M,d}$.

The computation of the systems of eigenvalues of a collection of commuting diagonalizable endomorphisms involves standard linear algebra techniques, such as the computation of characteristic polynomials and kernels of matrices. There are, however, several tricks that greatly speed up this process, some of which are described in [Stein 2000, § 3.5.4].

EXAMPLE 3.1. All forms in $S_2(39)$ are new. Up to Galois conjugacy, the eigenvalues of the Hecke operators T_2, T_3, T_5, and T_7 on $\mathcal{S}_2(39)$ are $\{1, -1, 2, -4\}$ and $\{a, 1, -2a-2, 2a+2\}$, where $a^2 + 2a - 1 = 0$. (Note that these eigenvalues occur with multiplicity two.) Thus $S_2(39)$ has dimension 3, and is spanned by

$$f_1 = q + q^2 - q^3 - q^4 + 2q^5 - q^6 - 4q^7 + \cdots,$$

$$f_2 = q + aq^2 + q^3 + (-2a-1)q^4 + (-2a-2)q^5 + aq^6 + (2a+2)q^7 + \cdots,$$

and the Galois conjugate of f_2. We compute f_1 and f_2 using Sage as follows:

```
sage: CuspForms(39).newforms('a')
[q + q^2 - q^3 - q^4 + 2*q^5 + O(q^6),
 q + a1*q^2 + q^3 + (-2*a1 - 1)*q^4 + (-2*a1 - 2)*q^5 + O(q^6)]
```

3.1. Summary. To compute the q-expansion, to some precision, of each eigenforms in $S_2(N)$, we use the degeneracy maps so that we only have to solve the problem for $S_2(N)^{\text{new}}$. Here, using modular symbols we compute the systems of eigenvalues $\{a_2, a_3, a_5, \ldots\}$, then write down each of the corresponding eigenforms $q + a_2 q^2 + a_3 q^3 + \cdots$.

References

[Atkin and Lehner 1970] A. Atkin and J. Lehner, "Hecke operators on $\Gamma_0(m)$", *Math. Ann.* **185** (1970), 134–160.

[Birch 1991] B. J. Birch, "Hecke actions on classes of ternary quadratic forms", pp. 191–212 in *Computational number theory* (Debrecen, 1989), de Gruyter, Berlin, 1991.

[Birch and Kuyk 1975] B. Birch and W. Kuyk (editors), *Modular functions of one variable. IV*, Lecture Notes in Mathematics **476**, Springer, Berlin, 1975.

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

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over **Q**: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939.

[Cremona 1997] J. Cremona, *Algorithms for modular elliptic curves*, Second ed., Cambridge University Press, Cambridge, 1997. Available at http://www.maths.nott.ac.uk/personal/jec/book/.

[Cremona undated] J. Cremona, Elliptic curves data, undated. Available at http://www.warwick.ac.uk/~masgaj/ftp/data/.

[Diamond and Im 1995] F. Diamond and J. Im, "Modular forms and modular curves", pp. 39–133 in *Seminar on Fermat's Last Theorem*, Providence, RI, 1995.

[Diamond and Shurman 2005] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics **228**, Springer, New York, 2005.

[Greenberg and Harper 1981] M. Greenberg and J. Harper, *Algebraic topology: A first course*, Benjamin/Cummings, Reading, MA, 1981.

[Hijikata 1974] H. Hijikata, "Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$", *J. Math. Soc. Japan* **26**:1 (1974), 56–82.

[Kohel 2001] D. R. Kohel, "Hecke module structure of quaternions", pp. 177–195 in *Class field theory—its centenary and prospect* (Tokyo, 1998), edited by K. Miyake, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001.

[Lang 1995] S. Lang, *Introduction to modular forms*, Springer, Berlin, 1995. With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original.

[Manin 1972] J. Manin, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 19–66.

[Mazur 1973] B. Mazur, "Courbes elliptiques et symboles modulaires", pp. 277–294, Exp. No. 414 in *Séminaire Bourbaki, 24ème année* (1971/1972), Lecture Notes in Math. **317**, Springer, Berlin, 1973.

[Merel 1994] L. Merel, "Universal Fourier expansions of modular forms", pp. 59–94 in *On Artin's conjecture for odd 2-dimensional representations*, Springer, 1994.

[Mestre 1986] J.-F. Mestre, "La méthode des graphes: exemples et applications", pp. 217–242 in *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata)*, Nagoya Univ., Nagoya, 1986.

[Pizer 1980] A. Pizer, "An algorithm for computing modular forms on $\Gamma_0(N)$", *J. Algebra* **64**:2 (1980), 340–390.

[Ribet and Stein 2001] K. Ribet and W. Stein, "Lectures on Serre's conjectures", pp. 143–232 in *Arithmetic algebraic geometry* (Park City, UT, 1999), IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001.

[Sage 2008] W. Stein and the Sage Group, *Sage:* open source mathematical software (Version 3.0), 2008. Available at http://www.sagemath.org.

[Serre 1973] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics **7**, Springer, New York, 1973.

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten, Tokyo, and Princeton University Press, Princeton, NJ, 1971.

[Stein 2000] W. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley, 2000.

[Stein 2007] W. Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics **79**, American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[Wada 1971] H. Wada, "Tables of Hecke operations, I", pp. 10 in *Seminar on modern methods in number theory*, Inst. Statist. Math., Tokyo, 1971.

WILLIAM A. STEIN
ASSOCIATE PROFESSOR OF MATHEMATICS
UNIVERSITY OF WASHINGTON
wstein@gmail.com