The Hecke Stability Method
and Ethereal Forms

By

George Johann Schaeffer

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy
in
Mathematics
in the
Graduate Division
of the
University of California, Berkeley

Committee in charge:
Professor Akshay Venkatesh, Co-chair
Professor Kenneth A. Ribet, Co-chair
Professor Martin Olsson
Professor David Wagner

Spring 2012
Abstract

The Hecke Stability Method and Ethereal Forms

by

George Johann Schaeffer

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Akshay Venkatesh, Co-chair
Professor Kenneth A. Ribet, Co-chair

The purpose of this thesis is to outline the Hecke stability method (HSM), a novel method for the computation of modular forms.

The HSM relies on the following idea: A finite-dimensional space of ratios of modular forms that is stable under the action of a Hecke operator should consist of modular forms (i.e., without poles). This principle is correct over \( \mathbb{C} \), but more care is required over \( \overline{\mathbb{F}}_p \) due to complications arising near the supersingular points on \( X_1(N) \). Formalizing this main idea as a theorem comprises most of our theoretical work.

Though it can be utilized in a variety of settings, the main application of the Hecke stability method is the computation of weight 1 modular forms. These spaces cannot be computed using the algorithms (e.g., modular symbols algorithms) that are typically employed to compute modular forms of higher weight.

Furthermore, to provide a complete picture of the weight 1 modular forms of level \( N \), we must account for certain sporadic discrepancies between the space of classical forms and the space of mod \( p \) modular forms. Ultimately, our approach is motivated by the effect this “ethereality” phenomenon may have on the statistics of number fields via the theory of modular Galois representations.
To John, and to the last three years.
# Contents

Introduction v

I Theoretical and computational groundwork 1

1 Modular forms ......................................................... 1
   1.1 Moduli of level structures .................................... 2
   1.2 Katz modular forms ............................................ 4
   1.3 Test objects and $q$-expansion .............................. 5
   1.4 Basic structure theory of modular forms ..................... 5
   1.5 Base change and mod $p$ modular forms ..................... 7
   1.6 Level 1 modular forms and weight 1 Eisenstein series ... 7
   1.7 Fractional modular forms ..................................... 9

2 Hecke operators ..................................................... 11
   2.1 Hecke correspondences on moduli ............................ 11
   2.2 Hecke operators on (fractional) modular forms .......... 13
   2.3 Hecke correspondences on $q$-expansions .................. 14
   2.4 Hecke eigenforms and Galois representations .............. 15

3 Computing with modular forms ................................... 16
   3.1 Computing modular forms when $k \geq 2$ ................. 16
   3.2 Computing mod $p$ modular forms when $k = 1$ ............ 18
   3.3 Locating the zeros of a modular form .................... 18

II Isogeny graphs 23

4 Isogeny graphs on $\Gamma_0(N)$-structures ..................... 24
   4.1 The full and derived isogeny graphs ....................... 24
   4.2 Isogeny graphs and endomorphisms of level structures .... 25
   4.3 Ordinary and supersingular isogeny graphs ............... 27

5 Combinatorial results on isogeny graphs ...................... 29
   5.1 Local structure of isogeny graphs ........................ 30
   5.2 Polar conditions ............................................. 30
   5.3 The technical lemma ....................................... 32
III Hecke stability

6 The Hecke stability theorem ........................................ 36
   6.1 Preparation ...................................................... 36
   6.2 Statement, proof, and consequences .......................... 38

7 Computing weight 1 modular forms ................................. 39
   7.1 Application of the Hecke stability theorem .................. 39
   7.2 Formal implementation ......................................... 41
   7.3 Certification and identification of cusp forms ............. 45

8 Ethereal forms and the extended HSM ............................. 47
   8.1 Ethereality ..................................................... 47
   8.2 Detection of ethereal characteristics ....................... 49
   8.3 Lower bounds on the group $E(N,\chi)$ ........................ 54
   8.4 Complexity of the extended HSM ............................. 56

References ............................................................... 58

A Tables ................................................................. 63
Notation

The symbol \( \subset \) will always denote inclusion or equality, with \( \subseteq \) reserved for proper inclusions.

The letter \( \phi \) will always denote Euler’s totient function, while the variant \( \varphi \) will have no fixed meaning. In most contexts, \( \pi_N \) will denote the projection map defined in Section 1.1, but \( \pi_1(X,x) \) will denote the fundamental group of a topological space in Section 4.2.

If \( F \) is a field (always perfect in this thesis), \( \bar{F} \) will denote a (tacit) choice of algebraic closure.

If \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{R}^\times \) is a character, \( f_\chi \) will denote the conductor of the character. As is standard, we will also use \( \chi \) to denote the function \( \mathbb{Z} \to R \) induced by the character. \( \varepsilon_N \) will typically denote the quadratic character of conductor \( N \) (with level implicit from context), and \( 1 \) will be used to denote the trivial character (also with level implicit from context).

When \( G \) is a graph, \( \mathcal{V}(G) \) will denote its set of vertices and \( \mathcal{E}(G) \) will denote its set of edges (or arcs, when \( G \) is directed). We treat \( G \) as the disjoint union \( \mathcal{V}(G) \cup \mathcal{E}(G) \). The symbol \( \leftrightarrow_G \) (resp. \( \rightarrow_G \)) will denote the adjacency relation when \( G \) is an undirected (resp. directed) graph; the subscript will be omitted wherever the ambient graph is implicit from context.

Let \( s \) be a section of some line bundle \( \mathcal{L} \) on a curve \( X \). The notation \( \text{ord}_\tau(s) \) will mean the order of section \( s \) at a geometric point \( \tau \in X \); positive orders correspond to zeros and negative orders correspond to poles. \( Z(s) \) denotes the set of geometric points on \( X \) where \( s \) vanishes.
Introduction

Modular forms have found utility both in number theory (e.g., the proof of Fermat’s last theorem [Wil95]) and other areas of mathematics (e.g., the construction of families of expander graphs [Sar90]). A major achievement of modern number theory is the following correspondence between Galois representations and modular forms:

\[ \left\{ \text{new cuspidal Hecke eigenforms over } \overline{\mathbb{F}}_p \text{ of weight } k \text{ and level } N \right\} \leftrightarrow \left\{ \text{representations } \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{F}}_p) \text{ of “Serre type,” unramified outside } Np \right\} \]

established by the work of many researchers over the course of the last five decades and codified in theorems of Eichler–Shimura [Shi71], Deligne [Del68], Deligne–Serre [DS74] (→), and Khare–Wintenberger [KW09] (←).

The weight 1 case \((k = 1)\) of this correspondence is special for a number of reasons:

- The projective Galois representations associated to weight 1 new cuspidal Hecke eigenforms over \(\overline{\mathbb{F}}_p\) are unramified at \(p\) when \(p > 2\). [CV92] [Wie11]

- Let \(M_k(N; R)\) denote the \(R\)-module of modular forms of weight \(k\) and level \(N\) over the ring \(R\) (in the sense of Katz [Kat72]). For \(p \nmid N\), the reduction map \(M_k(N; \mathbb{Z}[\frac{1}{N}]) \to M_k(N; \mathbb{F}_p)\) is surjective when \(k \geq 2\), but this is not necessarily the case when \(k = 1\).

Hecke eigenforms of weight 1 and level \(N\) over \(\overline{\mathbb{F}}_p\) that lie outside of

\[ \text{im}(M_1(N; \mathbb{Z}[\frac{1}{N}]) \to M_1(N; \mathbb{F}_p)) \otimes \overline{\mathbb{F}}_p \]

are the ethereal forms. The existence of such forms is equivalent to the presence of nontrivial \(p\)-torsion in the group \(H^1(X_1(N), \omega)\) (where \(\omega\) is a certain line bundle defined in Section 1.2). The first example of such a form was given by Mestre in a letter to Serre in 1987; see [Edi06] and Example 8.1.5. The first examples defined of a field of odd characteristic are due to Buzzard (see [Buz12]).

The representations attached to known examples of new ethereal forms in characteristic \(p \geq 7\) have “large” image, which means such forms could potentially be used to construct number fields with large Galois group and small, prescribed ramification (as in [Buz12]).
• The modular symbols algorithms that are used to compute spaces of weight \( k \geq 2 \) modular forms (see Theorem 3.1.1) do not extend directly to weight 1. In [Edi06], Edixhoven notes that

"... There seem to be no tables of mod \( p \) modular forms of weight one, and worse, no published algorithm to compute such tables."

The topic of this thesis is the development of the Hecke stability method (HSM), a procedure for effectively computing and analyzing weight 1 modular forms in a way that takes the ethereal forms into account. The HSM addresses and (in most cases) solves the problem posed by Edixhoven above.

**The main idea of the Hecke stability method**

Let \( F \) be a field, let \( M(N; F) = \bigoplus_{k \geq 0} M_k(N; F) \) be the \( F \)-algebra of modular forms of level \( N \) graded by weight, and let \( M^{\text{frac}}(N; F) \) be the \( \mathbb{Z} \)-graded \( F \)-algebra generated by ratios of homogeneous elements from \( M(N; F) \).

The HSM is based on the following idea: If \( V \subset M^{\text{frac}}(N; F) \) is a finite-dimensional subspace of \( M(N; F) \) that is stable under the action of a Hecke operator \( T_\ell \), then \( V \subset M(N; F) \) (i.e., \( V \) contains no elements with poles) provided that the set

\[
\Pi(V)^{ss} = \{ \tau \in X_1(N)^{ss}_F : \text{there exists } f \in V \text{ with } \text{ord}_\tau(f) < 0 \}
\]

(where \( X_1(N)^{ss}_F \) is the supersingular locus of the modular curve) is either empty or "small" compared to \( \text{char } F \) (in an explicit sense). In particular, the desired inclusion \( V \subset M(N; F) \) is guaranteed whenever \( \text{char } F = 0 \).

The formalization of this main idea as the Hecke stability theorem (Theorem 6.2.1) and the proof of that theorem—which occupies Chapters II and the first section of Chapter III—comprise most of the theoretical work of this thesis.

**Hecke stability and weight 1 modular forms**

Suppose that we want to compute a space of the form \( M_1(N, \chi; F) \) where \( N \geq 5 \), \( F \) is either \( \mathbb{C} \) or \( \overline{\mathbb{F}}_p \) with \( p \nmid 2N \),\(^1\) and \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times \) is an odd Dirichlet character (i.e., \( \chi(-1) = -1 \)). After constructing a nonempty finite subset \( A \subset M_1(N, \chi^{-1}; F) \setminus \{0\} \), we have inclusions

\[
M_1(N, \chi; F) \subset V(0)(N; F; A) := \bigcap_{\lambda \in A} \lambda^{-1}M_2(N, 1; F) \subset M_1^{\text{frac}}(N, \chi; F).
\]

The target space \( M_1(N, \chi; F) \) and the space \( V(0)(N; F; A) \) above are finite-dimensional, while \( M_1(N, \chi; F) \) and the ambient space \( M_1^{\text{frac}}(N, \chi; F) \) are stable under the Hecke

\(^1\)The reader should not be overly concerned by the exclusion of \( p = 2 \) here (see Remark 3.2.2.)
operators. Hence, for any prime $\ell$ that does not divide $N$ and which is not the characteristic of $F$, the largest $T_\ell$-stable subspace of $V^{(0)}(N; F; A)$, namely

$$V^{(\infty)}_\ell(N; F; A) := \{ f \in V^{(0)}(N; F; A) : \text{for all } r \geq 0, T_\ell^r f \in V^{(0)}(N; F; A) \},$$

is equal (by the Hecke stability theorem) to $M_1(N, \chi; F)$, provided that the intersection $X_1(N)_{\overline{F}}^\infty \cap \bigcap_{\lambda \in A} Z(\lambda)$ is empty or “sufficiently small” compared to $\text{char } F$. Rough estimates for the size of this set can be given using general results on the zeros of modular forms (see for example [Mil97] Proposition 4.12, Proposition 1.4.1.c below, or Corollary 7.1.3 below), and in Section 3.3 we will give an explicit method for determining the projection of the set $\bigcap_{\lambda \in A} Z(\lambda)$ onto the $j$-line.

One advantage of this approach is that it requires a minimal amount of auxiliary computation: After one computes

- An integral basis for $M_2(N, 1; \mathbb{Z}[[1/N]])$ once per level, and
- A nonempty set of (nonzero) forms $A \subset M_1(N, \chi^{-1}; F)$ (per character),

then a basis for $V^{(\infty)}_\ell(N; F; A)$ can be computed using linear algebra on $q$-expansions (of sufficiently high precision) because we know how to interpret $T_\ell$ on $q$-expansions (Proposition 2.3.1). The auxiliary computations are implemented in the [SAGE] computer algebra package (see also Sections 1.6 and 3.1). The computation of $V^{(\infty)}_\ell(N; F; A)$ and ways to interpret its output are covered in Sections 7.2 and 7.3.

Ethereality and the extended HSM

As mentioned above, the reduction map

$$M_1(N; \mathbb{Z}[[1/N]]) \rightarrow M_1(N; \mathbb{F}_p)$$

(with $p \nmid N$) can fail to be surjective for certain $p$, called the ethereal characteristics of level $N$. In short, not every weight 1 modular form mod $p$ lifts to a classical weight 1 modular form over $\mathbb{C}$. For a satisfactory account of all weight 1 modular forms of level $N$, we therefore require a method for their computation that takes these characteristics into account.

The Hecke stability algorithm (Algorithm 7.2.6) produces a basis for $M_1(N, \chi; \mathbb{C})$ by constructing a descending sequence

$$V^{(0)}_\ell(N; \mathbb{C}; A) \supset \cdots \supset V^{(n)}_\ell(N; \mathbb{C}; A) = M_1(N, \chi; \mathbb{C})$$

of vector spaces over $\mathbb{C}$; by design, Algorithm 7.2.6 computes bases for these spaces whose $q$-expansions have coefficients in a ring $\mathcal{O}_A$ of algebraic integers. By analyzing the $\mathcal{O}_A$-modules generated by these bases, we can derive a finite list of prime ideals $p \subset \mathcal{O}_{\mathbb{Q}(\chi)}$ that contains every $p$ for which

$$M_1(N, \chi; \mathcal{O}_A) \rightarrow M_1(N, \chi; \mathcal{O}_A/p)$$
is not surjective. This “extended” version of the HSM is the subject of Section 8.

In theory, the extended HSM allows us to describe the prime-to-$N$ component $E(N) \subset H^1(X_1(N); \omega)$ completely. Appendix A contains tables that describe certain “easily computable” factors of $E(N)$ for all odd levels $N < 750$, and our data indicates that this group $E(N)$ apparently grows very quickly in $N$. Because of the relationship between this group and representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we anticipate that this observation will provide motivation for future investigation.

Outline

Chapter I is a self-contained review of the theoretical concepts and computational results that we will require. Of particular importance are the results concerning the behavior of fractional modular forms under the Hecke operators (especially Corollary 2.2.3 and Corollary 2.3.4). We will also briefly present relevant results from previous work on the computation of modular forms (Sections 3.1 and 3.2) and in Section 3.3 we will sketch an algorithm for determining the zero set of a modular form.

Chapter II outlines the technical details of the combinatorial argument that we will use to prove the Hecke stability theorem (Theorem 6.2.1). Briefly, we will relate the Hecke operator $T_\ell$ to the adjacency operator of the isogeny graph $G_\ell(N; F)$. In the ordinary case these graphs are easy to describe (Theorem 4.3.1), but the supersingular case is rather more complicated (Lemma 4.3.2 and Lemma 4.3.4). In the end, we will describe the structure of $G_\ell(N; F)$ locally (Lemma 5.1.2); this will allow us to formulate lower bounds on the size of $\Pi(V)^{ss}$ (as above) when it is nonempty (Lemma 5.3.3).

Chapter III contains the statement of the Hecke stability theorem and its proof (Section 6.2). Section 7.1 demonstrates how the Hecke stability theorem adapts to the particular setting of weight 1 forms, and Section 7.2 contains the Hecke stability algorithm, which can be used to compute spaces of such forms under certain conditions. Section 7.3 covers methods for certifying the output of the Hecke stability algorithm and for identifying cusp forms. Finally, Section 8 covers the extended HSM, which modifies the Hecke stability algorithm (Algorithm 8.2.7) to detect ethereal characteristics.

Appendix A contains tables, including tables that list all ethereal forms of quadratic character at levels $N < 750$. 
Acknowledgements

First of all, I would like to thank Akshay Venkatesh, who agreed to be my advisor despite the obvious challenges of our transbay relationship. This thesis would not exist if not for his inspired suggestions and his constant enthusiasm for my work and growth as a mathematician.

Among the excellent faculty at UC Berkeley, I would like to thank Ken Ribet and Martin Olsson for their invaluable advice over the years, as well as Dave Wagner, for bravely serving on my dissertation committee and for providing helpful comments on this dissertation. I would also like to thank John Voight of the University of Vermont, Kevin Buzzard of Imperial College London, and Frank Calegari of Northwestern University for their encouragement and guidance during the course of this research.

Finally, I would like to thank my family and friends, who supported me in so many ways these last five years. You guys are the best!
Chapter I

Theoretical and computational groundwork

This chapter collects the necessary background material on modular forms (in the sense of Katz), fractional modular forms, Hecke operators, and methods for computing with these objects ($q$-expansions, modular symbols, etc.).

Sections 1.1–1.5 are an exposition of the basic results in the theory of modular forms as constructed by Katz in his seminal paper [Kat72]. Section 1.6, which describes modular forms of level 1 and Eisenstein series of weight 1, mainly follows [DS05], Chapter 4. Section 1.7 concerns fractional modular forms, objects that are not treated consistently in the literature but that are essential in this thesis.

Section 2 covers the action of the Hecke operators on modular forms and fractional modular forms, as well as the interpretation of this action via $q$-expansions. This section also quotes formal statements concerning the correspondence between modular forms over $\overline{\mathbb{F}}_p$ and Galois representations.

In Sections 3.1 and 3.2 we review some of the previous work on the computation of modular forms. In section 3.3 we give an algorithm for the computation of the zero set of a modular form; although we have a specific purpose for this algorithm in mind, it may be of independent interest.

1 Modular forms

Modular forms are typically introduced as a class of holomorphic functions on the Poincaré upper half-plane. A holomorphic function

$$f : \mathfrak{h}^* = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q}) \rightarrow \mathbb{C},$$

where

$$\mathfrak{h} = \{ z \in \mathbb{C} : \operatorname{Im} z > 0 \},$$
is a modular form (in the classical sense) of weight $k$ and level $N$ if for every $z \in \mathfrak{h}^*$ and every matrix $\gamma \in \text{SL}_2(\mathbb{Z})$ with

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}$$

we have $f(\frac{az+b}{cz+d}) = (cz + d)^k f(z)$.

The quotient of $\mathfrak{h}$ by the group of matrices as above parametrizes pairs $(E, P)$ where $E/\mathbb{C}$ is an elliptic curve and $P \in E(\mathbb{C})$ is a point of order exactly $N$, so modular forms admit a moduli interpretation. For example, classical modular forms of level 1 attach numerical data to elliptic curves (see also Example 1.6.6). This viewpoint allows us to construct a theory of modular forms over general rings.

### 1.1 Moduli of level structures

An elliptic curve over a ring $R$ (always commutative with unit) is a smooth projective curve $E/R$ of genus 1 equipped with a section $\text{Spec } R \rightarrow E$. Elliptic curves can be defined over a general scheme (see [Kat72] Section 1.0), but we will not require that level of generality.

When $R$ is a $\mathbb{Z}[\frac{1}{N}]$-algebra we define two kinds of level $N$ structure over $R$:

- A $\Gamma_1(N)$-structure over $R$ is a pair $(E, P)$ where $E/R$ is an elliptic curve and $P \in E(R)$ is a point of order (exactly) $N$ (see also [KM85] Section 3.2).

- A $\Gamma_0(N)$-structure over $R$ is a pair $(E, C)$ where $C \subset E[N]$ is a finite flat subgroup scheme over $R$ that is cyclic and locally free of rank $N$ (see also [KM85] Section 3.4).

We denote by $[\Gamma_i(N)]_R$ the set of all isomorphism classes of $\Gamma_i(N)$-structures over $R$. If $(E, \alpha)$ is a $\Gamma_i(N)$-structure (for $i = 0, 1$), we denote the corresponding object of $[\Gamma_i(N)]_R$ by $[E, \alpha]$. When $N = 1$ we will drop the subscript: $[\Gamma(1)]_R = [\Gamma_0(1)]_R = [\Gamma_1(1)]_R$. The $j$-invariant $[\Gamma_1(N)]_R \rightarrow R$ is the map induced by $(E, \alpha) \mapsto j(E)$ on level structures. $j : [\Gamma(1)]_R \rightarrow R$ is a bijection when (e.g.) $R$ is an algebraically closed field.

An isogeny between $\Gamma_i(N)$-structures $(E_1, \alpha_1)$ and $(E_2, \alpha_2)$ over $R$ is an isogeny $\varphi : E_1 \rightarrow E_2$ (defined over $R$) such that $\varphi(\alpha_1) = \alpha_2$. The set $[\Gamma_i(N)]_R$ can be given the structure of a category whose arrows are isomorphism classes of isogenies over $R$ between $\Gamma_i(N)$-structures over $R$. Note that the degree of an isogeny is an isomorphism invariant, so deg is a map from the arrows of $[\Gamma_i(N)]_R$ to $\mathbb{N}$.

When $F$ is an algebraically closed field we define for every $[E, C] \in [\Gamma_0(N)]_F$ the numerical invariant $w([E, C]) = \frac{1}{2} |\text{Aut}(E, C)|$ where $\text{Aut}(E, C)$ is the subgroup of those $u \in \text{Aut}(E)$ such that $u(C) = C$ (this does not depend on the choice of representative). A point $\tau \in [\Gamma_0(N)]_F$ is called elliptic if $w(\tau) > 1$. If $\tau \in [\Gamma_0(N)]_R$ is elliptic, then $j(\tau) \in \{0, 1728\}$.

There are various natural correspondences between moduli of level structures:
There is a projection map \( \pi_N : [\Gamma_1(N)]_R \to [\Gamma_0(N)]_R \) induced by the map \((E, P) \mapsto (E, \langle P \rangle)\) on level structures.

There is an action of \((\mathbb{Z}/N\mathbb{Z})^\times\) on \([\Gamma_1(N)]_R\) via the diamond bracket: If \(a \in (\mathbb{Z}/N\mathbb{Z})^\times\), then \(\langle a \rangle : [\Gamma_1(N)]_R \to [\Gamma_1(N)]_R\) induced by \((E, P) \mapsto (E, aP)\). \(\langle a \rangle\) acts on the fibers of \(\pi_N\); that is,

\[
\begin{array}{ccc}
[\Gamma_1(N)]_R & \xrightarrow{\langle a \rangle} & [\Gamma_1(N)]_R \\
\pi_N & \downarrow & \pi_N \\
[\Gamma_0(N)]_R & &
\end{array}
\]

commutes.

For each \(N' \mid N\) with \(N/N'\) prime we have primitive degeneracy maps \(\delta_{N,N'} : [\Gamma_1(N)]_R \to [\Gamma_1(N')]_R\) and \(\delta_{N,N'} : [\Gamma_1(N)]_R \to [\Gamma_1(N')]_R\) induced by \((E, P) \mapsto (E, \frac{N}{N'}P)\) and \((E, P) \mapsto (E/\langle \frac{N}{N'}P \rangle, P + \langle \frac{N}{N'}P \rangle)\) respectively.

For any divisor \(N' \mid N\), a degeneracy map \(\delta : [\Gamma_1(N)]_R \to [\Gamma_1(N')]_R\) is a composition of primitive degeneracy maps.

We also define for \(N' \mid N\) a standard projection-degeneracy map \(\beta_{N,N'} : [\Gamma_1(N)] \to [\Gamma_0(N')]\) induced by \((E, P) \mapsto (E, \langle \frac{N}{N'} \rangle P)\) on level structures; this is the composition of degeneracy maps of the first kind and the projection \(\pi_N\).

The following innocuous lemma will make an appearance in the proof of Theorem 6.2.1:

**Lemma 1.1.1.** Let \(F\) be an algebraically closed field, let \(N \geq 1\) be an integer, let \(N' \mid N\), and suppose there is an isogeny \(\varphi : \tau \to \tau_0'\) in \([\Gamma_0(N')]_F\) with \(\text{deg}(\varphi) = d\) relatively prime to \(N\). For every \(\tau_0 \in \beta_{N,N'}^{-1}(\tau_0')\) there exists \(\tau \in \beta_{N,N'}^{-1}(\tau')\) and an isogeny \(\psi : \tau \to \tau_0\) of degree \(d\) such that \(\beta_{N,N'} \psi = \varphi \beta_{N,N'}\).

**Proof.** Let \(\varphi : (E, C) \to (E_0, C_0)\) be an isogeny of \(\Gamma_0(N')\)-structures over \(F\) of degree \(d\) prime to \(N\), and let \(e\) be a multiplicative inverse of \(d\) modulo \(N\). Choose \(P_0 \in E(F)\) such that \(\frac{N}{N'} P_0\) generates \(C_0\), and let \(P = \hat{\varphi}(eP_0)\). Because \(d = \text{deg} \varphi\) is relatively prime to \(N\), \(\hat{\varphi}(C_0) = C\) and since \(\frac{N}{N'}P_0\) generates \(C_0\), \(\hat{\varphi}(\frac{N}{N'}eP_0) = \frac{N}{N'}P\) generates \(C\). The diagram

\[
\begin{array}{ccc}
(E, P) & \xrightarrow{\varphi} & (E_0, P_0) \\
\downarrow{\beta_{N,N'}} & & \downarrow{\beta_{N,N'}} \\
(E, C) & \xrightarrow{\varphi} & (E_0, C_0)
\end{array}
\]

commutes, since \(\varphi(P) = \varphi \hat{\varphi}(eP_0) = deP_0 = P_0\). Take \(\psi = \varphi : [E, P] \to [E_0, P_0]\.\)
1.2 Katz modular forms

The modern geometric theory of modular forms has its roots in seminal works of Katz [Kat72], Katz–Mazur [KM85], and Deligne–Rapoport [DR73]. A theory of modular forms in the context of Deligne–Mumford stacks is also available (see Conrad’s paper [Con06]), but Katz’s theory will suffice for us.

Proposition 1.2.1. For \( N \geq 5 \), the functor \( \Gamma_1(N) : \text{Rings}_{\mathbb{Z}[1/N]} \to \text{Sets} : R \mapsto [\Gamma_1(N)]_R \) is representable by a smooth affine curve \( Y_1(N) \) over \( \mathbb{Z}[\frac{1}{N}] \) that is finite and flat over the affine j-line. The normalization of the projective j-line in \( Y_1(N) \) is a smooth proper curve \( X_1(N) \) over \( \mathbb{Z}[\frac{1}{N}] \).

Proof. See [Kat72] Section 1.4, or [KM85].

The scheme \( X_1(N) \setminus Y_1(N) \) is finite and étale over \( \mathbb{Z}[\frac{1}{N}] \) and over \( \mathbb{Z}[\frac{1}{N}, \mu_N] \) it is a disjoint union of sections called the cusps of \( X_1(N) \). These cusps may be interpreted as isomorphism classes of pairs \((\text{Tate}(q), \zeta q^{j/N})\) where \( \text{Tate}(q) = \mathbb{G}_m/q\mathbb{Z} \) is the Tate curve (an elliptic curve over \( \mathbb{Z}((q^{1/N})) \), see [Kat72], section A1.2 or [Sil94] Section V.3), \( \zeta \) is a primitive \( N \)th root of unity, and \( i, j \in [0, N) \) are chosen so that \( \zeta^i q^{j/N} \) has order exactly \( N \). The curve \( X_1(N) \) parametrizes “isomorphism classes of generalized elliptic curves with \( \Gamma_1(N) \)-structure” (see [Con06] or [NP00] (1.1.1)). A cusp is called principal if it corresponds to \((\text{Tate}(q), \zeta)\) for \( \zeta \) a primitive \( N \)th root of unity.

Remark 1.2.2. Over \( \mathbb{C} \), the curve \( X_1(N) \) is isomorphic to \( \Gamma_1(N) \setminus \mathfrak{h}^* \) where the group

\[
\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}
\]

acts on \( \mathfrak{h}^* = \{ \tau \in \mathbb{C} : \text{Im} \tau > 0 \} \cup \mathbb{P}^1(\mathbb{Q}) \) by fractional linear transformations. The cusps of \( X_1(N)_\mathbb{C} \) are the (finitely many) orbits of this action on \( \mathbb{P}^1(\mathbb{Q}) \) (see for example [DI95]).

There is a unique invertible sheaf \( \omega \) on \( X_1(N) \) whose restriction to the open subscheme \( Y_1(N) \) is the pullback along the zero section of the Kähler differentials on the universal \( \Gamma_1(N) \)-structure \( \mathcal{E}_{\Gamma_1(N)}^{\text{univ}}/Y_1(N) \) and whose sections at the completion \( \mathbb{Z}[\frac{1}{N}, \zeta_N][[q^{1/N}]] \) at each cusp are the \( \mathbb{Z}[\frac{1}{N}, \zeta_N][[q^{1/N}]] \)-multiples of \( \omega_{\text{can}} \) (the canonical differential) on the Tate curve. (see [Kat72] Sections 1.5 and A1.2, [KM85] Section 10.13, [Con06] Section 2.5). Let \( \omega^k_R \) denote the \( k \)-fold tensor power of \( \omega \otimes_{\mathbb{Z}[1/N]} R \).

Definition 1.2.3 ([Kat72] Section 1.5). A modular form of weight \( k \) and level \( N \) over \( R \) is a global section of \( \mathcal{O}_R^k \) on \( X_1(N)_R \). The \( R \)-module of such forms is

\[
\mathcal{M}_k(N; R) = H^0(X_1(N)_R; \omega^k_R).
\]

A cusp form of weight \( k \) and level \( N \) over \( R \) is a modular form (of the same type) that vanishes at the cusps of \( X_1(N) \); the submodule of cusp forms is therefore

\[
\mathcal{S}_k(N; R) = H^0(X_1(N)_R; \omega^k_R(\text{-cusps})),
\]

where cusps is the reduced divisor of cusps on \( X_1(N)_R \).
1.3 Test objects and $q$-expansion

Modular forms can be interpreted concretely on $Y_1(N)$ via $\Gamma_1(N)$-test objects: Triples $(E, P, \omega)$ where $(E, P)$ is a $\Gamma_1(N)$-structure and $\omega$ is a nonvanishing differential on $E$. In this context, a modular form of weight $k$ and level $N$ over $R$ is a rule

$$f : \{\Gamma_1(N)\text{-test objects over } R\} \rightarrow R$$

such that

i. The value $f(E, P, \omega)$ depends only on the isomorphism class of the test object,
ii. $f(E, P, u\omega) = u^{-k}f(E, P, \omega)$ for all $u \in R^\times$, and
iii. $f$ commutes with arbitrary extensions of scalars.

See also for example [Kat72] Section 1.1 or [Gor02] Section 4.3.1.

Let $R$ be a $\mathbb{Z}[\frac{1}{N}, \mu_N]$-algebra, let $c$ be a cusp of $X_1(N) \subset R$, and let $(\text{Tate}(q), \zeta^iq^{j/N})$ be a $\Gamma_1(N)$-structure on the Tate curve corresponding to $c$. By evaluating $f$ at the $\Gamma_1(N)$-test object $(\text{Tate}(q), \zeta^iq^{j/N}, \omega_{\text{can}})$ over $R \otimes \mathbb{Z}[[q^{1/N}]]$, we obtain a power series $f^c(q^{1/N}) \in R \otimes \mathbb{Z}[[q^{1/N}]]$ called the $q$-expansion of $f$ at $c$ ([Kat72] 1.2). If $c$ is a cusp of $X_1(N)$ we denote by $a^c_{n/N}(f)$ the coefficient of $q^{n/N}$ in the $q$-expansion of $f$ at $c$.

**Proposition 1.3.1** ([Kat72] Corollary 1.6.2). Suppose that $A \subset R$ is a subring that is a $\mathbb{Z}[[\frac{1}{N}]]$-module and let $f \in M_k(N; R)$. If there exists a cusp $c$ such that $f^c(q) \in A \otimes \mathbb{Z}[[q^{1/N}]]$, then $f \in M_k(N; A)$.

**Proof.** This is Corollary 1.6.2 in [Kat72].

If $c$ corresponds to $(\text{Tate}(q), \zeta^iq^{j/N})$ we denote by $e(c) = \frac{N}{\gcd(j,N)}$ the width of the cusp $c$. Note that $q$-expansion at $c$ is actually a map $M_k(N; R) \rightarrow R \otimes \mathbb{Z}[[q^{1/e(c)}]]$. A cusp $c$ is principal if and only if $e(c) = 1$ and so the $q$-expansion of a modular form at a principal cusp lies in $R \otimes \mathbb{Z}[[q]]$.

1.4 Basic structure theory of modular forms

Let $N \geq 5$ and let $R$ be a $\mathbb{Z}[\frac{1}{N}]$-algebra. In this section we collect a number of standard results about the structure of the $R$-module $M_k(N; R)$.

The line bundle $\omega_R^k$ has degree $d_k(N) = \frac{k}{24}[\text{SL}_2(\mathbb{Z}) : \Gamma_1(N)]$ where $\Gamma_1(N)$ is the group defined in Example 1.2.2. This observation has the following consequences:

**Proposition 1.4.1.**

a. At each cusp $c$ the map

$$M_k(N; R) \rightarrow R \otimes \mathbb{Z}[[q^{1/e(c)}]]/(q^{(d_k(N)+1)/e(c)} : f \mapsto f^c(q^{1/N}) \mod q^{(d_k(N)+1)/e(c)}$$

is injective. A fortiori, $q$-expansion at each cusp is injective.

b. If $F$ is a field, then $M_k(N; F)$ is a finite-dimensional $F$-vector space.

When $k \geq 2$, there are formulas for $\dim M_k(N; F)$ (see [Ste07] Chapter 6).
c. If $F$ is algebraically closed field, $\sum_{\tau \in X_1(N) F} \ord_{\tau}(f) = d_k(N)$

**Remark 1.4.2.** Our knowledge of weight 1 modular forms is so limited that there is no general formula for computing $\dim_{\mathbb{C}} M_1(N; \mathbb{C})$. Currently, our best estimates rely mostly on lower bounds coming from the space of **dihedral forms** (see [BG09] for instance).

For every $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, the correspondence $\langle a \rangle : [\Gamma_1(N)]_R \to [\Gamma_1(N)]_R$ induces an automorphism $X_1(N) \to X_1(N)$ with the interpretation $(Tate(q), \zeta^i q^{j/2N}) \mapsto (Tate(q), \zeta^{ai} q^{aj/2N})$ at the cusps. Note that in particular $c(\langle a \rangle c) = c(c)$.

Each of the diamond correspondences pulls back to a **diamond operator** $\langle a \rangle^* : M_k(N; R) \to M_k(N; R)$. On test objects, we have $(\langle a \rangle^* f)(E, P, \omega) = f(E, aP, \omega)$.

The diamond operators comprise a commuting family of linear operators on $M_k(N; R)$. A modular form $f \in M_k(N; R)$ is a simultaneous eigenform for these operators if and only if there exists a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{R}^\times$ such that $\langle a \rangle^* f = \chi(a)f$ for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$; in such a case we say that $\chi$ is the **character** (or **nebentypus**) of $f$. We denote by $M_k(N, \chi; R)$ the submodule of $M_k(N; R)$ consisting of all forms of character $\chi$.

Note that if $f \in M_k(N, \chi; R)$ for some character $\chi$ and $\tau \in X_1(N)_R$, then $\ord_{\tau}(f) = \ord_{\langle a \rangle^* \tau}(f)$.

**Proposition 1.4.3.** If $R$ is a $\mathbb{Z}[\frac{1}{N}, \mu_{\phi(N)}]$-algebra, then

$$M_k(N; R) = \bigoplus_{\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{R}^\times, \chi(-1) = (-1)^k} M_k(N, \chi; R)$$

**Proof.** This is standard, see [DS05] Section 4.3 or [RS11] Section 8.2. \qed

The above decomposition allows us to attend to the spaces $M_k(N, \chi; R)$ individually, rather than to the whole space $M_k(N; R)$ at once. Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

and let $\text{Sturm}_k(N) = \frac{k}{12}[\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)] + 1$. Note that $\text{Sturm}_k(N) - 1 = \frac{2d_k(N)}{\phi(N)}$, so $\text{Sturm}_k(N)$ is significantly smaller than $d_k(N)$.

**Proposition 1.4.4.** Let $N \geq 5$, let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{R}^\times$ satisfy $\chi(-1) = (-1)^k$, and let $c \in X_1(N)_R$ be a cusp. The map

$$M_k(N, \chi; R) \to R \otimes \mathbb{Z}[[q^{1/\epsilon(c)}]]/(q^{\text{Sturm}_k(N)/\epsilon(c)}) : f \mapsto f^c(q) \mod q^{\text{Sturm}_k(N)/\epsilon(c)}$$

induced by $q$-expansion at $c$ is injective.

**Proof.** See Section 3.3 of [Kil08] or W. Stein’s remark in the documentation for the `sturm_bound` command for generic spaces of modular forms in SAGE [SAGE]. \qed
If \( N' \mid N \), a degeneracy map \( \delta : [\Gamma_1(N)]_R \to [\Gamma_1(N')]_R \) gives rise to a morphism \( \delta : X_1(N) \to X_1(N') \) that pulls back to an embedding \( \delta^* : M_k(N'; R) \hookrightarrow M_k(N; R) \). The oldforms of \( M_k(N; R) \) are elements of the submodule generated by \( \{ \delta^* M_k(N'; R) \} _{N', \delta} \) as \( N' \) ranges over all divisors of \( N \) and \( \delta \) ranges over all degeneracies \( \delta : X_1(N) \to X_1(N') \).

It is also occasionally useful to treat \( M(N; R) = \bigoplus_{k \geq 0} M_k(N; R) \) as an \( R \)-algebra graded by weight. This allows us to multiply modular forms, so long as we keep track of the weight.

1.5 Base change and mod \( p \) modular forms

Our central goal is to describe weight 1 modular forms both in the classical setting (over \( \mathbb{C} \)) and over finite fields, so we must be able to treat these settings on equal footing.

**Proposition 1.5.1.** Let \( R \) be a \( \mathbb{Z}[[\frac{1}{N}]] \)-algebra and let \( S \) be an \( R \)-algebra. If \( k \geq 2 \) or \( S/R \) is flat, the canonical map \( M_k(N; R) \otimes_R S \to M_k(N; S) \) is an isomorphism.

**Proof.** Part of this is Theorem 1.7.1 in [Kat72], with the whole claim appearing as Theorem 12.3.2 in [DI95].

**Corollary 1.5.2.** Let \( p \subset R \) be a prime ideal. For each cusp \( c \) of \( X_1(N) \) the diagram

\[
\begin{array}{ccc}
M_k(N; R) & \xrightarrow{f \mapsto f'(q)} & R \otimes \mathbb{Z}[q^{1/N}] \\
& \downarrow & \\
M_k(N; R) \otimes R/p & \xrightarrow{f \mapsto f'(q)(R/p)} & (R/p) \otimes \mathbb{Z}[q^{1/N}] \\
& \downarrow & \\
M_k(N; R/p) & \xrightarrow{f \mapsto f'(q)(R/p)} & (R/p) \otimes \mathbb{Z}[q^{1/N}] 
\end{array}
\]

commutes and the map \( M_k(N; R) \to M_k(N; R/p) \) is surjective provided that \( k \geq 2 \).

The omission of \( k = 1 \) in the above hints at an important issue in the study of weight 1 modular forms. In Section 8 we will show that while reduction \( M_1(N; \mathbb{Z}[[\frac{1}{N}]]) \to M_1(N; \mathbb{F}_p) \) is surjective for almost all primes \( p \), there are indeed cases where surjectivity fails. This means that spaces of weight 1 modular forms mod \( p \) must be computed directly, whereas in weights \( k \geq 2 \) it is sufficient to compute a suitable basis for \( M_k(N; \mathbb{Z}[[\frac{1}{N}]] \) and then reduce.

1.6 Level 1 modular forms and weight 1 Eisenstein series

There are various explicitly constructed modular forms that are invaluable tools for computation. Most relevant to us are the modular forms of level 1 and the primitive weight 1 Eisenstein series with character.
Modular forms of level 1 over \( \mathbb{C} \) are the first nontrivial examples of modular forms one encounters in a course on the subject. Since the projective \( j \)-line \( X(1) \) is not representable, these forms do not a priori fit into the picture of Katz modular forms we sketched in Section 1.2. However, because of the degeneracy maps \([\Gamma_1(N)]_R \rightarrow [\Gamma(1)]_R\), these forms are present at every level \( N \geq 5 \).

**Remark 1.6.1.** We will refrain from constructing the Eisenstein subspace of \( M_k(N; R) \), because it is not entirely clear how this should be done over an arbitrary ring \( R \). For a thorough explanation of Eisenstein series over \( \mathbb{C} \) see [DS05] Chapter 4, and for an explanation of how such objects should be interpreted on moduli see [Khu09].

**Definition 1.6.2.** An element \( f \in M_k(N; R) \) is said to be of level 1 if the value of \( f \) on a test object \( (E, P, \omega) \) does not depend on the point \( P \).

**Proposition 1.6.3.** For every even \( k \geq 4 \) there is a level 1 modular form \( G_k \in M_k(N; R) \) whose \( q \)-expansion at any principal cusp \( c \) is

\[
G_k^c(q) = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sum_{m \mid n} m^{k-1} q^n \in \mathbb{Z}[q],
\]

where \( B_k \) is the \( k \)th Bernoulli number.

The weight \( k \) level 1 modular forms are those forms that lie in the intersection of \( M_k(N; R) \) and the graded subring of \( M(N; R) \) generated by \( G_4 \) and \( G_6 \).

**Proof.** Standard (see for example [Ste07] Chapter 2).

**Proposition 1.6.4.** The image \( \tilde{G}_{p-1} \in M_{p-1}(N; \mathbb{F}_p) \) of \( G_{p-1} \) is the Hasse invariant.

1. \( \tilde{G}_{p-1} \) has a simple zero at every supersingular point of \( X_1(N)_F \) (all those \( [E, P] \in X_1(N) \) such that \( E \) a supersingular curve).

2. \( (\tilde{G}_{p-1})^c(q) = 1 \) at every cusp \( c \in X_1(N)_F \). In fact, the kernel of \( q \)-expansion \( M(N; \mathbb{F}_p) \rightarrow \mathbb{F}_p \otimes \mathbb{Z}[[q^{1/N}]] \) is generated by \( 1 - \tilde{G}_{p-1} \).

**Proof.** See for example [Gor02] Section 4.5.1.

The Hecke stability method we will describe in Chapter III relies on the existence of forms \( \lambda \in M_1(N, \chi^{-1}; F) \) that can be easily computed. Below we construct the **primitive weight 1 Eisenstein series** associated to a character. These will typically serve as our auxiliary forms in the implementation of the Hecke stability method.

**Lemma 1.6.5.** Let \( N \geq 5 \), let \( F = \mathbb{C} \) or \( F = \mathbb{F}_p \) with \( p \nmid 2N \), and let \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow F^\times \) be an odd\(^1\) character. Let \( \chi' : (\mathbb{Z}/f_N \mathbb{Z})^\times \rightarrow F^\times \) be the primitive character that induces \( \chi \) and define \( L_x \in F \) by

\[
L_x = -\sum_{r=0}^{f_N-1} \chi'(r) \left( \frac{r}{f_N^{-1}} - \frac{1}{2} \right).
\]

\(^1\)Odd meaning \( \chi(-1) = -1 \).
Fix a principal cusp \( \mathfrak{c} \). There is a unique modular form \( \lambda_\chi \in \mathcal{M}_1(N, \chi^{-1}; F) \) such that

\[
\lambda_\chi(q) = L_\chi + 2 \sum_{n=1}^{\infty} \sum_{m | n} \chi'(m)q^n.
\]

**Proof.** The construction over \( F = \mathbb{C} \) is standard, see [DS05] Section 4.8.

It remains to treat the case \( F = \bar{\mathbb{F}}_p \). Let \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \bar{\mathbb{F}}_p^\times \) be an odd primitive character, let \( r \) be the degree of \( \mathbb{F}_p(\chi)/\mathbb{F}_p \), and let \( K = \mathbb{Q}(\zeta_{p^r-1}) \). If \( \mathfrak{p} \) is a prime of \( K \) above \( p \), then \( \mathbb{F}_p \cong \mathbb{F}_p(\chi) \) and reduction modulo \( \mathfrak{p} \) sends \( \zeta_{p^r-1} \) to a generator of \( \mathbb{F}_p^\times \). Pulling \( \chi \) back along \( K^\times \rightarrow \mathbb{F}_p^\times \cong \mathbb{F}_p(\chi) \) yields a character (odd and primitive) \( \hat{\chi} : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow K^\times \hookrightarrow \mathbb{C}^\times \); this character reduces to \( \chi \) modulo \( \mathfrak{p} \).

Let \( \lambda_{\hat{\chi}} \) be the element of \( \mathcal{M}_1(N, \hat{\chi}^{-1}; K) \subset \mathcal{M}_1(N, \hat{\chi}^{-1}; \mathbb{C}) \) obtained as above. By Lemma 1.5.1, the reduction \( \lambda_\chi \) of \( \lambda_{\hat{\chi}} \) modulo \( \mathfrak{p} \) has the desired \( q \)-expansion. \( \square \)

**Example 1.6.6.** Let \( F \) be an algebraically closed field that admits an inverse of \( 6N \). If \( N \) is prime and \( \chi \) has conductor \( N \), we have the following moduli interpretation of \( \lambda_\chi \) (see [Khu09]): There is a constant \( c \in F \) such that for every \( \Gamma_1(N) \)-test object \( (E, P, \omega) \) over \( F \),

\[
\lambda_\chi(E, P, \omega) = c \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(d)t(dP)
\]

where \( t(dP) \) is the slope of the tangent line to \( E \) at \( dP \) on the Weierstrass model

\[
E : Y^2 = X^3 + G_4(E, \omega)X + G_6(E, \omega).
\]

**Lemma 1.6.7.** Let \( N \geq 5 \), let \( F = \mathbb{C} \) or \( F = \bar{\mathbb{F}}_p \) with \( p \nmid 2N \), and let \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow F^\times \) be an odd character. Suppose we have a factorization \( \chi = \chi_1\chi_2 \). Let \( \chi'_1 \) and \( \chi'_2 \) be the primitive characters that induce \( \chi_1 \) and \( \chi_2 \).

Fix a principal cusp \( \mathfrak{c} \). There exists a unique \( \lambda_{\chi_1, \chi_2} \in \mathcal{M}_1(N, \chi^{-1}; F) \) such that

\[
\lambda_{\chi_1, \chi_2}(q) = \sum_{n=1}^{\infty} \sum_{m | n} \chi'_1(m)\chi'_2(n/m)^{-1}q^n.
\]

**Proof.** Similar to the preceding lemma. \( \square \)

### 1.7 Fractional modular forms

Ultimately, our goal is to compute spaces of weight 1 modular forms, but these spaces are rather difficult to handle directly. Instead, our strategy will be to embed the target space, \( \mathcal{M}_1(N, \chi; F) \) with \( F \) a field say, into a space of “fractional modular forms.”

That is to say, once we have constructed a nonempty finite subset \( A \subset \mathcal{M}_1(N, \chi^{-1}; F) \) \( \setminus \{0\} \) of auxiliary forms (consisting of primitive Eisenstein series, for example) we obtain an inclusion

\[
\mathcal{M}_1(N, \chi; F) \subset \bigcap_{\lambda \in A} \lambda^{-1}\mathcal{M}_2(N, 1; F).
\]
Elements of the right hand side are \textit{not necessarily} modular forms: They may have poles where the auxiliary forms in $A$ simultaneously vanish.

We have a second inclusion $\bigcap_{\lambda \in A} \lambda^{-1} M_2(N; F) \subset M_1^{\text{frac}}(N, \chi; F)$, and much of the machinery of modular forms (e.g., $q$-expansion and Hecke operators) can be interpreted in the ambient space $M_1^{\text{frac}}(N, \chi; F)$ of weight 1 level $N$ fractional modular forms. We propose to use this machinery to isolate the the subspace the machinery of modular forms (e.g., Definition 1.7.1.

For each $X$ a field that admits an inverse of $1$ fraction $\frac{k}{1}$ interpreted in the ambient space $M_1^{\text{frac}}(N, \chi; F)$. Such an $M_1^{\text{frac}}(N, \chi; F)$ embeds into $M_1^{\text{frac}}(N, \chi; F)$ as the finite-dimensional subspace consisting of those $f \in M_1^{\text{frac}}(N, \chi; F)$ that have poles nowhere on $X_1(N)_F$.

Formally, we define the space of fractional modular forms as follows: Let $F$ be a field that admits an inverse of $N$, and let $K$ be the sheaf of rational functions on $X_1(N)_F$.

**Definition 1.7.1.** A fractional modular form of weight $k$ and level $N$ over $F$ is a global section of the sheaf $\omega_F^k \otimes K$ on $X_1(N)_F$:

$$M_1^{\text{frac}}(N; F) = H^0(X_1(N)_F, \omega_F^k \otimes K).$$

Here are some basic facts and definitions concerning fractional modular forms:

- $M_k^{\text{frac}}(N; F)$ is an $F$-vector space, though it is certainly not finite-dimensional. $M_k(N; F)$ embeds into $M_k^{\text{frac}}(N; F)$ as the finite-dimensional subspace consisting of those $f \in M_k^{\text{frac}}(N; F)$ that have poles nowhere on $X_1(N)_F$.

- For each $j \geq 0$ we have a map

$$M_{k+j}(N; F) \times M_j(N; F) \setminus \{0\} \longrightarrow M_k^{\text{frac}}(N; F); (g, h) \mapsto g/h,$$

and the disjoint union of these maps is surjective: That is, for every $f \in M_k^{\text{frac}}(N; F)$, there exists $j \geq 0$ and $h \in M_j(N; F)$ such that $hf \in M_{k+j}(N; F)$ (see for example Proposition 1.7.3 below). Such an $h$ is called a denominator of $f$.

- For each $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times$ we define $M_k^{\text{frac}}(N, \chi; F)$ to be the subspace of $M_k^{\text{frac}}(N; F)$ such that $\langle a \rangle^t f = \chi(a)f$ for every $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.

- For a fixed $h \in M_j(N; F)$ and $V \subset M_{k+j}(N; F)$, we denote the image of

$$V \rightarrow M_k^{\text{frac}}(N; F) : g \mapsto g/h \text{ by } h^{-1}V .$$

Note that if $h \in M_j(N, \theta; F)$, then $h^{-1}M_k(N, \chi; F) \subset M_k^{\text{frac}}(N, \theta^{-1}\chi; F)$.

- The $q$-expansion maps extend to $M_k^{\text{frac}}(N; F)$ exactly as one would expect, with the $q$-expansion map at a cusp $c \in X_1(N)_F$ being an injection

$$M_k^{\text{frac}}(N; F) \longrightarrow F(\mu_N) \otimes \mathbb{Z}((q^{1/N})).$$

If $f \in M_k^{\text{frac}}(N; F)$ satisfies $f = g/h$ for modular forms $g, h$, then at each cusp $c$ we have $f^c(q) = g^c(q)/h^c(q)$. 

10
Example 1.7.2. The fractional modular form of weight 0 (the modular function) $1728G_4^3/(G_4^3 - G_6^2)$ is the $j$-invariant in the sense that for every $\tau \in X_1(N)_F$, $\tau$ is represented by a $\Gamma_1(N)$-structure $(E, P)$ (defined over $R$) if and only if

$$j(E) = \frac{1728G_4(\tau)^3}{G_4(\tau)^3 - G_6(\tau)^2},$$

and $\tau$ is cuspidal if and only if $j$ has a pole at $\tau$.

We will rely on this formula in Section 3.3 to devise an algorithm for computing the projection of the zero set of a modular form to the $j$-line.

Proposition 1.7.3. Every fractional modular form has a denominator of level 1.

Proof. The level 1 form $\Delta$ is zero at every cusp of $X_1(N)$. If $\tau$ is a moduli point, then the level 1 form $(1728 - j(\tau))G_4^3 + j(\tau)G_6^2$ vanishes at $\tau$. The claim follows because a product of level 1 modular forms is easily seen to be a level 1 modular form. 

2 Hecke operators

The Hecke operators are a distinguished commutative family of endomorphisms of $M_k(N; R)$. The spectral theory of these operators provides the bridge between modular forms and Galois representations (see Theorems 2.4.1 and 2.4.2 below).

Throughout this section we will assume for simplicity that $F$ is an algebraically closed field. The action of the Hecke operator $T_\ell$ can be interpreted as follows: The value of $T_\ell f$ at a moduli point $[E, P] \in X_1(N)_F$ is (roughly speaking) the average of $f$ over those points $[E', P'] \in X_1(N)_F$ that are $\ell$-isogenous to $[E, P]$.

2.1 Hecke correspondences on moduli

Let $\ell$ be a prime that is not the characteristic of $F$. A $\Gamma_1(N; \ell)$-structure over $F$ is a triple $(E, P; H)$ where $(E, P)$ is a $\Gamma_1(N)$-structure over $F$ and $H$ is a subgroup of $E$ of order $\ell$ such that $P \notin H$. We denote by $[\Gamma_1(N; \ell)]_F$ the set of isomorphism classes of $\Gamma_1(N; \ell)$-structures over $F$. We have maps

$$\begin{array}{ccc}
[\Gamma_1(N; \ell)]_F & \xrightarrow{\gamma_1} & [\Gamma_1(N)]_F \\
& \downarrow & \\
[\Gamma_1(N)]_F & \xrightarrow{\gamma_2} & [\Gamma_1(N)]_F
\end{array}$$

where $\gamma_1$ and $\gamma_2$ are induced by the maps $(E, P; H) \mapsto (E, P)$ and $(E, P; H) \mapsto (E/H, P + H)$ on level structures, respectively.

The $\ell$th Hecke correspondence is the map $\text{Hecke}_\ell = \gamma_2 \gamma_1^* : \text{Div}[\Gamma_1(N)]_F \to \text{Div}[\Gamma_1(N)]_F$. It is therefore induced by $(E, P) \mapsto \sum_H (E/H, P + H)$ where the sum ranges over all cyclic $H \subset E[\ell]$ of order $\ell$ such that $P \notin H$.
Now let \([E, C] \in [\Gamma_0(N)]_F\) and let \([E, P] \in \pi_N^{-1}([E, C])\) (so that \(P\) generates \(C\)). We define \(\text{Hecke}_\ell([E, C]) = \pi_N \ast \text{Hecke}_\ell([E, P])\), and one easily checks that this does not depend on the choice of generator \(P \in C\). This yields a Hecke correspondence \(\text{Hecke}_\ell : \text{Div}[\Gamma_0(N)]_F \to [\Gamma_0(N)]_F\). When we need to differentiate between this correspondence and the correspondence on \(\Gamma_1(N)\)-structures, we denote them by \(\text{Hecke}_0^\ell\) and \(\text{Hecke}_1^\ell\), respectively.

**Example 2.1.1.** Let \(F = \mathbb{C}\) or \(F = \overline{\mathbb{F}}_p\). For every prime \(\ell\) that is not the characteristic of \(F\), there is a polynomial called the **modular polynomial** \(\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]\) such that for every \(j_1 \in F\),

\[
\Phi_\ell(j_1, Y) = \prod_{j_2 \in F} (Y - j_2)^{|\{H \subset E_{j_1}, H \text{ cyclic of order } \ell, E_{j_1}/H \cong E_{j_2}\}|}
\]

where \(E_{j_0}\) denotes an elliptic curve with \(j\)-invariant \(j_0\). Thus, \(\Phi_\ell\) “cuts out” the correspondence \(\text{Hecke}_\ell\) on \([\Gamma(1)]_C\) in the sense that

\[
\text{Hecke}_\ell([E_{j_1}]) = \sum_{j_2 \in C} v_{(Y-j_2)}(\Phi_\ell(j_1, Y))[E_{j_2}].
\]

For instance,

\[
\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + Y^2X) - 162000(X^2 + Y^2) + 40773375XY + 8748000000(X + Y) - 157464000000000,
\]

We have \(\Phi_2(0, Y) = (Y - 54000)^3\), so the elliptic curve \(E_0\) is 2-isogenous to a unique curve (up to isomorphism), the curve \(E_{54000}\) and there are three isogenies \(E_0 \to E_{54000}\). Thus, for every cyclic subgroup \(H \subset E_0(F)\) of order 2, \(E_0/H\) is isomorphic to \(E_{54000}\).

On the other hand, we have \(\Phi_2(54000, Y) = Y(Y^2 - 2835810000Y + 6549518250000)\), so there is one 2-isogeny \(E_{54000} \to E_0\), and \(E_{54000}\) is also 2-isogenous to the curves with \(j\)-invariants \(1417905000 \pm 818626500\sqrt{3}\).

We therefore have the following diagram of 2-isogenies among elliptic curves over \(\mathbb{C}\) near \(E_0\) (labeled with \(j\)-invariants):

![Figure. 2-isogenies near \(j = 0\).](Image)

For algorithms to compute \(\Phi_\ell\) in general, see [Cox89] section 13.B or [LC04].
2.2 Hecke operators on (fractional) modular forms

For $N \geq 5$, the functor $[\Gamma_1(N; \ell)]$ is representable by a smooth affine curve $Y_1(N; \ell)$ and the maps $\gamma_1, \gamma_2 : Y_1(N; \ell) \to Y_1(N)$ are étale. The normalization of the projective line in $Y_1(N; \ell)$ is a smooth proper curve $X_1(N; \ell)$ (see [NP00] 1.2.4), so we have a diagram

$$
\begin{array}{ccc}
X_1(N; \ell) & \xrightarrow{\gamma_1} & Y_1(N) \\
\downarrow \gamma_2 & & \downarrow \\
X_1(N) & &
\end{array}
$$

with the Hecke correspondence on $X_1(N)$ being the map obtained by pulling back the arrow on the left and then following the arrow on the right.

The $\ell$th Hecke correspondence on moduli induces an operator on fractional modular forms of weight $k$ level $N$, the $\ell$th Hecke operator:

$$T_\ell = \text{Hecke}_\ell^* : M_k^{\text{frac}}(N; F) \to M_k^{\text{frac}}(N; F).$$

It is clear immediately from the definitions that $T_\ell$ restricts to an operator on $M_k(N; F)$.

Lemma 2.2.1. Suppose that $\ell \neq \text{char } F$ and $\ell \nmid N$. If $h \in M_j(N; F)$ is a denominator for $f \in M_k^{\text{frac}}(N; F)$, then $T_\ell f$ has a denominator of weight $(\ell + 1)j$.

Proof. Let $Q_\ell : M_j(N; F) \to M_{(\ell+1)j}(N; F)$ be the map given on moduli by

$$(Q_\ell f)([E, P]) = \prod_H f([E/H, P + H]),$$

where $H$ ranges over the cyclic subgroups of $E[\ell]$ of order $\ell$ ($Q_\ell$ is a sort of “multiplicative Hecke operator”). If $h$ is a denominator for $f$, then $Q_\ell h$ is a denominator for $T_\ell f$, and it is clear from the interpretation on test objects that $Q_\ell h$ has weight $(\ell + 1)j$ where $j$ is the weight of $h$. \qed

Lemma 2.2.2. Let $f \in M_k^{\text{frac}}(N; F)$, let $\tau \in Y_1(N)_F$, and suppose that $\text{Hecke}_\ell(\tau) = \sum_i[\tau_i]$. We have

$$\text{ord}_\tau(T_\ell f) \geq \min_i \text{ord}_{\tau_i}(f)$$

with equality holding if there is a unique index $i$ for which $\text{ord}_{\tau_i}(f)$ attains this minimum.

Proof. By definition, $T_\ell = \gamma_1^* \gamma_2^*$. The morphisms $\gamma_1, \gamma_2 : Y_1(N; \ell) \to Y_1(N)$ are étale, hence unramified. It follows that $\gamma_2$ pulls uniformizers at points on $Y_1(N)$ back to uniformizers at points on $Y_1(N; \ell)$.

For any $\tau' \in Y_1(N; \ell)_F$ we have $\text{ord}_{\gamma_2(\tau)}(f) = \text{ord}_{\tau'}(\gamma_2^* f)$. Let $g = \gamma_2^* f$, $\tau \in Y_1(N)_F$, and $\gamma_1^*(\tau) = \sum_i[\tau_i]$ with $\gamma_2(\tau_i) = \tau_i$. Let $z_i$ be a uniformizer at $\tau_i$, let $z$ be a uniformizer at $\tau$, and let $n = -\min_i \text{ord}_{\tau_i}(g)$. Multiplication by $z^n$ at $\tau$ has the same
effect as simultaneous multiplication by $\gamma_i^*$ at each $\tau_i$, and thus, we may assume that $\min_i \text{ord}_{\gamma_i}(g) = \min_i \text{ord}_\tau(f) = 0$. The claim reduces to the following: If $g$ is regular at each $\tau_i$, then $\gamma_i g$ is regular at $\tau$, and if moreover $g$ is nonzero at $\tau_i$ for a unique index $i$, then $\gamma_i g$ is nonzero at $\tau$. The claim now follows from the definition of the push-forward.

Corollary 2.2.3. Let $f \in M_k^\text{frac}(N; F)$, let $\tau \in Y_1(N)_F$, and suppose that Hecke\(_\ell\)(\(\tau\)) = $\sum_i [\tau_i]$. If there is a unique index $i$ such that $f$ has a pole at $\tau_i$, then $T\ell f$ has a pole at $\tau$.

Colloquially, suppose $\tau \in Y_1(N)_F$ and let $\{\tau_i\}_i$ be the collection of all $\ell$-isogenies with domain $\tau$. If there is a unique $i$ such that $f$ has a pole at $\tau_i$, then $T\ell f$ has a pole at $\tau$. In short, this is because $T\ell f$ at $\tau$ averages the values of $f$ at the points $\tau_i$, and if exactly one of these values is a pole, the average must also be a pole. This “pole propagation” property of $T\ell$ is central to the proof of Theorem 6.2.1.

Proposition 2.2.4. For all primes $\ell$ that are invertible in $F$, $T\ell(\langle a \rangle) = \langle a \rangle T\ell$. In particular, for all $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times$, $T\ell$ restricts to an operator on $M_k^\text{frac}(N, \chi; F)$.

Proof. Standard, see [DS05] Proposition 5.2.4. □

The correspondence Hecke\(_n\) and the operator $T_n$ can be defined for arbitrary values of $n$ in a similar fashion, though we will exclusively rely on the operators $T_\ell$ for $\ell$ prime. For any subring $R \subset F$, the $R$-algebra generated by $\{T_n\}_n$ is denoted $\mathbb{T}(N; R)$.

2.3 Hecke correspondences on $q$-expansions

The theory of $q$-expansions allows us to treat fractional modular forms as concrete objects (Laurent series), and this is invaluable from a computation point of view. The Hecke operators can be interpreted on $q$-expansions, and ultimately, this is what will allow us to implement the Hecke stability method of Chapter III.

Proposition 2.3.1. If $\ell \nmid N$ and $f \in M_k^\text{frac}(N, \chi; F)$, then at any cusp $c$ of $X_1(N)$ we have the formula

$$(T\ell f)^c(q^{1/N}) = \sum_{n \in \mathbb{Z}} a_{\ell n/N}(f) q^{n/N} + \chi(\ell) \ell^{k-1} \sum_{n \in \mathbb{Z}} a_{n/N}(f) q^{kn/N}.$$

Proof. The proof is identical to that of Formula 1.11.1 in [Kat72]. □

Simply by inspecting the formula above, we can derive several corollaries:

Corollary 2.3.2. The operator $T_\ell : M_k(N; F) \to M_k(N; F)$ restricts to an operator on cusp forms.

Corollary 2.3.3. For any cusp $c \in X_1(N)_R$, $T_\ell$ restricts to an operator on

$$\{ f \in M_k^\text{frac}(N; F) : f^c(q) \in R \otimes \mathbb{Z}[[q^{1/N}]] \}.$$
Corollary 2.3.4. If $\text{ord}_c(f) < 0$ (and $\ell \nmid N$), then $\text{ord}_c(T_\ell f) = \ell \text{ord}_c(f)$.

Corollary 2.3.5. Let $V$ be a finite-dimensional subspace of $M_k^\text{frac}(N; F)$ that is stable under the action of $T_\ell$. For all $f \in V$ and all cusps $c \in X_1(N)_F$, we have $\text{ord}_c(f) \geq 0$.

Proof. If $\text{ord}_c(f) < 0$, then by the preceding corollary we have $\text{ord}_c(T_\ell^r f) = \ell^r \text{ord}_c(f)$ for all $r \geq 0$, so the span of $\{T_\ell^r f\}_{r \geq 0}$ is not finite-dimensional. \qed

2.4 Hecke eigenforms and Galois representations

A modular form $f \in M_k(N, \chi; R)$ is called a Hecke eigenform if it is a simultaneous eigenform for all $T_\ell$ with $\ell \nmid N$. Because $M_k(N; F)$ is finite-dimensional and the operators $\{T_\ell\}_{\ell \mid N}$ commute amongst each other, $M_k(N; F)$ has a basis of Hecke eigenforms (we are assuming that $F$ is algebraically closed). A Hecke eigenform that is not an oldform is called a newform.

If $f \in M_k(N; F)$ is a Hecke eigenform, we use $a(f; T_\ell)$ to denote the $T_\ell$-eigenvalue of $f$. If $f$ is a newform, there is a cusp $c$ such that $a_\ell^c(f) = a(f; T_\ell)$ for all $\ell \nmid N$.

Theorem 2.4.1. Let $f \in M_k(N, \chi; \overline{\mathbb{F}}_p)$ be a newform. There exists a continuous semisimple representation

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\overline{\mathbb{F}}_p)$$

unramified outside $Np$, such that for all $\ell \nmid Np$ and any Frobenius $\sigma_\ell$ above $\ell$ we have

$$\text{tr} \rho_f(\sigma_\ell) = a(f; T_\ell) \quad \text{and} \quad \text{det} \rho_f(\sigma_\ell) = \chi(\ell)\ell^{k-1}.$$

Furthermore, this representation is irreducible only if $f$ is a cusp form.

Proof. This is quoted as Theorem 6.1 in [DS74] in the context of $p$-adic representations (rather than mod $p$ representations) associated to newforms of weight $k \geq 2$. In short, one obtains the above by reduction to the residue field and (in the case of $k = 1$) multiplication by the Hasse invariant (see Proposition 1.6.4). \qed

A converse to this theorem was conjectured by Serre and proven recently by Khare and Wintenberger in [KW09]:

Theorem 2.4.2 (Khare–Wintenberger). Let $F$ be a finite field. A representation $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(F)$ is said to be of Serre type if it is continuous, absolutely irreducible, 2-dimensional, and odd (the determinant of an image of a complex conjugation is $-1$). Let $N(\rho)$ and $k(\rho)$ be defined as in [Kha07].

Denote by $p$ the characteristic of $F$. If $p > 2$ and $N(\rho)$ is odd, then there is a newform $f \in S_{k(\rho)}(N(\rho), \det \rho; F)$ such that $\rho = \rho_f$ (with notation as in the last theorem).

An unusual feature of the weight 1 case is that the projective representations over $\overline{\mathbb{F}}_p$ arising from spaces of weight 1 cusp forms are unramified at $p$:
Theorem 2.4.3 (Coleman–Voloch, [CV92]). Assume the notation of the preceding theorem. If \( k = 1 \) and \( p > 2 \), then the projective representation \( \tilde{\rho}_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{PGL}_2(\overline{\mathbb{F}}_p) \) is unramified at \( p \).

For weight 1 forms over \( \mathbb{C} \) we also have the following:

Theorem 2.4.4 (Deligne–Serre, [DS74]). Let \( f \in M_1(N, \chi; \mathbb{C}) \) be a newform. There exists a continuous representation \( \rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{C}) \) unramified outside \( N \), such that for all \( \ell \nmid N \) and any Frobenius \( \sigma_\ell \) above \( \ell \) we have
\[
\text{tr} \rho_f(\sigma_\ell) = a(f; T_\ell) \quad \text{and} \quad \det \rho_f(\sigma_\ell) = \chi(\ell).
\]
Furthermore, this representation is irreducible if and only if \( f \) is a cusp form.

The Deligne–Serre theorem is central to the study of the so-called ethereal forms over \( \overline{\mathbb{F}}_p \) (see Section 8).

3 Computing with modular forms

The machinery of \( q \)-expansion and the Sturm bound (see Proposition 1.4.4) allow us to treat modular forms as finite algebraic objects (namely, truncated power series). To compute a space of modular forms \( V \) over a ring \( R \) is to provide a procedure that produces the image of a basis for \( V \) under some truncated \( q \)-expansion map \( V \to R[[q]]/(q^P) \) for any chosen precision \( P \geq 0 \).

3.1 Computing modular forms when \( k \geq 2 \)

Methods for computing spaces of modular forms of weight \( k \geq 2 \) are well-established. One of the most versatile methods comes from the theory of modular symbols (see [Ste05] and [Ste07]).

Briefly, a modular symbol of weight \( k \) \((k \geq 2)\), level \( N \), and character \( \chi \) (of level \( N \) and the same parity as \( k \)) is a formal sum of terms \( X^iY^{k-2-i}\{\alpha, \beta\} \) where \( 0 \leq i \leq k-2 \) and \( \alpha, \beta \in \mathbb{P}^1(\mathbb{Q}) \); here \( \{\alpha, \beta\} \) can be visualized as a geodesic arc from \( \alpha \) to \( \beta \) through \( \mathfrak{h} \). Let \( K = \mathbb{Q}(\chi) \); the space \( \mathcal{M}_k(N, \chi; K) \) is the torsion free \( K \)-module of such objects modulo torsion and the relations
\[
X^iY^{k-2-i}\{\alpha, \beta\} + X^iY^{k-2-i}\{\beta, \gamma\} + X^iY^{k-2-i}\{\gamma, \alpha\} = 0,
\]
\[
X^iY^{k-2-i}\{\alpha, \beta\} + X^iY^{k-2-i}\{\beta, \alpha\} = 0,
\]
and for each \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \), the relation
\[
(dX - bY)^i(-cX + aY)^{k-2-i}\{M\alpha, M\beta\} = \chi(d)X^iY^{k-2-i}\{\alpha, \beta\}.
\]
This space has an explicit, easily computable description as a Hecke module, and there is an isomorphism
\[ \mathcal{M}_k(N, \chi; \mathbb{C}) \longrightarrow \mathcal{M}_k(N, \chi; \mathbb{C}) \oplus S_k(N, \chi; \mathbb{C}) \]
of Hecke modules. This isomorphism allows us to construct a basis of eigenforms for \( \mathcal{M}_k(N, \chi; \mathbb{C}) \), and after linear transformation (invertible over \( K \)), we obtain a basis in \( \mathcal{M}_k(N, \chi; \mathcal{O}_K) = \mathcal{M}_k(N, \chi; \mathbb{Z}[\chi]) \).

**Theorem 3.1.1.** There is an algorithm that, on input \((k, N, \chi, P)\) with \( k \geq 0, N \geq 5, \chi \) a Dirichlet character of level \( N \) and the same parity as \( k \), and \( P \geq 0 \), computes the space \( \mathcal{M}_k(N, \chi; K) \) in terms of a basis \( B \subset \mathcal{O}_K[[q]]/(q^P) \) for its image under \( q \)-expansion \( \mathcal{M}_k(N, \chi; K) \rightarrow K[[q]]/(q^P) \).

The same is true upon replacing \( \mathcal{M}_k(N, \chi; K) \) with \( S_k(N, \chi; K) \).

**Proof.** Stein’s excellent book [Ste07] on the subject of computing modular forms explicates two such algorithms, Algorithm 9.12 (due to Merel), and Algorithm 9.14. The description of the Hecke action on \( \mathcal{M}_k(N, \chi; K) \) does not generalize to weight \( k = 1 \) (but see [Mar06]).

**Remark 3.1.2.** There are of course many other methods for computing spaces of modular forms; among them are the Eichler–Selberg trace formula (see [Hij74]) and the theory theta functions (see [Kan11]).

Of special interest in the context of this thesis is Mestre and Oesterlé’s method of graphs that computes \( S_2(N, 1; \mathbb{Z}[1/N]) \) by relating each Hecke operator \( T_\ell \) to the structure of the supersingular isogeny graph \( \mathcal{G}_\ell(N; \mathbb{F}_p)^{ss} \) (see Chapter II and [Mes11], especially Theorem 2.1). The space \( \mathcal{M}_2(N, 1; \mathbb{Q}) \) is the auxiliary space required in our implementation of Algorithm 7.2.6, and this can be computed very easily once \( S_2(N, 1; \mathbb{Q}) \) has been computed.

**Remark 3.1.3.** When \( k \) is very large, the computation of \( \mathcal{M}_k(N, \chi; \mathbb{C}) \) directly via modular symbols becomes rather cumbersome. In some cases, we can employ the following “divide and conquer” strategy: For even \( i \), multiplication in the graded ring \( \mathcal{M}(N; \mathbb{C}) \) gives a map
\[ \mathcal{M}_i(N, 1; \mathbb{C}) \times \mathcal{M}_{k-i}(N, \chi; \mathbb{C}) \longrightarrow \mathcal{M}_k(N, \chi; \mathbb{C}). \]
We compute bases \( B_1 \) and \( B_2 \) for \( \mathcal{M}_i(N, 1; \mathbb{C}) \) and \( \mathcal{M}_{k-i}(N, \chi; \mathbb{C}) \), respectively (either by this same method or using modular symbols when \( i \) and \( k - i \) are small). Finally, we can check using dimension formulas (see [Ste07] Chapter 6) that the image of the above map on \( B_1 \times B_2 \) generates \( \mathcal{M}_k(N, \chi; \mathbb{C}) \), in which case we can derive a basis for this space rather quickly.
3.2 Computing mod $p$ modular forms when $k = 1$

Spaces of weight 1 modular forms over $\mathbb{F}_p$ are of special interest because the projective Galois representations associated to such forms by Theorem 2.4.1 are unramified at $p$ (Theorem 2.4.3). Moreover, such forms do not necessarily lift to characteristic zero (see Section 8).

In [Edi06], Edixhoven provides a method for computing $M_1(N, \chi; \mathbb{F}_p)$ where $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{F}_p^\times$ is an odd character. At the heart of this method is the exact sequence

$$0 \longrightarrow S_1(N, \chi; \mathbb{F}_p) \xrightarrow{q \mapsto q^p} S_p(N, \chi; \mathbb{F}_p) \xrightarrow{\Theta} S_{p+2}(N, \chi; \mathbb{F}_p)$$

where $\Theta$ is a derivation map on cusp forms whose effect on $q$-expansions is

$$(\Theta f)(q) = \sum_{n=1}^{\infty} na_n(f)q^n.$$ 

The image of $S_1(N, \chi; \mathbb{F}_p)$ under $q \mapsto q^p$ can be produced once a basis for $S_p(N, \chi; \mathbb{F}_p)$ has been computed. Combining this with the explicit construction of weight 1 Eisenstein forms of a given character (see [DS05] Section 4.8), we obtain an algorithm for computing $M_1(N, \chi; \mathbb{F}_p)$.

**Theorem 3.2.1.** There is an algorithm that, on input $(N, p, \chi, P)$ with $N \geq 5$, $p$ a prime, $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{F}_p^\times$ an odd character, and $P \geq 0$, computes the space $M_1(N, \chi; \mathbb{F}_p)$ in terms of a basis $B \subset \mathbb{F}_p[\chi][[q]]/(q^P)$ for its image under $q$-expansion $M_k(N, \chi; \mathbb{F}_p) \to \mathbb{F}_p[[q]]/(q^P)$.

**Proof.** See [Edi06].

The algorithm requires an auxiliary computation of $M_p(N, \chi; \mathbb{F}_p)$, which can be computed using modular symbols algorithms. However, the complexity of this computation grows quickly with $p$, so this step can become expensive. In Section 8, we will demonstrate that for a complete picture of the weight 1 modular forms of level $N$, one must compute $M_1(N; \mathbb{F}_p)$ directly for relatively large primes $p$ (see also the tables in the appendix).

**Remark 3.2.2.** In Chapter III we will focus mainly on computing spaces of modular forms modulo odd primes $p$. The omission of $p = 2$ is not serious because we can defer to Edixhoven’s algorithm in this particular case, as well as for any other small characteristics that may cause problems.

3.3 Locating the zeros of a modular form

The Hecke stability method relies on manipulating the elements of the space $V = \bigcap_{\lambda \in A} \lambda^{-1}M_2(N, 1; F)$ where $A \subset M_1(N, \chi^{-1}; F) \setminus \{0\}$. For a better understanding of this space and the Hecke stability method in Chapter III, we require techniques for describing the set $\mathbb{Z}(A) = \bigcap_{\lambda \in A} \mathbb{Z}(\lambda)$. 

18
Example 3.3.1. Because of constraints imposed by the degree of \( \omega \) (see Proposition 4.12 in [Mil97]), the weight 1 Eisenstein series \( \lambda_{\varepsilon_3} \) and \( \lambda_{\varepsilon_7} \) have zeros only over \( j = 0 \).

Using the interpretation in Example 1.6.6 we can check that

- \( \lambda_{\varepsilon_3}([E, P]) = 0 \) if and only if \( j(E) = 0 \) and \( P \) is killed by \( \sqrt{-3} \in \text{End}(E_0) \), and
- \( \lambda_{\varepsilon_7}([E, P]) = 0 \) if and only if \( j(E) = 0 \) and \( P \) is killed by either of the endomorphisms \( 2 + \sqrt{-3} \) or \( 2 - \sqrt{-3} \) on \( E_0 \).

We conclude that \( jZ(\lambda_{\varepsilon_3}) = jZ(\lambda_{\varepsilon_7}) = \{0\} \).

In general, if \( N \) is prime and congruent to 1 modulo 3, then \( N = (a + \frac{b+\sqrt{-3}}{2})(a + \frac{b+\sqrt{-3}}{2}) \) for \( a, b \in \mathbb{Z} \). We have \( \lambda_{\varepsilon_N}([E, P]) = 0 \) whenever \( j(E) = 0 \) and either \( (a + \frac{b+\sqrt{-3}}{2})P = O \) or \( (a + \frac{b+\sqrt{-3}}{2})P = O \).

We will now sketch a method for computing the set \( jZ(\lambda) \) where \( \lambda \) is any modular form over \( \mathbb{C} \) with character. Our method is inspired by the work of Gekeler, who in [Gek01] computes the zeros of the level 1 Eisenstein series \( G_k \) for all \( k \in [4, 488] \). We will work exclusively over \( \mathbb{C} \) because the method over \( \mathbb{F}_p \) is identical, and because the elements of \( A \) that we will typically employ lift to characteristic zero. Note also that if \( \delta \) is a degeneracy map which is a composition of degeneracy maps of the first kind (see Section 1.1), then \( jZ(\lambda) = jZ(\delta^* \lambda) \).

Let \( k \geq 1 \), let \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times \) be a character of the same parity as \( k \), let \( K = \mathbb{Q}(\chi) \), and let \( \lambda \in M_k(N, \chi^{-1}; \mathbb{C}) \) be nonzero. Fix also a principal cusp \( \epsilon \in X_1(N)\mathbb{C} \); for the remainder of this section, all \( q \)-expansions will tacitly be \( q \)-expansions at \( \epsilon \).

Inspecting the dimension formulas (see [Ste07] Chapter 6, particularly Section 6.3) we observe that \( \dim_K M_{12t}(N, 1; K) = \dim_K M_{12t-k}(N, \chi; K) \) is bounded above by a constant, so there is a least \( t \) satisfying

\[
\dim_K M_{12t}(N, 1; K) - \dim_K M_{12t-k}(N, \chi; K) \leq t.
\]

Let \( V \) be the span of \( \{(1728G_4^3)^{i-1}(G_4^3 - G_6^2)^i\}_{i=0} \) and note that \( \dim_K V = t + 1 \), so the intersection

\[
\lambda M_{12t-k}(N, \chi; K) \cap V
\]

(in the ambient space \( M_{12t}(N, 1; K) \)) is nontrivial. Using the algorithm of Theorem 3.1.1 (or Remark 3.1.3) and linear algebra on \( q \)-expansions (of sufficiently high precision) we can determine a basis for this intersection. This yields a set \( S \) of polynomials \( J_1, \ldots, J_r \in K[X, Y] \) homogeneous of degree \( \leq t \) such that for each \( i \) there exists \( g_i \in M_{12t-k}(N, \chi; K) \) such that

\[
\lambda g_i = J_i(1728G_4^3, G_4^3 - G_6^2).
\]

Therefore when \( \lambda(\tau) = 0 \) for some \( \tau \in \mathfrak{h}^* \), we have for each \( i \)

\[
J_i(1728G_4(\tau)^3, G_4(\tau)^3 - G_6(\tau)^2) = 0.
\]

Combining this with the identity in Example 1.7.2 we may conclude the following:
• If $\tau \in \mathfrak{h}$, then $j(\tau)$ is a root of $J_i(t, 1) \in \mathbb{K}[t]$ for every $i$, and
• If $\tau \in \mathbb{P}^1(\mathbb{Q})$, then $Y \mid J_i(X, Y)$ for every $i$.

**Theorem 3.3.2.** There is an algorithm that, on input $(k, N, \chi, \lambda)$ where $k \geq 1$, $N \geq 5$, $\chi$ is a character of level $N$ and the same parity as $k$, and $\lambda \in \mathfrak{M}_k(N, \chi; \mathbb{C})$, computes a finite set $J \subset \mathbb{P}^1(\mathbb{Q})$ that contains $j\mathbb{Z}(\lambda)$.

**Proof.** This is the algorithm sketched above. \hfill $\Box$

**Remark 3.3.3.** The algorithm above requires that we calculate a basis for the space $\mathfrak{M}_{12r-k}(N, \chi; K)$, and this can be rather demanding. However, the “divide and conquer” approach in Remark 3.1.3 can be employed to speed this computation up, provided that it works in this particular case.

**Example 3.3.4.** Let us compute the zero set of $\lambda_{\varepsilon_{11}}$ (normalized so that this form has the $q$-expansion in Lemma 1.6.5 at our fixed cusp). We have

$$\dim_{\mathbb{Q}} \mathfrak{M}_{12}(11, 1; \mathbb{Q}) = 12 \quad \text{and} \quad \dim_{\mathbb{Q}} \mathfrak{M}_{11}(11, \varepsilon_{11}; \mathbb{Q}) = 11$$

so $\lambda_{\varepsilon_{11}}, \mathfrak{M}_{11}(11, \varepsilon_{11}; \mathbb{Q})$ must intersect the (2-dimensional) span of $\{1728G_4^3, G_4^3 - G_6^2\}$ inside $\mathfrak{M}_{12}(11, 1; \mathbb{Q})$. Using SAGE, there is $g \in \mathfrak{M}_{11}(11, \varepsilon_{11}; \mathbb{Q})$ such that

$$\lambda_{\varepsilon_{11}}(q)g(q) \equiv (1728G_4(q)^3) - (-32^3)(G_4(q)^3 - G_6(q)^2) \mod q^{13},$$

and this $g$ has $q$-expansion

$$g(q) = -1728(1 + 33486q - 674124q^2 + 26560340q^3 + 295485038q^4 + \cdots).$$

Since $13 = \text{Sturm}_{12}(11)$, we have the equality of modular forms $\lambda_{\varepsilon_{11}}, g = (1728G_4^3) - (-32^3)(G_4^3 - G_6^2)$. The modular form on the right hand side has a simple zero at every point of $X_1(11)$ above $j = -32^3$, so we have $j\mathbb{Z}(\lambda_{\varepsilon_{11}}) = \{-32^3\}$.

The reader may notice that $-32^3$ is the $j$-invariant of the elliptic curve $\mathbb{C}/\mathbb{Z}[\frac{1 + \sqrt{-11}}{2}]$ (see Table 12.20 in [Cox89]). This “CM zero” phenomenon continues to some extent.

**Example 3.3.5.** Using the method above, we can show that the set $j\mathbb{Z}(\lambda_{\varepsilon_{23}})$ coincides with the root set of the polynomial

$$3^{24}t^2 - 167748973363200t + 42202348650496000,$$

which is an irreducible quadratic whose roots are $p$-integral away from $p = 3$ (note that 3 is the class number of $\mathbb{Q}(\sqrt{-23})$ and that $L_{\varepsilon_{23}} = 3$). In particular, this means that the reduction of $\lambda_{\varepsilon_{23}}$ modulo 3 is a cusp form, and (by combining [Sil94] Section II.6 and [Ser81] Théorème 20) that the zeros of $\lambda_{\varepsilon_{23}}$ have few primes of supersingular reduction (the first few are $p = 5, 7, 17, 19, 37, 97, 613, 823, 983, \ldots$). This latter property will be ideal in the context of the Hecke stability method (see Chapter III, specifically Theorem 7.1.1).
It is an amusing and illustrative exercise to verify computationally that Corollary 2.2.3 and Corollary 2.3.4 work as promised.

**Example 3.3.6.** Let \( f = \Delta/\lambda_7 \in M_{11}^{\text{mod}}(7, \varepsilon_7; \mathbb{Q}) \) where \( \Delta, \lambda_7 \) are defined as in Section 1.6. We know from Example 3.3.1 that \( jZ(\lambda_7) = \{ \infty \} \).

Example 2.1.1 and Corollary 2.2.3, the poles of \( T_2f \) are simple and lie above \( j = 54000 \). The modular form

\[
(1728G_4^3) - 54000(G_4^3 - G_6^2) = 432(121G_4^3 - 125G_6^2)
\]

(of weight 12 and level 1) has zeros at every point of \( X_1(7) \) above \( j = 54000 \), so let \( h = 121G_4^3 - 125G_6^2 \). Corollary 2.2.3 predicts that \( h \) is a denominator for \( T_2f \), so we should have \( h \cdot T_2f \in M_{23}(7, \varepsilon_7; \mathbb{Q}) \). The \( q \)-expansion of \( h \cdot T_2f \) is

\[
104q - 5537344q^2 - 47703600q^3 + 317633800q^4 + 175369047952q^5 + \cdots
\]

and we can verify with SAGE that this \( q \)-expansion indeed does lie in the image of \( M_{23}(7, \varepsilon_7; \mathbb{Q}) \to \mathbb{Q}[[q]]/(q^P) \) any choice of precision \( P \) (see Lemma 7.2.4).

![Figure](image)

**Figure.** Pole propagation by \( T_2 \) near \( j = 0 \).

In the above figure, gray indicates that the form in question has a pole over the elliptic curve with that \( j \)-invariant. Note that the Hecke operator \( T_2 \) “moves” the pole above \( j = 0 \) to a pole above \( j = 54000 \).

**Example 3.3.7.** For a slightly more complicated example, consider \( f = g/\lambda_{11} \) where \( g \) is the unique normalized element of \( S_2(11, 1; \mathbb{Q}) \): \( g(q) = q \prod_{n \geq 1} (1 - q^n)^2(1 - q^{11n})^2 \). Then \( f \in M_{11}^{\text{trac}}(11, \varepsilon_{11}; \mathbb{Q}) \) and since \( jZ(g) = \{ \infty \} \) (as can be ascertained with Proposition 1.4.1.c), \( f \) has a pole above \( j = -32^3 \) (Example 3.3.4).

By Corollary 2.2.3, \( T_2f \) ought to have poles above the (three distinct) roots of \( \Phi_2(-32^3, T) \) on the \( j \)-line. A modular form of weight 36 and level 1 with a simple zero at each of these roots is

\[
h = (G_4^3 - G_6^2)^3 \Phi_2( -32^3, \frac{1728G_4^3}{G_4^3 - G_6^2} ),
\]

(where \( \Phi_2 \) is the modular polynomial as defined in Example 2.1.1) and SAGE verifies that \( h \cdot T_2f \in M_{37}(11, \varepsilon_{11}; \mathbb{Q}) \). (Of course, one must also check that \( T_2f \) has poles above each \( \alpha_i \), and this part of the computation is somewhat more involved.)
The above figure illustrates the propagation of the pole above $j = -32^3$ propagates to poles above the roots $\alpha_1, \alpha_2, \alpha_3$ of $\Phi_2(-32^3, T)$ by the Hecke operator $T_2$.

**Example 3.3.8.** Let $\lambda_{\varepsilon_5}^{(2)}$ be the “principal” weight 2 Eisenstein series with quadratic character $\varepsilon_5 : (\mathbb{Z}/5\mathbb{Z})^\times \to \{\pm 1\}$: This form has $q$-expansion

$$\lambda_{\varepsilon_5}^{(2)}(q) = 1 - 5 \sum_{n \geq 1} \sum_{m | n} \varepsilon_5(m)mq^n.$$  

The modular curve $X_1(5)$ has 4 cusps, and one can prove (using arguments similar to those in [Boy00]) that $\lambda_{\varepsilon_5}^{(2)}$ vanishes (to order 1) at exactly 2 of these cusps $c_1$ and $c_2$; over $\mathbb{C}$ these correspond to $\Gamma_1(5) \cdot 0$ and $\Gamma_1(5) \cdot \frac{1}{2}$.

Consider the fractional modular form $f = G_4/\lambda_{\varepsilon_5}^{(2)} \in M_2^{\text{frac}}(5, \varepsilon_5; \mathbb{Q})$. $f$ has a simple pole at $c_i$ for $i = 1, 2$. By Corollary 2.3.4, $T_\ell f$ ought to have a pole of order $\ell$ at each of these cusps. Indeed, taking $\ell = 2$, we can verify using SAGE that

- $T_2 f \notin M_2(5, \varepsilon_5; \mathbb{Q})$, and
- $\lambda_{\varepsilon_5}^{(2)} \cdot T_2 f \notin M_4(5, \varepsilon_5; \mathbb{Q})$, but
- $(\lambda_{\varepsilon_5}^{(2)})^2 \cdot T_2 f \in M_6(5, \varepsilon_5; \mathbb{Q})$.

Thus, since $\text{ord}_{c_i}(\lambda_{\varepsilon_5}^{(2)}) = 1$, $\text{ord}_{c_i}(T_2 f) = -2$ for $i = 1, 2$, as predicted by Corollary 2.3.4.
Chapter II

Isogeny graphs

In broad terms, an isogeny graph is a graph whose vertices represent moduli of level structures and whose edges represent isogenies between those moduli. Isogeny graphs have found many applications in modern number theory:

- Computing bases for spaces of modular forms. For example, the method of graphs outlined in [Mes11] relates the adjacency matrices of ℓ-isogeny graphs on the supersingular points of $[\Gamma_0(N)]_{\overline{F}_p}$ (this is the graph $G_\ell(N; \overline{F}_p)^{ss}$ below) with the action of $T_\ell$ on $M_2(Np, 1; \mathbb{C})$. Computing the eigenvalues of this finite graph yields a basis of eigenforms for this space.

- The computation of the endomorphism ring of an elliptic curve. [Koh96] [Bis11a] [Bis11b]

- Computation of the modular polynomials $\Phi_\ell$ (as defined in Example 2.1.1). [BLS10]

- The construction of cryptographically secure hashing functions. [CGL07] [Bis11b] [JD11] [Sar90]

The combinatorial properties of isogeny graphs on the moduli of $\Gamma_0(N)$-structures (over one of the fields $\mathbb{C}$ or $\overline{F}_p$) will provide a key step in the proof of Theorem 6.2.1; this chapter is meant to provide a self-contained exposition of the necessary theory.

Section 4 describes the structure of the our isogeny graphs, relying mainly on the theory of elliptic curves as well as some elementary constructions from algebraic topology. In Section 5 we will distill the theory of the preceding section into the precise technical result (Lemma 5.3.3) we will need in the proof of Theorem 6.2.1. The gist of this chapter is that the graphs with which we are concerned admit local embeddings (at every vertex) of large graphs with few cycles, though over $\overline{F}_p$ the meaning of “large” depends on the size of $p$ relative to $N$ (see Lemma 5.1.2).
4 Isogeny graphs on $\Gamma_0(N)$-structures

Throughout this chapter we fix the following: a level $N \geq 1$, a field $F$ with either $F = \mathbb{C}$ or $F = \overline{\mathbb{F}}_p$ for $p \nmid N$, and a prime $\ell$ that does not divide $N$ and that is not equal to the characteristic of $F$.

4.1 The full and derived isogeny graphs

Definition 4.1.1. The full isogeny graph $G_\ell(N; F)$ is the directed graph whose vertex set is $[\Gamma_0(N)]_F$ and whose adjacency operator is the Hecke correspondence $\text{Hecke}^0_\ell$.

That is, if $[E, C] \in [\Gamma_0(N)]_F$ and $\text{Hecke}^0_\ell([E, C]) = [E_0, C_0] + \cdots + [E_\ell, C_\ell]$, then for each index $i \in [0, \ell]$ there is an arc in $G_\ell(N; F)$ from $[E, C]$ to $[E_i, C_i]$.

Example 4.1.2. When $N = 1$, we can label each vertex of $G_\ell(N; F)$ with $j_0 \in F$. For each pair $j_1, j_2 \in F$, the number of arcs $j_1 \to j_2$ in $[\Gamma(1)]_F$ is exactly the multiplicity of the factor $(Y - j_2)$ in $\Phi_\ell(j_1, Y)$ where $\Phi_\ell$ is the modular polynomial (see Example 2.1.1).

Immediately we see that every vertex of $G_\ell(N; F)$ has outdegree $\ell + 1$ (since $\ell \nmid N$).

Definition 4.1.3. The derived isogeny graph $G'_{\ell}(N; F)$ whose vertex set is $[\Gamma_0(N)]_F$ and whose arcs are isomorphism classes of degree $\ell$ isogenies between $\Gamma_0(N)$-structures over $F$.

The full and derived isogeny graphs have the same vertex set, but how do their arc sets compare? By the construction of $\text{Hecke}^0_\ell$, the arc sets differ only at those vertices $\tau$ that represent $\Gamma_0(N)$-structures $(E, C)$ such that there are distinct cyclic $H_1, H_2 \subset E$ of order $\ell$ satisfying $(E, C; H_1) \cong (E, C; H_2)$. This means that $\text{Aut}(E, C)$ is strictly larger than $\{\pm 1\}$, so $[E, C]$ must be an elliptic point.

Proposition 4.1.4. $G'_{\ell}(N; F)$ is a subgraph of $G_\ell(N; F)$ and $G_\ell(N; F) \setminus G'_{\ell}(N; F)$ consists of (finitely many) arcs that are based at the elliptic points of $G_\ell(N; F)$.

The advantage of the derived isogeny graph is that the dualization map $\varphi \mapsto \hat{\varphi}$ on isogenies induces an involution on the arcs of $G'_{\ell}(N; F)$ that switches the origin and destination of an arc. This allows us to give $G'_{\ell}(N; F)$ the structure of an undirected graph: An (undirected) edge of $G'_{\ell}(N; F)$ is an orbit of dualization on the arcs of $G'_{\ell}(N; F)$. That is, if $[\varphi] : \tau \to \tau'$ is an arc in $G'_{\ell}(N; F)$, the corresponding edge $\tau \leftrightarrow \tau'$ is $\{[\varphi] : \tau \to \tau', [\hat{\varphi}] : \tau' \to \tau\}$.

Because $G'_{\ell}(N; F)$ was obtained by deleting finitely many arcs of $G_\ell(N; F)$, it may not be $\ell + 1$-regular. Instead, if we define the degree of a vertex $\tau \in \mathcal{V}(G'_{\ell}(N; F))$ to be the outdegree of $\tau$ in $G'_{\ell}(N; F)$ (as a directed graph), then $\deg_{G'_{\ell}(N; F)}(\tau) = \ell + 1$ whenever $u(\tau) = 1$. Computing the degree of a vertex in this way also accounts for a minor subtlety at vertices with self-dual loops (edges $\{[\varphi]\}$ where $[\hat{\varphi}] = [\varphi]$).

---

1We permit multiple edges (or arcs) as well as loops in our definition of graph.
2-Isogenies near 0

\[1417905000 + 818626500 \sqrt{3}\]

\[1417905000 - 818626500 \sqrt{3}\]

Level 7 example

\[54000\]

\(f_0\)

\(\alpha \bar{\alpha}\)

\[54000\]

\(T_2 f_0\)

\(\alpha \bar{\alpha}\)

\(G(1; C)\) \(G(1; C)\)

\(4\)

Figure. Comparing full and derived isogeny graphs.

The figure above illustrates the basic differences between the full and derived 2-isogeny graphs of level 1 over \(\mathbb{C}\) near \(j = 0\) (see also the figure in Example 2.1.1).

4.2 Isogeny graphs and endomorphisms of level structures

Our goal in this section is to relate the combinatorial structure of the derived isogeny graph \(G'_\ell(N; F)\) with the endomorphism rings of its vertices. The intuition behind this relationship is simple: If \(x\) is a directed cycle in \(G'_\ell(N; F)\) based at some vertex \(\tau\), we obtain a family of endomorphisms of \(\tau\) by composing along the isogenies representing the arcs in \(x\). Two distinct cycles should represent commuting elements of \(\text{End}(\tau)\) only if those cycles commute in the fundamental group of \(G'_\ell(N; F)\).

Concretely, fix a connected component \(G\) of \(G'_\ell(N; F)\) and identify \(G\) with the graph obtained by fixing a set of representatives for the vertices and edges of this component: That is, \(G\) is a connected graph whose vertices are \(\Gamma_0(N)\)-structures \((E, C)\) over \(F\) and whose edges are dualization orbits \(\{\varphi, \hat{\varphi}\}\) of \(\ell\)-isogenies between them; we demand that the map \(G \rightarrow G'_\ell(N; F)\) obtained by taking isomorphism classes is an isomorphism of graphs onto the connected component of \(G'_\ell(N; F)\) with which we started. Any such choice of representatives is certainly noncanonical, but this will not matter.

Now, if

\[x : (E, C) = (E_1, C_1) \xrightarrow{\varphi_1} (E_2, C_2) \xrightarrow{\cdots} (E_n, C_n) \xrightarrow{\varphi_n} (E_1, C_1)\]

is a directed cycle in \(G\) based at \((E, C)\), we define

\[\Phi_{(E,C)}(x) = \hat{\varphi}_1 \cdots \hat{\varphi}_n \in \text{End}(E, C),\]

and this gives a monoid homomorphism

\[\Phi_{(E,C)} : \{\text{directed cycles in } G \text{ based at } (E, C)\} \longrightarrow \text{End}_\ell(E, C),\]

where the operation on the left is concatenation and \(\text{End}_\ell(E, C)\) is the monoid

\[\{ \alpha \in \text{End}(E, C) : N(\alpha) \in \ell \mathbb{Z} \}\]

under multiplication; we of course take \(\Phi_{(E,C)}\) of the trivial cycle at \((E, C)\) to be 1. If we denote the length of the cycle \(x\) by \(|x|\) then clearly \(N(\Phi_{(E,C)}(x)) = \ell^{|x|}\).
**Lemma 4.2.1.** Let \((E, C), (E', C')\) be vertices of \(G\) and let \(x\) be a directed cycle in \(G\) (without basepoint) on which both these vertices lie. \(\alpha = \Phi_{(E,C)}(x)\) and \(\beta = \Phi_{(E',C')}(x)\) are algebraic conjugates in the sense that there is an irreducible polynomial \(F \in \mathbb{Z}[t]\) of degree at most 2 such that \(F(\alpha) = F(\beta) = 0\).

**Proof.** Let

\[
x : (E, C) \rightarrow (E_1, C_1) \xrightarrow{\varphi_1} (E_2, C_2) \rightarrow \cdots \rightarrow (E_n, C_n) \xrightarrow{\varphi_n} (E_1, C_1)
\]

and choose a prime \(\nu \neq \text{char } F\). Applying the \(\nu\)-adic Tate functor yields

\[
\text{Tate}_\nu(E_1) \xrightarrow{\text{Tate}_\nu(\varphi_1)} \text{Tate}_\nu(E_2) \rightarrow \cdots \rightarrow \text{Tate}_\nu(E_n) \xrightarrow{\text{Tate}_\nu(\varphi_n)} \text{Tate}_\nu(E_1).
\]

Fixing bases for the various \(\text{Tate}_\nu(E_i)\), we may consider each \(\text{Tate}_\nu(\varphi_i)\) as a \(2 \times 2\) matrix \(M_i\) with coefficients in \(\mathbb{Z}_\nu\). The element \(\alpha = \varphi_{(E,C)}(x)\) has the same characteristic polynomial as \(M_1 \cdots M_n\).

Now, suppose that \((E'_j, C'_j) = (E_j, C_j)\) for some \(j \in [1, n]\). The characteristic polynomial of \(\beta = \Phi_{(E',C')}(x)\) is the same as that of \(M_j \cdots M_n M_1 \cdots M_{j-1}\), which is the same as that of \(\alpha\), because the characteristic polynomial of a product of \(2 \times 2\) matrices is invariant under cyclic permutations of the terms. \(\square\)

The following corollary is not a direct consequence of the preceding lemma, but it is related in that its proof is basically identical.

**Corollary 4.2.2.** Let \((E, C), (E', C')\) be vertices of \(G\), let \(d\) be the graph distance between these vertices, and let \(\alpha \in \text{End}(E, C)\). There is an embedding \(\mathbb{Z}[\ell^d \alpha] \hookrightarrow \text{End}(E', C')\).

**Corollary 4.2.3.** If \(x\) is a directed cycle in \(G\) based at some vertex \((E, C)\), then \(x\) is contractible (i.e., nullhomotopic) if and only if \(\Phi_{(E,C)}(x)\) is a rational integer.

**Proof.** We proceed by induction on \(|x|\) (with our base case being \(|x| = 0\)). Because the edges of \(G'_{\ell}(N; F)\) are orbits of the arcs of \(G_{\ell}(N; F)\) under dualization, a nontrivial directed cycle \(x\) in \(G\) based at \((E, C)\) is contractible if and only if it has the form

\[
(E, C) \xrightarrow{a} \cdots \xrightarrow{a} (E', C') \xleftarrow{\Phi_{(E',C')}} (E'', C'') \xrightarrow{\Phi_{(E'',C'')}} (E', C') \xrightarrow{b} \cdots \xrightarrow{b} (E, C)
\]

where \(y = ab\) is also a contractible directed cycle based at \((E, C)\). By considering \(x\) from the basepoint \((E', C')\), we have \(\Phi_{(E',C')}(x) = \ell \Phi_{(E',C')}(y)\), so by Lemma 4.2.1, \(\Phi_{(E,C)}(x)\) contains a rational integer if and only if \(\Phi_{(E',C')}(y)\) does. The claim follows by induction, since \(y\) is contractible and \(|y| < |x|\). \(\square\)

Let \(\text{End}_{\ell}^F(E, C)\) denote the submonoid of \(\text{End}_{\ell}(E, C)\) consisting of those elements that are rational integers (away from elliptic points, this is just \(\pm \ell^N\)). The quotient monoid \(\text{End}_{\ell}(E, C)/\text{End}_{\ell}^F(E, C)\) is a group, with inversion induced by conjugation (dualization) in \(\text{End}(E, C)\). The above corollary implies that \(\Phi_{(E,C)}(x) \in \text{End}_{\ell}^F(E, C)\) if and only if \(x\) is contractible. Combining the results of this section yields the following structure theorem for isogeny graphs:
Theorem 4.2.4. The map $\Phi(E, C)$ induces a group embedding

$$\tilde{\Phi}(E, C) : \pi_1(G, (E, C)) \to \text{End}_\ell(E, C).$$

Hence, for all $\tau \in \mathcal{G}_\ell(N; F)$, $\Phi(E, C)$ induces a (noncanonical) group embedding

$$\tilde{\Phi}_\tau : \pi_1(G'(N; F), \tau) \to \text{End}_\ell(\tau).$$

where $\text{End}_\ell(\tau)$ and $\text{End}_\ell^\tau(\tau)$ are defined in a similar way as above.

Remark 4.2.5. If the connected component of $\tau$ in $\mathcal{G}_\ell(N; F)$ contains no elliptic points, then $\tilde{\Phi}_\tau$ is actually an isomorphism: Let $\alpha \in \text{End}_\ell'(E, C)$ and let $H_1 \subset \cdots \subset H_n = \ker \alpha$ where $H_1$ and each successive quotient $H_{i+1}/H_i \subset E[N]$ is cyclic of order $\ell$. Because the component $G$ containing $(E, C)$ has no elliptic points, we may find a cycle $x$ in $G$ based at $(E, C)$ by taking successive quotients $E \to E/H_1 \to \cdots \to E/H_n$ and so $\Phi(E, C)(x) = \pm \hat{\alpha}$; it follows that the map $\tilde{\Phi}(E, C)$ as defined above is surjective.

4.3 Ordinary and supersingular isogeny graphs

Let $G$ be a connected component of $\mathcal{G}_\ell'(N; F)$ and hereafter, let $W_G$ denote the set of vertices in $G$ that are elliptic points of $[\Gamma_0(N)]_F$ (see Section 1.1).

Since $\mathcal{V}(G)$ is contained in an isogeny class, either $G$ is ordinary (the vertices have commutative endomorphism rings), or $G$ is supersingular (the vertices have noncommutative endomorphism rings, see [Sil09] Section III.9 and Theorem V.3.1). In the ordinary case we have a fairly complete combinatorial description of $G$:

Theorem 4.3.1. Let $G$ be an ordinary connected component of $\mathcal{G}_\ell'(N; F)$, and let $K_G$ be the number field $\text{End}(\tau) \otimes \mathbb{Z} \mathbb{Q}$ for some (any) $\tau \in \mathcal{V}(G)$. Note that $K_G$ is either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$.

a. $G$ contains at most one elliptic point.

b. If $\ell$ is inert or $\ell$ is nonprincipally ramified in $K_G/\mathbb{Q}$, then $G$ is an infinite tree such that every nonelliptic vertex has degree $\ell + 1$.

c. If $\ell$ is split or $\ell$ is principally ramified in $K_G/\mathbb{Q}$, then $G$ is an infinite volcano (a graph with a unique simple cycle) and every nonelliptic vertex has degree $\ell + 1$.

d. In case (c.), every vertex on the simple cycle has the same endomorphism ring $\mathcal{O}$ up to isomorphism, and this ring is maximal among the endomorphism rings of the vertices of $G$. If $\ell = l_1l_2$ in $\mathcal{O}$, then the length of the unique simple cycle in $G$ (the crater) is the least $r$ such that $l_1^r$ and $l_2^r$ are both principal ideals of $\mathcal{O}$.
e. If $G$ contains an elliptic point, then it is either a tree or it contains a loop that is based at the elliptic point.

\[ \text{Figure.} \] Ordinary 2-isogeny graphs: The graph on the left is an infinite 3-regular tree. The graph on the right is an infinite 3-regular volcano with a crater of length 5.

**Proof.** (a.) Let $\tau_1, \tau_2 \in W_G$. Since these lie on the same ordinary connected component, $w(\tau_1) = w(\tau_2)$, so there is an elliptic curve $E/F$ with $j(E) \in \{0, 1728\}$ and cyclic subgroups $C_1, C_2 \in E[N]$ such that $(E, C_i)$ represents the vertex $\tau_i$. Let $\varphi : (E, C_1) \to (E, C_2)$ be the isogeny obtained by composing along some path from $\tau_1$ to $\tau_2$ in $G$. We have $\varphi \in \text{End}(E)$, and by ellipticity, $\varphi \in \text{End}(E) = \text{End}(E, C_1)$, since both are isomorphic to $\mathbb{Z}[\zeta]$ where $\zeta$ is a primitive 3rd or 4th root of unity. Hence $\varphi(C_1) = C_1$, so $C_1 = C_2$, and therefore $\tau_1 = \tau_2$.

Claims (b.–d.) are consequences of Kohel’s thesis [Koh96]; alternately, one can view these isogeny graphs as quotients of the Bruhat–Tits tree [Ser03]. These may also be derived directly by combining Theorem 4.2.4, elementary facts about elliptic curves ([Sil09] Section III.9), and the standard computation of the fundamental group of a graph in terms of spanning trees ([Mas91] Section 6.5). Claim (e.) follows from the claims that precede it.

A unified description in the supersingular case is more difficult: If $(E, C)$ is a supersingular $\Gamma_0(N)$-structure over $\mathbb{F}_p$, then $\text{End}(E, C)$ is isomorphic to a level $N$ Eichler order of “the” quaternion algebra $\mathbb{B}_{p,\infty}$ ramified at $p, \infty$ (see e.g., [Pra95] Section 6). Since quaternion algebras are not commutative, the structure theorem tells us very little a priori. A fundamental result on supersingular isogeny graphs is the following:

**Theorem 4.3.2.** The subgraph $G'_i(N; \mathbb{F}_p)_{\text{ss}} \subset G'_i(N; \mathbb{F}_p)$ on the set of supersingular moduli $[\Gamma_0(N)]_{\mathbb{F}_p}^{\text{ss}}$ is a finite connected graph.

**Proof.** See [Mes11] Section 2.4.

Though it is impractical to make general statements about the global structure of $G'_i(N; \mathbb{F}_p)_{\text{ss}}$ as $N$ and $p$ vary, the argument in Section 2.1 of [GL04] allows us to describe the structure of this graph “locally.”

**Lemma 4.3.3** (Goren–Lauter). Let $\tau \in [\Gamma_0(N)]_{\mathbb{F}_p}^{\text{ss}}$ and let $\alpha, \beta \in \text{End}(\tau)$. If $\alpha \beta \neq \beta \alpha$, then $4N(\alpha)N(\beta) \geq Np$. 

28
Proof. The case $N = 1$ is treated in [GL04], and the proof adapts to the general case by noting that the discriminant of an Eichler order $O \subset \mathcal{B}_{p,\infty}$ of level $N$ is $(Np)^2$.

**Corollary 4.3.4.** If $\tau$ is a vertex of $G'_G(N; \overline{\mathbb{F}}_p)^{ss}$ and $x$ and $y$ are directed cycles based at $\tau$ that do not commute in $\pi_1(G'_G(N; \overline{\mathbb{F}}_p)^{ss}, \tau)$, then $4\ell^{|x|+|y|} \geq Np$, or equivalently, $|x| + |y| \geq \log_4 \left( \frac{Np}{4} \right)$.

**Proof.** By Theorem 4.2.4, $\alpha = \Phi_\tau(x)$ and $\beta = \Phi_\tau(y)$ do not commute in $\text{End}_G(\tau)$, so since $N(\alpha) = \ell^{|x|}$ and $N(\beta) = \ell^{|y|}$, the claim follows from the preceding lemma. □

Colloquially, “small cycles in $G'_G(N; \overline{\mathbb{F}}_p)^{ss}$ cannot be too close together.” Thus $G'_G(N; \overline{\mathbb{F}}_p)^{ss}$ is “locally isomorphic” to an ordinary isogeny graph. This idea can be formalized in specific applications; for example, the next lemma can generalize the claims (a.) and (e.) in Theorem 4.3.1 to the supersingular component.

**Lemma 4.3.5.** Let $G = G'_G(N; \overline{\mathbb{F}}_p)^{ss}$ and let $\tau \in V(G)$.

a. If $\tau_1, \tau_2 \in W_G$ are distinct, then $4\ell^{\text{dist}_G(\tau_1, \tau_2)} \geq p$ or $4\ell^{2\text{dist}_G(\tau_1, \tau_2)} \geq Np$.

b. If $\tau \in W_G$, $x$ is an irreducible noncontractible directed cycle in $G$ based at $\tau$, and $|x| \geq 2$, then $4\ell^{|x|} \geq Np$.

**Proof.** (a.) If $w(\tau_1) \neq w(\tau_2)$, then $\mathbb{Z}[u_1] \hookrightarrow \text{End}(\tau_1)$ and $\mathbb{Z}[u_2] \hookrightarrow \text{End}(\tau_2)$ where $u_1$ and $u_2$ are roots of unity generating distinct quadratic extensions of $\mathbb{Q}$. By Corollary 4.2.2, there is an embedding $\mathbb{Z}[\ell^{\text{dist}(\tau_1, \tau_2)}] \hookrightarrow \text{End}(\tau_2)$, so since $u_1$ and $u_2$ cannot commute in $\text{End}(\tau_2) \otimes_{\mathbb{Z}} \mathbb{Q}$, the elements $\alpha = \ell^{\text{dist}(\tau_1, \tau_2)}u_1$ and $u_2$ do not commute in $\text{End}(\tau_2)$. By Lemma 4.3.3,

$$4\ell^{2\text{dist}_G(\tau_1, \tau_2)} = 4N(\alpha)N(u_2) \geq Np.$$

If instead we have $\tau_1 \neq \tau_2$ and $w(\tau_1) = w(\tau_2)$ then there exists an elliptic curve $E/F$ with $j(E) \in \{0, 1728\}$ and cyclic subgroups $C_1, C_2 \subset E[N]$ of order $N$ such that $(E, C_i)$ represents $\tau_i$ for $i = 1, 2$. There also exists $\Phi : (E, C_1) \rightarrow (E, C_2)$ of degree $\ell^{\text{dist}_G(\tau_1, \tau_2)}$, and since $\varphi : E \rightarrow E$, we have $\varphi \in \text{End}(E)$. Let $\zeta$ generate $\text{Aut}(E) = \text{Aut}(E, C_1)$, and suppose for contradiction that $4\ell^{\text{dist}_G(\tau_1, \tau_2)} < p$. By Lemma 4.3.3, $\zeta$ and $\varphi$ commute in $\text{End}(E)$, so $\varphi \in \mathbb{Z}[\zeta] = \text{End}(E, C_1)$, from which it follows that $\varphi(C_1) = C_1$ and that $\tau_1 = \tau_2$, a contradiction.

(b.) Let $\alpha \in \varphi_\tau(x)$ and let $\zeta \in \text{Aut}(\tau)$ be a generator. If $\zeta \alpha \neq \alpha \zeta$, then the claim follows immediately from Lemma 4.3.3. If instead $\zeta \alpha = \alpha \zeta$, then $\alpha \in \mathbb{Z}[\zeta]$ (since $\mathbb{Z}[\zeta]$ is a maximal quadratic order). By our hypotheses on $x$, $\alpha \notin \ell \mathbb{Z}$ and $\alpha$ is irreducible. Since $\mathbb{Z}[\zeta]$ is a maximal quadratic order with trivial class group, $N(\alpha) = \ell$, so $|x| = 1$. □

### 5 Combinatorial results on isogeny graphs

We have now established the structural results that we will need to prove the technical lemma required in the proof of the Hecke stability theorem. Below, Lemma 5.1.2 shows
that when we assume certain relations among the data \( N, p, \ell \), the local structure of \( \mathcal{G}_\ell(N; \bar{\mathbb{F}}_p) \) is easily described. This will be used in the proof of Lemma 5.3.3, which provides lower bounds on the size of a “polar condition” (a certain kind of vertex set, see Definition 5.2.4) on the graph \( \mathcal{G}_\ell(N; F) \).

### 5.1 Local structure of isogeny graphs

**Definition 5.1.1.** For a connected undirected graph \( G \), \( v_0 \in V(G) \), and \( n \geq 0 \), the neighborhood \( \mathcal{N}_n(G, v_0) \) (of radius \( n \) around \( v_0 \) in \( G \)) is the maximal subgraph of \( G \) on the vertex set

\[
\{ v \in V(G) : \text{dist}_G(v, v_0) \leq n \}
\]

such that if \( \text{dist}_G(v, v_0) = \text{dist}_G(w, v_0) = n \), \( v \) is not adjacent to \( w \) in \( \mathcal{N}_n(G, v_0) \). (In words, we discard all edges between vertices at distance \( n \) from the root.)

We consider \( \mathcal{N}_n(G, v_0) \) as being rooted at \( v_0 \).

We summarize our local structural results on \( \mathcal{G}_\ell'(N; F) \) as follows:

**Lemma 5.1.2.** Let \( G \) be a connected component of \( \mathcal{G}_\ell'(N; F) \), \( \tau \in V(G) \), and assume either that \( G \) is ordinary, or that \( G = \mathcal{G}_\ell'(N; \bar{\mathbb{F}}_p)_{\text{ss}}, 4\ell^4 n < Np, \) and \( 4\ell^2 n < p \).

Let \( (G', \tau) = \mathcal{N}_n(G, \tau) \).

a. \( G' \) is either **acyclic** (contains no cycles) or **monocyclic** (contains exactly one cycle).

b. \( G' \) contains at most one elliptic point.

c. If \( G' \) contains both a cycle and an elliptic point, then that cycle is a loop based at the elliptic point.

d. If \( \tau' \in V(G') \) satisfies \( \text{dist}_{G'}(\tau, \tau') < n \) and \( w(\tau') = 1 \), then \( \deg \tau' = \ell + 1 \).

**Proof.** (a.) follows from Corollary 4.3.4. (b.) follows from Lemma 4.3.5.a and the observation that the distance between any two vertices in \( G' \) is at most \( 2n \). (c.) follows from Lemma 4.3.5.b. (d.) is a direct consequence of Proposition 4.1.4.

### 5.2 Polar conditions

In this section we will define “polar conditions,” vertex sets on a graph that abstract the poles of a meromorphic eigenfunction on that graph. Our goal is to provide lower bounds for polar conditions on \( \mathcal{G}_\ell(N; F) \). Intuitively, we will do this by giving lower bounds on (quasi)polar conditions on trees, and then using Lemma 5.1.2 to embed these trees into \( \mathcal{G}_\ell'(N; F) \).

First, we standardize some notation for trees:

**Definition 5.2.1.** Let \( r \geq 0 \), let \( d \geq 2 \), and \( j \in \{-1, 0, 1\} \). We denote by \( \mathcal{T}_r(d, j) \) the unique rooted tree (up to isomorphism) satisfying the following specifications:
• The root \(v_0\) of \(T_r(d, j)\) has degree \(d + j\),
• Every vertex \(v\) of \(T_r(d, j)\) satisfies \(\text{dist}(v, v_0) \leq r\) (the tree has depth \(r\)), and
• For all vertices \(v\) of \(T_r(d, j)\), \(\text{dist}(v, v_0) \in (0, r)\) implies \(\text{deg} v = d + 1\).

**Definition 5.2.2.** A **quasipolar condition** on \(T_r(d, j)\) is a vertex set \(Q\) on \(T_r(d, j)\) such that

• \(Q\) contains the root \(v_0\), and
• For all \(v \not\in Q\) we have either \(\text{deg}(v, Q) = \sum_{v' \in Q} \text{deg}(v, v') \neq 1\) or \(\text{dist}(v, v_0) = r\).

In colloquial terms, if a vertex \(v\) of \(T_r(d, j)\) has exactly one neighbor in \(Q\), either \(v \in Q\) or \(v\) is a leaf.

**Lemma 5.2.3.** If \(Q\) is a quasipolar condition on \(T_r(d, j)\), then

\[
|Q| \geq 1 + (d + j) \sum_{i=0}^{\lfloor r/2 \rfloor - 1} d^i
\]

**Proof.** We proceed by induction on \(r\). If \(r \leq 1\), the conclusion is vacuous, so we will assume that \(r \geq 2\). When \(r = 2\), then for all \(v_1 \in \mathcal{V}(G)\) with \(\text{dist}_G(v_0, v_1) = 1\), either \(v_1 \in Q\), or there is \(v_2 \in \mathcal{V}(G)\) satisfying \(v_2 \neq v_0\) and \(v_0 \leftrightarrow v_1 \leftrightarrow v_2 \in Q\). Hence \(|Q| \geq 1 + \text{deg}_G(v_0) = 1 + (d + j)\) by the definition of a quasipolar condition.

When \(r \geq 3\), let \(Y = \{ v \in Q : \text{dist}_G(v, v_0) \in \{1, 2\} \}\); we have \(|Y| \geq d + j\) (by the argument in the case \(r = 2\)). For each \(y \in Y\), let \(T_y\) be the subtree of \(T_r(d, j)\) whose vertex set consists of the descendants of \(y\) in the rooted tree \(T_r(d, j)\). Members of \(\{T_y\}_{y \in Y}\) are pairwise disjoint (as subgraphs of \(G\)), and each is isomorphic to either \(T_{r-1}(d, 0)\) or \(T_{r-2}(d, 0)\). The restriction of \(Q\) to each \(T_y\) is a quasipolar condition, so by induction we have

\[
|Q| \geq 1 + \sum_{y \in Y} \left( 1 + d \sum_{i=0}^{\lfloor (r-2)/2 \rfloor - 2} d^i \right) \geq 1 + (d + j) \sum_{i=0}^{\lfloor (r-1)/2 \rfloor - 1} d^i.
\]

\[
|Q| \geq 1 + \sum_{y \in Y} \left( 1 + d \sum_{i=0}^{\lfloor (r-2)/2 \rfloor - 2} d^i \right) \geq 1 + (d + j) \sum_{i=0}^{\lfloor (r-2)/2 \rfloor - 1} d^i.
\]

\[ \square \]

**Definition 5.2.4.** Let \(G\) be a directed graph. A **polar condition** on \(G\) is a nonempty \(\Pi \subset \mathcal{V}(G)\) such that for all \(v \in \mathcal{V}(G) \setminus \Pi\), we have \(\text{deg}(v, \Pi) = \sum_{v' \in \Pi} \text{deg}(v, v') \neq 1\).

Colloquially, if \(v\) is a vertex of \(G\) and there is a unique arc \(v \rightarrow \Pi\), then \(v \in \Pi\).
**Example 5.2.5.** If $G$ is a finite undirected graph and $f : V(G) \to R$ is an eigenfunction for the adjacency matrix of $G$ (for $R$ a ring) with a nonzero eigenvalue, then

$$V(G) \setminus D_f = \{ v \in V(G) : f(v) \neq 0 \}$$

is easily seen to be a polar condition on $G$.

The following is nearly trivial, but should be mentioned:

**Lemma 5.2.6.**

a. A union of polar conditions on a graph is a polar condition.

b. If $\Pi$ is a polar condition on a graph $G$ and $G' \subset G$ is a connected component of $G$, then $\Pi \cap V(G')$ is either empty or a polar condition on $G'$.

Our next result shows that the same lower bound of Lemma 5.2.3 applies to polar conditions on undirected graphs $G$ that admit certain embeddings $T_r(d,j) \hookrightarrow G$.

**Lemma 5.2.7.** Let $G$ be an undirected graph, let $\Pi \subset V(G)$ be a polar condition on $G$, and let $r \geq 2$. Suppose that for some $v_0 \in \Pi$, one of the following conditions holds:

i. The rooted graphs $(G',v_0) = N_r(G,v_0)$ and $T_r(d,j)$ are isomorphic,

ii. There is an edge $e$ adjacent to $v_0$ such that the rooted graphs $(G',v_0) = N_r(G \setminus \{e\},v_0)$ and $T_r(d,j)$ are isomorphic, or

iii. $N_r(G,v_0)$ contains a unique cycle $x$, $v_0$ lies on $x$, and the rooted graphs $(G',v_0) = N_r(G \setminus E(x),v_0)$ and $T_r(d,j)$ are isomorphic.

Then $|\Pi \cap V(G')| \geq 1 + (d + j) \sum_{i=0}^{\lceil r/2 \rceil - 1} d^i$.

*Proof.* Let $E$ be the set of edges deleted in conditions (ii.) and (iii.) so that $(G',v_0) = N_r(G \setminus E,v_0)$ is isomorphic to $T_r(d,j)$ by hypothesis. With $E$ chosen as above, the restriction of $\Pi$ to $(G',v_0) \simeq T_r(d,j)$ is a quasipolar condition. \qed

### 5.3 The technical lemma

Finally, we will combine our structural results on isogeny graphs with the lower bound on polar conditions $\Pi$ on $G_\ell(N,F)$. We begin by showing that it suffices to prove such a result for the derived isogeny graph $G'_\ell(N,F)$.

**Lemma 5.3.1.** Let $G$ be a connected component of $G_\ell(N,F)$ and let $G'$ the corresponding component of $G'_\ell(N,F)$. Note that $V(G) = V(G')$.

a. If $\Pi'$ is a polar condition on $G'$, then $\Pi'$ is a polar condition on $G$.

b. If $\Pi$ is a polar condition on $G$, then there exists a polar condition $\Pi'$ on $G'$ such that $\Pi \subset \Pi'$ and $\Pi' \setminus \Pi \subset W_G$. 

32
Proof. Let $S$ be any subset of $V(G) = V(G')$. By Proposition 4.1.4, $\deg_G(\tau, S) = \deg_{G'}(\tau, S)$ whenever $\tau$ is nonelliptic. Both claims follow easily from this statement.

We call a vertex $\tau$ of $G'_L(N; F)$ admissible if it is nonelliptic and it does not lie on any cycles of length 1 or 2.

**Lemma 5.3.2.** Let $G$ be a component of $G'_L(N; F)$, and let $\Pi \subset V(G)$ be a polar condition. Assume either that $G$ is ordinary or that $G = G'_L(N; \mathbb{F}_p)$, $4\ell^8 < Np$, and $4\ell^4 < p$. There exists $\tau \in \Pi$ such that $\tau$ is admissible.

*Proof.* This follows from standard arguments using Corollary 4.3.4 and Lemma 4.3.5.

**Lemma 5.3.3.** Let $G$ be a connected component of the full isogeny graph $G'_L(N; F)$, let $\Pi \subset V(G)$ be a polar condition, and let $n \geq 2$. Assume either that $G$ is ordinary or that $G = G'_L(N; \mathbb{F}_p)$ with $4\ell^{4n} < Np$ and $4\ell^{2n} < p$.

Under these hypotheses, $\Pi$ contains at least $\ell^{\lceil n/2 \rceil} + \ell^{\lceil n/2 \rceil - 1}$ nonelliptic points.

*Proof.* In light of Lemma 5.3.1, it is sufficient to prove the lower bound upon replacing $G'_L(N; F)$ with $G'_L(N; F)$ by Lemma 5.3.2, we may fix $\tau \in \Pi$ such that $\tau$ is admissible.

Let $G_1 = N_n(G, \tau)$. We will apply Lemma 5.1.2 to the structure of $G_1$ freely and without comment. We have the following cases:

a. $G_1$ is acyclic and contains no elliptic points: Then $(G_1, \tau)$ is isomorphic to $T_n(\ell, 1)$ as a rooted graph, so by Lemma 5.2.7,

$$|\Pi \cap V(G_1)| \geq 1 + (\ell + 1) \sum_{i=0}^{\lceil n/2 \rceil - 1} \ell^i > \ell^{\lceil n/2 \rceil} + \ell^{\lceil n/2 \rceil - 1},$$

and $\Pi \cap V(G_1)$ contains no elliptic points.

b. $G_1$ is acyclic and contains a single elliptic point: Let $\tau'$ denote the unique elliptic point of $G_1$ and note that because $G_1$ is acyclic, there is a unique shortest path from $\tau$ to $\tau'$ in $G_1$. Let $e$ be the first edge in this path (so $e$ is adjacent to $\tau$) so that $(G_1, \tau) = N_n(G \setminus \{e\}, \tau)$ is isomorphic to $T_n(\ell, 0)$ as a rooted graph, so condition (ii.) in the statement of Lemma 5.2.7 holds,

$$|\Pi \cap V(G_1)| \geq 1 + \ell \sum_{i=0}^{\lceil n/2 \rceil - 1} \ell^i = \sum_{i=0}^{\lceil n/2 \rceil} \ell^i \geq \ell^{\lceil n/2 \rceil} + \ell^{\lceil n/2 \rceil - 1},$$

and $G_1$ contains no elliptic points.

c. $G_1$ is monocyclic and contains a single elliptic point: Under these conditions, the unique cycle of $G_1$ is a loop based at the elliptic point (Lemma 5.1.2.c). We may therefore proceed as in the previous case.
d. $G_1$ is monocyclic and contains no elliptic points: Let $x$ be the unique cycle of $G_1$.  
If $\tau \notin \mathcal{V}(x)$, then we may proceed as in case (b).
If instead $\tau \in \mathcal{V}(x)$, then $|x| \geq 3$ (by the admissibility of $\tau$). We write

\[ x : \tau = \tau_1 \rightarrow \tau_2 \rightarrow \cdots \rightarrow \tau_{|x|} \rightarrow \tau_1, \]

and observe that $(G', \tau) = \mathcal{N}_n(G \setminus E(x), \tau)$ is isomorphic to $T_n(\ell, -1)$:

(In the figure above and those below, gray vertices are those we know are elements of $\Pi$. The subgraphs in bold are those that we assert are isomorphic to the rooted tree in question.) Case (iii.) of Lemma 5.2.7 holds, so $|\Pi \cap \mathcal{V}(G')| \geq \ell^{|n/2|}$.

Since $\Pi$ is a polar condition, we also have one of the following subcases:

- $\tau_2 \in \Pi$ and $\mathcal{N}_{n-1}(G \setminus E(x), \tau_2) \simeq T_{n-1}(\ell, -1)$:

- There is an edge $e : \tau_2 \rightarrow \tau'_2 \in \Pi$ for $\tau'_2$ lying outside of the cycle $x$ and $\mathcal{N}_{n-2}(G \setminus E(x) \cup \{e\}, \tau'_2) \simeq T_{n-2}(\ell, 0)$:
Each of these subcases verifies one of conditions (ii.) or (iii.) of Lemma 5.2.7. Let 
\((G'', \tau'') = N_{n-i}(G \setminus E(x), \tau_3) \simeq T_{n-2}(\ell, -1)\) or \(T_{n-1}(\ell, -1)\):

Remark 5.3.4. One can almost certainly improve the bounds in cases (c.) and (d.) in
the above proof by combining Corollary 4.3.4 with increasingly intricate combinatorial
arguments. However, the bound \(|\Pi \cap V(G_1)| \geq 1 + (\ell + 1) \sum_i \ell_i\) obtained in case (a.)
appears to be as sharp as our current approach will permit.

Corollary 5.3.5. If \(G\) is an ordinary component of \(G_\ell(N; F)\) and \(\Pi\) is a polar condition
on \(G\), then \(\Pi\) is infinite.
Chapter III

Hecke stability

The Hecke stability method (HSM) is a technique for computing spaces of modular forms that exploits the action of the Hecke operators on these spaces. The main purpose of this method is to compute bases for the elusive spaces of weight 1 modular forms both in the classical setting and over finite fields.

The Hecke stability method is based on the following non-rigorous principle:

A finite-dimensional subspace \( V \subset \mathbf{M}_k^{\text{frac}}(N; F) \) that is stable under the action of a Hecke operator \( T_\ell \) should consist of modular forms (i.e., without poles).

Unfortunately, this preliminary statement is overly naïve (indeed counterexamples can be constructed easily in characteristic \( p \) using the Hasse invariant, see Proposition 1.6.4). What is true instead is that such a space \( V \) must consist of fractional modular forms whose poles are restricted to the supersingular locus of \( X_1(N)_F \). Consequently, the principle is correct unconditionally when \( F = \mathbb{C} \), but to compute weight 1 modular forms when \( F = \overline{F}_p \), we must apply this idea with more care.

Section 6 contains the main theorem of this chapter, Theorem 6.2.1, which describes general conditions under which a space \( V \) as above consists of modular forms. In Section 7 we apply this Hecke stability theorem to the specific problem of computing weight 1 modular forms over a given field. In addition to giving a formal implementation of the HSM in this particular situation, we will provide additional computational techniques that assist in verifying its output. Finally, in Section 8, we present the extended Hecke stability method, whose purpose is to compute spaces of weight 1 modular forms while taking into account the existence of ethereal characteristics.

6 The Hecke stability theorem

6.1 Preparation

To illustrate the intuition behind the Hecke stability theorem, we begin with a simple example:
Example 6.1.1. Let \( N = 7n \) and let \( \varepsilon_7 : (\mathbb{Z}/7n\mathbb{Z})^\times \to \{ \pm 1 \} \) denote the quadratic character of conductor 7. Recall that for a fixed principal cusp \( \mathfrak{c} \) there exists a modular form \( \lambda_{\varepsilon_7} \in M_1(7n, \varepsilon_7; \mathbb{Z}) \) whose \( q \)-expansion is

\[
\lambda_{\varepsilon_7}(q) = 1 + 2 \sum_{n=1}^{\infty} \sum_{m|n} \varepsilon_7'(m)q^n
\]

where \( \varepsilon_7' : (\mathbb{Z}/7\mathbb{Z})^\times \to \{ \pm 1 \} \). By Example 3.3.1, \( jZ(\lambda_{\varepsilon_7}) = \emptyset \). Hence, for \( F = \mathbb{Q} \) or \( F = \mathbb{F}_p \) (with \( p \nmid 14 \)), elements of

\[
V = \lambda_{\varepsilon_7}^{-1}M_2(7n, 1; F)
\]

are fractional modular forms that may have poles over \( j = 0 \). \( M_1(7n, \varepsilon_7; F) \) is the subspace of \( V \) consisting of those elements that do not have any poles, but how do we identify such forms?

Arguing as in Example 2.1.1, when \( F \notin \{ \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_{11} \} \) we have \( E_{54000} \nmid E_0 \) over \( F \) and there is a unique 2-isogeny \( E_{54000} \to E_0 \) over \( F \). Applying Corollary 2.2.3 we observe that if \( f \) has a pole (necessarily above \( j = 0 \)), then \( T_2f \) has a pole above \( j = 54000 \). In particular, \( \lambda_{\varepsilon_7} \cdot T_2f \) has a pole, so \( \lambda_{\varepsilon_7} \cdot T_2f \notin M_2(7n, 1; F) \), so \( T_2f \notin V \). Thus, we obtain

\[
M_1(7n, \varepsilon_7; F) = \{ f \in V : T_2f \in V \}.
\]

Slightly more delicate arguments (working with \( \Gamma_0(7) \)-structures instead of just \( \Gamma(1) \)-structures) extend the above to the cases \( F = \mathbb{F}_5 \) and \( F = \mathbb{F}_{11} \). The point is that the set on the right-hand side is easy to compute in terms of \( q \)-expansions.

We would like to generalize the above example so that we can apply the same ideas to any finite-dimensional \( V \subset M_1^{\text{frac}}(N; F) \). Of course, the situation in the example above is overly simple. For example, the set

\[
\Pi(V) = \{ \tau \in Y_1(N)_F : \text{there exists } f \in V \text{ such that } \text{ord}_\tau(f) < 0 \}
\]

is very small in Example 6.1.1 (its projection to the \( j \)-line consists of a single point), but it can of course be arbitrarily large in the general case. The purpose of Chapter II was to generalize the crucial “pole propagation” step above where we invoked Corollary 2.2.3.

Lemma 6.1.2. Let \( k \geq 1 \), let \( N \geq 5 \), and let \( F = \mathbb{C} \) or \( F = \mathbb{F}_p \) with \( p \nmid N \), and let \( \ell \) be a prime that does not divide \( N \) and that is not the characteristic of \( F \).

Suppose that \( V \subset M_1^{\text{frac}}(N; F) \) is invariant under the action of the Hecke operator \( T_\ell \). Let

\[
\Pi(V) = \{ \tau \in Y_1(N)_F : \text{there exists } f \in V \text{ such that } \text{ord}_\tau(f) < 0 \},
\]

and let \( N' \mid N \). If \( \Pi(V) \) is nonempty, then \( \beta_{N,N'}\Pi(V) \) (where \( \beta_{N,N'} \) is defined as in Section 1.1) is either empty or a polar condition on the full isogeny graph \( \mathcal{G}_\ell(N'; F) \).
Proof. Suppose that \( \tau \in \beta_{N,N'} \Pi(V) \), let \( G \) be the connected component of \( \mathcal{G}_\ell(N';F) \) with \( \tau \in \mathcal{V}(G) \), and suppose that we have \( \deg_G(\tau, \beta_{N,N'} \Pi(V)) = 1 \). We must show that \( \tau \in \beta_{N,N'} \Pi(V) \).

Let \( \tau_0 \in \beta_{N,N'} \Pi(V) \) be the unique vertex so that \( \tau \to G \tau_0 \), and let \( \phi : (E,C) \to (E_0,C_0) \) be an isogeny of degree \( \ell \) that represents this arc. Fix a \( \Gamma_1(N) \)-structure \((E_0,P_0)\) so that \((E_0,C_0) = (E_0,\left(\frac{N}{N'}P_0\right)) \) and \( \text{ord}_{E_0,P_0}(f) < 0 \). By Lemma 1.1.1, there exists a point \( P \in E[N] \) of order \( N \) and an \( \ell \)-isogeny \( \psi : (E,P) \to (E_0,P_0) \) such that

\[
(E,P) \xrightarrow{\psi} (E_0,P_0) \\
\beta_{N,N'} \downarrow \\
(E,C) \xrightarrow{\phi} (E_0,C_0)
\]

commutes.

Let Hecke\(_\ell([E,P]) = [E_0,P_0] + \cdots + [E_\ell,P_\ell] \), and note that by the uniqueness assumption on \( \tau \to G \tau_0 \), we have

\[
[E_0,P_0] \in \Pi(V), \quad \text{and for all } i \neq 0, [E_i,P_i] \notin \Pi(V).
\]

Therefore, by Corollary 2.2.3, we have \( \text{ord}_{[E,P]}(T_\ell f) < 0 \). Since \( T_\ell f \in V \), we have \([E,P] \in \Pi(V)\), hence \( \tau \in \beta_{N,N'} \Pi(V) \), as desired. \( \square \)

6.2 Statement, proof, and consequences

Theorem 6.2.1. Let \( k \geq 1 \), let \( N \geq 5 \), and let \( F = \mathbb{C} \) or \( \overline{\mathbb{F}}_p \) with \( p \nmid N \).

Suppose that \( V \subset M_k^{\text{frac}}(N;F) \) is a finite-dimensional subspace that is stable under the action of the Hecke operator \( T_\ell \) for some prime \( \ell \) that is distinct from the characteristic of \( F \) and that does not divide \( N \). If either

i. \( \Pi(V) \cap X_1(N)_{F}^{\text{ss}} \) is empty, or

ii. \( F = \overline{\mathbb{F}}_p \) and there exist \( N' \mid N \) and \( n \geq 2 \) such that \( 4\ell^{4n} < N'p \), \( 4\ell^{2n} < p \), and

\[
|\{ \tau \in \beta_{N,N'} \Pi(V) : \tau \text{ is supersingular and } w(\tau) = 1 \}| < \ell^{[n/2]} + \ell^{[n/2]−1},
\]

then \( V \subset M_k(N;F) \).

Proof. We already know that if \( V \subset M_k^{\text{frac}}(N;F) \) is finite-dimensional and \( T_\ell \)-stable, then for all \( f \in V \) and all cusps \( \mathfrak{c} \in X_1(N)_{F} \), \( \text{ord}_\mathfrak{c}(f) \geq 0 \) (this is Corollary 2.3.5).

By the bounds in Lemma 5.3.3 and the fact that \( \Pi(V) \) is a polar condition if it is nonempty (Lemma 6.1.2), either condition in the statement of the theorem implies that \( \beta_{N,N'} \Pi(V) \) must be empty. It follows that \( \Pi(V) \) is empty, so \( V \subset M_k(N;F) \). \( \square \)
Proof. Claim (a.) is a special case of the main theorem, since the Hecke operators respect the \( \mathbb{Z} \)-grading \( M(k)^{\text{frac}}(N; F) \).

For claim (b.) we note that every part of the argument used to prove part (a.) adapts to the setting of \( F \)-algebras except for Corollary 2.3.5. \( \square \)

**Corollary 6.2.2.** If \( V \subset M(k)^{\text{frac}}(N, \chi; \mathbb{C}) \) is finite-dimensional and stable under the action of a Hecke operator \( T_{\ell} \) (for \( \ell \nmid N \)), then \( V \subset M(k)(N, \chi; \mathbb{C}) \).

**Corollary 6.2.3.** If \( V \subset M(k)^{\text{frac}}(N, \chi; \overline{\mathbb{F}_p}) \) is finite-dimensional and stable under the action of a Hecke operator \( T_{\ell} \) (for \( \ell \nmid NP \)), then elements of \( V \) may have poles only on the supersingular locus.

Therefore, there exists \( t \geq 0 \) such that \( \tilde{G}_{p-1}^0 \subset V \subset M(k, (p-1)t)(N, \chi; \overline{\mathbb{F}_p}) \), so the image of \( V \) under \( q \)-expansion at any cusp \( \kappa \) is contained in the image of \( M(k, (p-1)t)(N, \chi; \overline{\mathbb{F}_p}) \) under that same \( q \)-expansion map.

**Proof.** The second part of the claim is an application of Proposition 1.6.4. \( \square \)

### 7 Computing weight 1 modular forms

Though it can be applied in more general settings, the particular utility of the Hecke stability theorem is that it can be used to compute spaces of weight 1 modular forms.

When \( k \geq 2 \), \( M(k)(N; F) \) can be computed using modular symbols algorithms (see Theorem 3.1.1). These methods do not adapt to the case \( k = 1 \). Furthermore, as we will see in Section 8, we must account for ethereal characteristics: primes \( p \) for which \( M(k)(N; \mathbb{Z}[\frac{1}{N}]) \to M(k)(N; \mathbb{F}_p) \) is not surjective. The Hecke stability algorithm has been designed with the existence of ethereal characteristics in mind (see Section 8.2).

#### 7.1 Application of the Hecke stability theorem

In this section, we fix a level \( N \geq 5 \) and we take \( F = \mathbb{C} \) or \( F = \overline{\mathbb{F}_p} \) with \( 2N \) nonzero in \( F \). Let \( \chi : (\mathbb{Z}/N\mathbb{Z})^* \to F^* \) be an odd character, and let \( A \subset M_1(N, \chi^{-1}; F) \) be a nonempty finite set of auxiliary forms (e.g., \( A = \{ \lambda_\chi \} \) where \( \lambda_\chi \) is the form defined in Proposition 1.6.5). Our goal is to compute a basis for \( M_1(N, \chi; F) \) using the Hecke stability theorem.

We now introduce some notation that will prevail throughout the remainder of our work. Let \( V^{(0)}_{\ell}(N; F; A) = \bigcap_{\lambda \in A} \lambda^{-1} M_2(N, 1; F) \) and for every \( i \geq 1 \), define

\[
V^{(i+1)}_{\ell}(N; F; A) = \{ f \in V^{(i)}_{\ell}(N; F; A) : T_{\ell}f \in V^{(i)}_{\ell}(N; F; A) \}.
\]

We will occasionally drop the arguments \( (N; F; A) \) where the choice of these data is obvious from context. Clearly, \( V^{(\infty)}_{\ell} = \bigcap_i V^{(i)}_{\ell} \) is the maximal \( T_{\ell} \)-stable subspace of \( V^{(0)}_{\ell} \). Since \( V^{(0)}_{\ell} \) is finite-dimensional, there is \( n \) such that \( V^{(n)}_{\ell} = V^{(n+1)}_{\ell} = \cdots = V^{(\infty)}_{\ell} \).

Our next goal is to provide conditions under which \( V^{(\infty)}_{\ell} = M_1(N, \chi; F) \) by applying Theorem 6.2.1.
Theorem 7.1.1. Let $N \geq 5$, let $F = \mathbb{C}$ or $\overline{\mathbb{F}}_p$ for $p \nmid 2N$, and let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be odd. Let $A \subset \mathcal{M}_1(N, \chi^{-1}; F) \setminus \{0\}$ be finite and nonempty, and let $Z(A) = \bigcap_{\lambda \in A} Z(\lambda)$.

Let $\ell$ be a prime that is not the characteristic of $F$ and that does not divide $N$. We have $V_{\ell}^{(\infty)}(N; F; A) = \mathcal{M}_1(N, \chi; F)$ if one of the following conditions holds:

i. $Z(A)$ contains no supersingular points,

ii. $F = \overline{\mathbb{F}}_p$ and there exists $n \geq 2$ such that $4\ell^{4n} < f_\chi p$, $4\ell^{2n} < p$, and

$$|\{ \tau \in \beta_{N, f_\chi} Z(A) : \tau \text{ is supersingular and } w(\tau) = 1 \}| < \ell^{[n/2]} + \ell^{[n/2]-1},$$

or

iii. $F = \overline{\mathbb{F}}_p$ and there exists $n \geq 2$ such that $4\ell^{4n} < p$ and

$$|\{ j_0 \in jZ(A) : j_0 \text{ is supersingular and } j_0 \neq 0, 1728 \}| < \ell^{[n/2]} + \ell^{[n/2]-1},$$

where $j : [\Gamma_1(N)]_F \to F$ is the $j$-invariant map $(E, P) \mapsto j(E)$.

Proof. Since $V_{\ell}^{(\infty)} \subset V_{\ell}^{(0)}$ and $\Pi(V_{\ell}^{(0)}(N; F; A)) \subset Z(A)$, this is just a special case of Theorem 6.2.1.

Recall that in Section 3.3 we gave an algorithm that can be used to determine $jZ(A)$, and Proposition 1.4.1.c can be used to provide bounds on the size of $\beta_{N, \chi} Z(A)$. For “standard” choices of $A$ (see Remark 7.2.8), the following bound is quite useful:

Corollary 7.1.2. Suppose that $A$ contains an element of the form $\delta^* \lambda$ where $\delta : [\Gamma_1(N)]_F \to [\Gamma_1(f_\chi)]_F$ is the degeneracy map induced by $(E, P) \mapsto (E, \chi e_1 P)$ and $\lambda \in \mathcal{M}_1(f_\chi, \chi^{-1}; F)$. Then

$$|\{ \tau \in \beta_{N, f_\chi} Z(A) : \tau \text{ is supersingular and } w(\tau) = 1 \}| \leq \frac{\text{SL}_2(\mathbb{Z}) : \Gamma_0(f_\chi)}{12}.$$ 

Proof. Let $\lambda' \in A$ satisfy $\lambda' = \delta^* \lambda$ and note that $\beta_{N, f_\chi} Z(\lambda') = \pi_{f_\chi} Z(\lambda)$, so it is enough to bound $\pi_{f_\chi} Z(\lambda)$.

Suppose that $k = \text{ord} \chi$ so that $\lambda^k \in \mathcal{M}_k(f_\chi, 1; F)$. By standard degree calculations (see e.g., [Mil97] Proposition 4.12), $\lambda^k$ has $\frac{1}{12}[\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ zeros, accounting for multiplicity and ellipticity. Since every nonelliptic zero of $\lambda^k$ has order a multiple of $k$, we have

$$|\{ \tau \in \pi_{f_\chi} Z(\lambda) : w(\tau) = 1 \}| = |\{ \tau \in Z(\lambda^k) : w(\tau) = 1 \}| \leq \frac{[\text{SL}_2(\mathbb{Z}) : \Gamma_0(f_\chi)]}{12}$$

from which the bound follows.

Corollary 7.1.3. Let $N \geq 5$, let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be an odd Dirichlet character, let $K = \mathbb{Q}(\chi)$. Fix a prime $\ell$ and $n \geq 2$ such that $\ell \nmid N$ and $\frac{1}{12}[\text{SL}_2(\mathbb{Z}) : \Gamma_0(f_\chi)] < \ell^{[n/2]} + \ell^{[n/2]-1}$.

If $p$ is a prime such that $p \nmid \ell N$ and $p > \max\{\frac{4\ell^{4n}}{f_\chi}, 4\ell^{2n}\}$, we have

$$V_{\ell}^{(\infty)}(N; \overline{\mathbb{F}}_p; \{\lambda_{\bar{\chi}}\}) = \mathcal{M}_1(N, \bar{\chi}; \mathbb{F}_p)$$

for every prime $p \subset \mathcal{O}_K$ over $p$, where $\bar{\chi}$ denotes the reduction of $\chi$ modulo $p$.

\footnote{The author believes strongly that these bounds can be improved drastically.}
7.2 Formal implementation

We continue with our choices of $N, F, \chi$ from the previous section. For computational purposes, we also fix the following data:

- A cusp $c \in X_1(N)_F$; all $q$-expansions henceforth will tacitly be $q$-expansions at this cusp (we will drop the superscript),
- A finite nonempty $A \subset M_1(N, \chi^{-1}; F) \setminus \{0\}$ such that for each $\lambda \in A$ the $q$-expansion $\lambda(q)$ can be computed to arbitrary precision (such as $A = \{\lambda_\chi\}$),
- a prime $\ell$ that does not divide $N$ and that is different from char $F$, and
- $P \geq 0$ (the precision).

As before, let

$$V_\ell^{(0)}(N; F; A) = \bigcap_{\lambda \in A} \lambda^{-1}M_2(N, 1; F)$$

and let $V_\ell^{(\infty)}(N; F; A)$ denote the largest subspace of $V_\ell^{(0)}(N; F; A)$ that is stable under the action of the Hecke operator $T_\ell$. Our goal is to compute $V_\ell^{(\infty)}$ in terms of an image of a basis $B$ under the truncated $q$-expansion map $M_1(N, \chi; F) \rightarrow F[[q]]/(q^P)$. So long as we choose $P \geq \text{Sturm}(N)$, the image of this basis is itself linearly independent over $F$.

For reasons that will become clear in Section 8, we would like to compute a basis for $V_\ell^{(\infty)}(N; F; A)$ in a way that is as integral as possible. Hence, let $O_A$ be the subring of $F$ obtained by adjoining the coefficients of the Laurent series $\{1/\lambda(q)\}_{\lambda \in A}$ to the image of $\mathbb{Z}[\frac{1}{N}] \rightarrow F$. For example, if $F = \mathbb{C}$ and $A = \{\lambda_\chi\}$, then $O_A = \mathbb{Z}[\frac{1}{N}, \frac{1}{\ell}, \chi]$ where $L_\chi$ is the constant defined in Lemma 1.6.5. In the spirit of Proposition 1.3.1, we denote by $M_1^{\text{frac}}(N, \chi; O_A)$ the $O_A$-submodule of $M_1^{\text{frac}}(N, \chi; F)$ consisting of those forms whose $q$-expansions (at the chosen cusp) have coefficients in $O_A$.

Algorithm 7.2.6 below produces a basis $B_1^{(i)}$ for each term in the descending sequence

$$V_\ell^{(0)}(N; F; A) \supset \cdots \supset V_\ell^{(\infty)}(N; F; A)$$

of $F$-vector spaces such that $B_1^{(i)} \subset M_1^{\text{frac}}(N, \chi; O_A)$ (note that the above sequence eventually stabilizes, since the initial space is finite-dimensional).

Since we will be working with $q$-expansions of fractional modular forms, we must be careful to compute these expansions to sufficiently high precision. Thus, we will require a version of Proposition 1.4.4 for fractional modular forms:

**Lemma 7.2.1.** Let $f_1, f_2 \in M_1^{\text{frac}}(N, \chi; F)$, and suppose that $f_1$ and $f_2$ have a common denominator $h \in M_k(N, \theta; F)$ where $k \geq 0$ and $\theta : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow F$ is a character of the same parity as $k$. If

$$f_1(q) \equiv f_2(q) \mod q^{\text{Sturm}(k+1)(N)},$$

then $f_1 = f_2$. 

41
Algorithm 7.2.2. The following procedure on input \((N, F, \chi, A, P)\) (with notation as above) produces a basis \(B_1^{(0)} \subset M_2^{\mathrm{frac}}(N, \chi; O_A)\) for the space \(V_1^{(0)}(N; F; A)\) in terms of its image under \(q\)-expansion \(M_1^{\mathrm{frac}}(N, \chi; F) \rightarrow F[[q]]/(q^P)\) (the output is a finite subset of \(O_A[[q]]/(q^P)\)).

1. Let \(P' \leftarrow \max\{P, \text{Sturm}(N)\}\).

2. Using the algorithm of Theorem 3.1.1, compute a basis \(B_0\) for \(M_2(N, 1; \mathbb{Z}[\frac{1}{N}])\) in terms of its image under the map \(M_2(N, 1; \mathbb{Z}[\frac{1}{N}]) \rightarrow O_A[[q]]/(q^{P'})\). Let \(d, e \leftarrow |B_0|\).

3. Compute \(q\)-expansions of the elements of \(A\) to precision \(P'\) (with coefficients in \(O_A\) by hypothesis), let \(r \leftarrow |A|\), and enumerate \(A = \{\lambda_1(q), \ldots, \lambda_r(q)\}\). Let \(t \leftarrow 1\).

4. Let \(B \leftarrow \{g(q)/\lambda_i(q) : g \in B_0\}\) (with \(q\)-expansions to precision \(P'\)).

5. If \(t = r\), then return \(B\) (truncated to precision \(P\) if necessary).

   Else, let \(B' \leftarrow \{g(q)/\lambda_{t+1}(q) : g \in B_0\}\), enumerate \(B = \{f_1(q), \ldots, f_d(q)\}\) and \(B' = \{f'_1(q), \ldots, f'_d(q)\}\), and form the matrix \(M \subset O_A^{[1, d+e] \times [0, P')}\) such that

   \[
   M_{ij} = \begin{cases} 
   a_j(f_i) & \text{for } i \in [1, d] \text{ and } j \in [0, P'), \text{ and} \\
   a_j(f'_{i-d}) & \text{for } i \in [d+1, d+e] \text{ and } j \in [0, P').
   \end{cases}
   \]

6. Compute a basis \(S \subset O_A^d \times \mathbb{F}^e\) for \(\ker M\), let \(\iota : \ker M \rightarrow O_A[[q]]/(q^{P'})\) be the map

   \[
   \iota(x_1, \ldots, x_d, y_1, \ldots, y_e) \mapsto \sum_{i=1}^d x_i f_i(q)
   \]

   and let \(B \leftarrow \iota(S)\). Increment \(t \leftarrow t + 1\), let \(d \leftarrow |B|\), and goto Step 5.

Proof. An easy exercise in linear algebra shows that at Step 5 the set \(B\) is a basis (in terms of \(q\)-expansions with coefficients in \(O_A\) to precision \(P'\)) for the space \(\bigcap_i^{d+e} M_2(N, 1; F)\). \(\square\)

\(^2\)For example, compute a basis over the fraction field of \(O_A\) and then scale.
Remark 7.2.3. The space \( V_\ell^{(0)}(N; F; A) \) does not depend on \( \ell \). In some cases (and often over \( F = \mathbb{C} \)), the set \( A \) of auxiliary forms can be chosen so that \( Z(A) \) is empty, in which case \( V_\ell^{(0)}(N; F; A) = M_1(N, \chi; F) \) automatically.

Because the computation of \( V_\ell^{(0)} \) requires a lower precision than the computation of \( V_\ell^{(\infty)} \) due to its independence from \( \ell \) (see next lemma), it is advisable to run Algorithm 7.2.2 and then check whether the equality \( V_\ell^{(0)}(N; F; A) = M_1(N, \chi; F) \) holds using the methods of Section 7.3. If this certification step fails, we can extend out computation of the initial space to the precision required by Algorithm 7.2.6 and then proceed.

For the extended Hecke stability method (and especially when \( f_\chi \) is prime), computing the initial space is typically insufficient (see also Example 8.2.5).

A basis for \( V_\ell^{(i+1)} \) can be easily computed from a basis for \( V_\ell^{(i)} \) using the formula in in Proposition 2.3.1 and linear algebra on \( q \)-expansions, and we may restrict our algebraic operations to \( O_A \). Again, since we are working with \( q \)-expansions of modular forms, we must be careful about the required precision:

Lemma 7.2.4. Let \( P = \text{Sturm}_{\ell+3}(N) \) (see Proposition 1.4.4). If \( f_1, f_2 \in V_\ell^{(0)} \) satisfy \( (T_\ell f_1)(q) \equiv f_2(q) \mod q^P \), then \( T_\ell f_1 = f_2 \). In other words, the map

\[
V_\ell^{(0)} \cup T_\ell V_\ell^{(0)} \longrightarrow F[[q]]/(q^P)
\]

induced by \( q \)-expansion is an injection.

Proof. Let \( \lambda \in A \) and note that the weight \( \ell + 2 \) form \( \lambda \cdot Q_\ell \lambda \) (with \( Q_\ell \) as defined in the proof of Lemma 2.2.1) is a common denominator for the elements of \( V_\ell^{(0)} \cup T_\ell V_\ell^{(0)} \).

Now apply Lemma 7.2.1. \( \square \)

Lemma 7.2.5. Suppose that \( V_\ell^{(i)} \) is d-dimensional with a basis \( B_1 = \{ f_1, \ldots, f_d \} \subset M_1^{\text{frac}}(N, \chi; O_A) \), let \( B_2 = \{ T_\ell f : f \in B_1 \} \subset M_1^{\text{frac}}(N, \chi; O_A) \), and let \( P = \text{Sturm}_{\ell+3}(N) \). Form the matrix \( M \in O_A^{[1,2d] \times [0,P]} \) such that

\[
M_{ij} = \begin{cases} 
 a_j(f_i) & \text{for } i \in [1, d] \text{ and } j \in [0, P) \\
 a_j(T_\ell f_i) & \text{for } i \in [d + 1, 2d] \text{ and } j \in [0, P).
\end{cases}
\]

The map

\[
\iota : \ker M \longrightarrow V_\ell^{(i)} : (x_1, \ldots, x_d, y_1, \ldots, y_d) \mapsto \sum_{i=1}^d y_i f_i
\]

is an injection with image \( V_\ell^{(i+1)} = \{ f \in V_\ell^{(i)} : T_\ell f \in V_\ell^{(i)} \} \).

In particular, if \( S \subset F^d \times O_A^d \) is a basis for \( \ker M \), then \( \iota(S) \) is a basis for \( V_\ell^{(i+1)} \).

Proof. The map \( \iota \) is injective because \( B_1 \) is linearly independent.

If \( s = (x_1, \ldots, x_d, y_1, \ldots, y_d) \in \ker M \), then

\[
(T_\ell \iota(s))(q) \equiv \sum_i y_i (T_\ell f_i)(q) \equiv - \sum_i x_i f_i(q) \mod q^P.
\]
Therefore, since \( \iota(s), f_1, \ldots, f_d \in V^{(0)}_\ell \) we have \( T_\ell \iota(s) = -\sum_i x_i f_i \) by Lemma 7.2.4, hence \( \iota(s) \in \{ f \in V : T_\ell f \in V \} \).

On the other hand, if \( f \in V \) and \( T_\ell f \in V \), then there exist \( x_1, \ldots, x_d, y_1, \ldots, y_d \in F \) with \( f = \sum_i y_i f_i \) and \( T_\ell f = -\sum_i x_i f_i \), so \( \sum_i x_i f_i + \sum_i y_i T_\ell f_i = 0 \), and the same is true after applying the \( q \)-expansion map \( V \to F[[q]]/(q^P) \), so \( (x_1, \ldots, x_d, y_1, \ldots, y_d) \in \ker M \).

**Algorithm 7.2.6.** The following procedure on input \( (N, F, \chi, A, \ell, P) \) (with notation as above) computes a basis \( B^{(\infty)}_1 \subset M^{\text{frac}}_1(N, \chi; \mathcal{O}_A) \) for \( V^{(\infty)}_\ell(N; F; A) \) in terms of its image under \( q \)-expansion \( M^{\text{frac}}_1(N, \chi; F) \to F[[q]]/(q^P) \).

1. Let \( P' = \max\{ P, \text{Sturm}_{\ell+3}(N) \} \).
2. Let \( t \leftarrow 0 \). Using Algorithm 7.2.2, compute a basis \( B^{(0)}_1 \subset M^{\text{frac}}_1(N, \chi; \mathcal{O}_A) \) for the initial space \( V^{(0)}_\ell(N; F; A) \) in terms of its image under \( q \)-expansion \( V^{(0)}_\ell(N; F; A) \to F[[q]]/(q^{P'}) \). Let \( d \leftarrow |B^{(0)}_1| \).
3. Compute \( B^{(t)}_2 = \{ T_\ell f : f \in B^{(t)}_1 \} \subset M^{\text{frac}}_1(N, \chi; \mathcal{O}_A) \) (in terms of \( q \)-expansions) to precision \( P' \) using the formula in Proposition 2.3.1.
4. Construct the matrix \( M^{(t)} \in \mathcal{O}_A^{[1,2d \times [0,P')] \) satisfying
   \[
   M^{(t)}_{i,j} = \begin{cases} 
   a_j(f_i) & \text{for } i \in [1,d] \text{ and } j \in [0,P') \\
   a_j(T_\ell f_i) & \text{for } i \in [d+1,2d] \text{ and } j \in [0,P').
   \end{cases}
   \]
5. If \( \dim_F \ker M^{(t)} = d \), terminate and return \( B = B^{(t)}_1 \) (truncated to precision \( P \), if necessary).
   
   Else, compute a basis \( S \subset F^d \times \mathcal{O}_A^d \) for \( \ker M^{(t)} \), let
   \[
   \iota : (x_1, \ldots, x_d, y_1, \ldots, y_d) \mapsto \sum_{i=1}^d y_i f_i \mod q^{tP'},
   \]
   and compute \( B_3 = \iota(S) \) to precision \( tP' \).
6. Increment \( t \leftarrow t + 1 \), let \( B^{(t)}_1 \leftarrow B_3 \), let \( d \leftarrow |B_3| \), and goto 3.

**Proof.** Using induction and Lemmas 7.2.4 and 7.2.5 it is easy to show that \( B^{(t)}_1 \subset M^{\text{frac}}_1(N, \chi; \mathcal{O}_A) \) is a basis for \( V^{(t)}_\ell(N; F; A) \) and that the algorithm terminates with \( t = n \) precisely when \( V^{(n)}_\ell(N; F; A) \) is closed under the action of \( T_\ell \).

**Corollary 7.2.7.** Let \( P = \text{Sturm}_{\ell+3}(N) \). If \( N, F, \chi, A, \ell \) satisfy one of the conditions in Theorem 7.1.1, then on input \( (N, F, \chi, A, \ell, P) \), Algorithm 7.2.6 computes \( M^{(1)}_1(N, \chi; F) \) in terms of a basis for its image under \( q \)-expansion \( M^{(1)}_1(N, \chi; F) \to F[[q]]/(q^P) \).
Remark 7.2.8. In practice, given the data $(N, F, \chi)$, we usually take $A$ to be the set of primitive weight 1 Eisenstein series of character $\chi^{-1}$ (as defined in Section 1.6). There are a few reasons for this choice:

- For almost every field $F$ as above the set $Z(A) = \bigcap_{\lambda \in A} Z(\lambda)$ contains no cuspidal zeros (proving this requires a rather tedious computation that we will not reproduce here). The presence of $f$ in the initial space with cuspidal poles increases the number of necessary iterations in Algorithm 7.2.6 drastically. The reason for this slowdown is apparent from the formula in Proposition 2.3.1 and linear algebra on (finite-tailed) Laurent series.
- When $|A| > 1$, it is often (but not always) the case that $Z(A)$ is empty. If we can prove this, then by Remark 7.2.3, we may not even need to apply Hecke stability. However, this is certainly not always the case, especially when $f_\chi$ is prime (see Examples 8.2.5 and 8.2.6). Hence, the HSM is still stronger (as an algorithm for computing modular forms) than Algorithm 7.2.2 applied alone.

Remark 7.2.9. One possible disadvantage of the Hecke stability method is that it apparently requires a relatively high level of precision for its output to be guaranteed. On the other hand, the output is a basis of $q$-expansions to that same high precision, so the requirement may not be so unfortunate after all.

Moreover, the HSM was designed to minimize auxiliary modular symbols computations needed to produce a basis for the whole space $M_1(N; F)$: It requires only that we compute the space $M_2(N, 1; F)$ to high precision once per level (rather than once per character of level $N$). It would of course be ideal to have a database of precomputed bases for $M_2(N, 1; \mathbb{Z}[[\frac{1}{N}])]$ on hand.

7.3 Certification and identification of cusp forms

Even when the conditions of Theorem 7.1.1 are not met, Algorithm 7.2.6 often produces a basis for the space of weight 1 modular forms anyway. It is therefore important to have methods to certify the desired equality $V_\ell(\infty)(N; F; A) = M_1(N, \chi; F)$ once a basis for the space on the left-hand side has been computed.

To demonstrate the need for such certification methods, we begin with an example in which the naïve version of Hecke stability stated at the beginning of this chapter fails.

Example 7.3.1. Let $g$ be the unique normalized element of $S_2(11, 1; \mathbb{F}_7)$; $g$ has $q$-expansion

$$g(q) = q \prod_{n=1}^{\infty} (1 - q^n)^2(1 - q^{11n})^2,$$

and $g(\tau) = 0$ only if $\tau$ is a cusp. Hence $f = g/\lambda_{11}$ has a pole above $j = -32^2 \equiv 6 \mod 7$ (see Example 3.3.4) so it is not a modular form. $f$ has $q$-expansion

$$f(q) = q + 3q^2 + 5q^4 + 5q^5 + 3q^6 + 2q^7 + q^8 + 3q^9 + \cdots$$
Since, for example, \( a_2(f) a_3(f) \neq a_6(f) \), \( f \) is neither a \( T_2 \)-eigenform nor a \( T_3 \)-eigenform. However, expanding further and applying the formula of Proposition 2.3.1 shows that

\[
(T_5 f)(q) = 5q + q^2 + 4q^4 + 4q^5 + q^6 + 3q^7 + 5q^8 + q^9 + \cdots = 5f(q)
\]

so \( f \) is a \( T_3 \)-eigenform. In fact, \( f \) is an eigenform for the subalgebra of \( \mathbb{T}(11; \overline{\mathbb{F}}_7) \) generated by \( \{ T_\ell : \ell = 5, 59, 113, 131, 191, \ldots \} \).

This is a failure of the naïve Hecke stability principle: \( \text{span}\{f\} \) is a finite-dimensional \( T_3 \)-stable subspace of \( \mathbf{M}_1^{\text{frac}}(11, \varepsilon_{11}; \overline{\mathbb{F}}_7) \) that does not consist of modular forms. As predicted by Theorem 6.2.1, the poles of \( f \) are limited to \( X_1(11)_{\overline{\mathbb{F}}_7}^{\text{ss}} \) (the elliptic curve \( E_{-323} \) is supersingular in characteristic 7). This pole is simple, so by Proposition 1.6.4, \( f' = \tilde{G}_6 \cdot f \) is an element of \( \mathbf{S}_7(11, \varepsilon_{11}; \overline{\mathbb{F}}_7) \) that satisfies \( f'(q) = f(q) \).

The space \( \mathbf{S}_7(11, \varepsilon_{11}; \overline{\mathbb{F}}_7) \) is 5-dimensional, and it decomposes as \( A \oplus B \) where \( A \) and \( B \) are simple Hecke modules of dimensions 4 and 1 (respectively); we have \( f' \in A \). Indeed, if \( e \in A \) is a newform, then \( f' \) is the (suitably normalized) trace of \( e \) from \( \overline{\mathbb{F}}_7(e)[[q]] \) down to \( \overline{\mathbb{F}}_7[[q]] \). The primes \( \ell \in \{ 5, 59, 113, 131, 191, \ldots \} \) at which the Hecke stability principle fails in weight 1 are precisely those primes \( \ell \) for which \( a_\ell(e) \) lies in the prime subfield \( \overline{\mathbb{F}}_7 \).

As alluded to above, one might try to certify \( V^{(\infty)}_\ell(\mathbf{N}; \mathbf{F}; A) = \mathbf{M}_1(\mathbf{N}, \chi; \mathbf{F}) \) by computing the action of the whole Hecke algebra on the space \( V^{(\infty)}_\ell(\mathbf{N}; \mathbf{F}; A) \). This condition is necessary for the desired equality, but whether or not it is sufficient is an open question (a positive answer would potentially be much stronger than Theorem 6.2.1). Instead, we use the following criterion for certification in practice:

**Proposition 7.3.2.** Let \( f \in \mathbf{M}_1^{\text{frac}}(\mathbf{N}; \mathbf{F}) \).

a. \( f \in \mathbf{M}_1(\mathbf{N}; \mathbf{F}) \) if and only if \( f^k \in \mathbf{M}_k(\mathbf{N}; \mathbf{F}) \) for all \( k \geq 1 \), and

b. \( f \in \mathbf{S}_1(\mathbf{N}; \mathbf{F}) \) if and only if \( f^k \in \mathbf{S}_k(\mathbf{N}; \mathbf{F}) \) for all \( k \geq 1 \).

**Example 7.3.3.** Continuing Example 7.3.1, we can prove that the form \( f \) is not a modular form simply by showing that \( f^2 \notin \mathbf{S}_2(11, \varepsilon_{11}; \overline{\mathbb{F}}_7) = \text{span}\{g\} \). This is apparent from the fact that \( f^2 \) vanishes to order 2 at the cusps while \( g \) vanishes to order 1.

The above criterion can easily be implemented as an algorithm, but we should be aware of two issues:

- Certification using Proposition 7.3.2 requires that we compute a basis for the auxiliary space \( \mathbf{M}_k(\mathbf{N}, \chi^k; \mathbf{F}) \). However, when \( \chi \) is quadratic, this certification method becomes ideal, since Algorithm 7.2.6 already requires us to compute a basis for \( \mathbf{M}_2(\mathbf{N}, \chi^2; \mathbf{F}) = \mathbf{M}_2(\mathbf{N}, 1; \mathbf{F}) \).

- As in Lemma 7.2.4, the power \( k \) must be chosen to be small enough so that the precision to which elements of \( V^{(\infty)}_\ell \) have been computed is high enough to guarantee that congruence modulo \( q^p \) implies equality.
Remark 7.3.4. In some cases we can choose the set of auxiliary forms $A$ such that $Z(A)$ contains no cusps (see Remark 7.2.8). Choosing such an $A$ and replacing $M_2(N, 1; F)$ with $S_2(N, 1; F)$ in the construction of the initial space $V_1^{(0)}(N; F; A)$ we can apply essentially the same procedure as Algorithm 7.2.6 to obtain a space $V_1^{(\infty)}(N; F; A)$ of fractional forms that contains $S_1(N, \chi; F)$ and that may provably be equal to it via either the Hecke stability theorem or the certification method above. In the context of the next section, such a computation is often enough (because of Proposition 8.1.3).

8 Ethereal forms and the extended HSM

In this section we explain the phenomenon of ethereality and develop the extended HSM, a procedure that extends Algorithm 7.2.6 by taking ethereality into account.

8.1 Ethereality

Returning to the theory of Section 1.1, have an exact sequence of sheaves

$$0 \to \omega_k^{[1/\mathbb{N}]} \to \omega_k^{\mathbb{Z}[1/N]} \to \omega_p^k \to 0.$$ 

Taking cohomology yields an exact sequence

$$0 \to M_k(N; \mathbb{Z}[1/N]) \to M_k(N; \mathbb{F}_p) \to H^1(X_1(N), \omega^k)[p] \to 0.$$ 

The surjectivity of the reduction map $M_k(N; \mathbb{Z}[1/N]) \to M_k(N; \mathbb{F}_p)$ is therefore controlled by the group $H^1(X_1(N), \omega^k)[p]$.

Theorem 8.1.1. Let $N \geq 5$.

a. If $k \geq 2$, then $H^1(X_1(N), \omega^k)$ is trivial, so the reduction map $M_1(N; \mathbb{Z}[1/N]) \to M_1(N; \mathbb{F}_p)$ is surjective for all $p$.

b. The group $H^1(X_1(N), \omega)$ is finitely generated. In particular, $M_1(N; \mathbb{Z}[1/N]) \to M_1(N; \mathbb{F}_p)$ is surjective for all but finitely many primes $p$.

Proof. Part (a.) follows from Theorem 1.7.1 in [Kat72]. Both claims can also be found in Section 4 of [Kha07].

Let $\mathcal{E}(N) = \prod_{p \nmid N} H^1(X_1(N), \omega)[p^\infty]$. The primes in the support of the finite group $\mathcal{E}(N)$ are precisely those primes $p \nmid N$ for which the surjectivity of $M_1(N; \mathbb{Z}[1/N]) \to M_1(N; \mathbb{F}_p)$ fails. Understanding the group $\mathcal{E}(N)$ is crucial to the study of weight 1 modular forms on $X_1(N)$ and, via Theorem 2.4.1 and Remark 8.1.4 below, the size of this group is relevant to arithmetic statistics (in the sense of [VE10]).
Definition 8.1.2. A Hecke eigenform \( f \in M_1(N; \overline{F}_p) \) is an ethereal form if it is not contained in
\[
\text{im}(M_1(N; \mathbb{Z}[\frac{1}{N}]) \to M_1(N; \overline{F}_p)) \otimes \overline{F}_p.
\]
The ethereal subspace is the subspace of \( M_1(N; \overline{F}_p) \) spanned by the ethereal forms.

The group \( \mathcal{E}(N)[p] \) and the cokernel of reduction \( M_1(N; \mathbb{Z}[\frac{1}{N}]) \to M_1(N; \overline{F}_p) \) are isomorphic as \( \mathbb{F}_p \)-vector spaces. Because the image of reduction is Hecke stable, \( \mathcal{E}(N)[p] \) is nontrivial if and only if there exists an ethereal form \( f \in M_1(N; \overline{F}_p) \). \( p \) is called an ethereal characteristic if it divides the order of \( \mathcal{E}(N) \).

Proposition 8.1.3. Ethereal forms are cusp forms.

Proof. Let \( f \in M_1(N; \overline{F}_p) \) be a Hecke eigenform, and assume (without loss) that \( f \) is a newform. Let \( \rho_f \) be the representation associated to \( f \) by Theorem 2.4.1. If \( \rho_f \) is reducible, then \( \rho_f = \theta_1 \oplus \theta_2 \) where \( \theta_1, \theta_2 : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{F}_p^\times \), so \( a_\ell(f) = \theta_1(\ell) + \theta_2(\ell) \). Since characters lift to characteristic zero (as in the proof of Proposition 1.6.5), \( f \) is not ethereal.

We conclude that if \( f \) is ethereal then \( \rho_f \) must be irreducible. By Theorem 2.4.1, \( f \) is a cusp form. \( \Box \)

Remark 8.1.4. One way to distinguish between ethereal and nonethereal newforms \( f \in M_1(N; \overline{F}_p) \) is that the representations associated to the latter lift to continuous Artin representations \( \rho : \text{Gal}(\overline{Q}/Q) \to \text{GL}_2(C) \) (by Theorem 2.4.4, see also [Kha07] Section 1). Because the topology on \( \text{Gal}(\overline{Q}/Q) \) is profinite, the image of \( \rho \) is a finite subgroup of \( \text{GL}_2(C) \). A well-known result of Dickson (see [Dic01] Section 260) classifies all finite subgroups of \( \text{PGL}_2(C) \) up to conjugacy. One consequence of this classification is that the only finite subgroup of \( \text{PGL}_2(C) \) is the icosahedral group \( A_5 \) (see [Buh78]).

In contrast, when \( f \) is ethereal, the data in Appendix A seems to indicate that the image of \( \bar{\rho}_f : \text{Gal}(\overline{Q}/Q) \to \text{PGL}_2(\overline{F}_p) \) is typically “as large as possible,” constrained only by the condition \( \det \rho_f = \chi \). Ethereal forms in characteristic \( p \) are therefore related to the existence of \( \text{PGL}_2(\overline{F}_p) \)-extensions of \( Q \) that are unramified at \( p \), and the group \( \text{PGL}_2(\overline{F}_p) \) is nonsolvable for \( p \geq 5 \).

Example 8.1.5. The first example of an ethereal form was given by Mestre in a letter to Serre in 1987 (see [Edi06] Appendix A). In that letter, Mestre described a newform \( f \in S_1(1429; \overline{F}_2) \) such that the image of \( \rho_f : \text{Gal}(\overline{Q}/Q) \to \text{GL}_2(\overline{F}_2) \) is \( \text{SL}_2(\overline{F}_8) \). Thus \( \rho_f \) does not lift to a representation \( \bar{\rho}_f : \text{Gal}(\overline{Q}/Q) \to \text{GL}_2(C) \) (by Dickson’s classification), so \( f \) does not lift to a modular form \( \tilde{f} \in M_1(1429; C) \) of weight 1 (by the Deligne–Serre theorem).

Example 8.1.6. The first examples of ethereal forms over fields of odd characteristic were given by Buzzard (see [Kha07] Section 4.1). Roughly speaking, Buzzard’s method for detecting ethereal forms involves computing auxiliary spaces that contain copies of \( S_1(N, \chi; F) \) and then computing their intersection. One must then certify the results
as in Section 7.3. This same sort of idea, which Buzzard attributes to Buhler [Buh78], is the basis for the initial step of the Hecke stability method.

Buzzard has used this method to prove the existence of an ethereal form \( f \in S_1(82; \overline{\mathbb{F}}_{199}) \). In [Buz12], he shows that the associated projective representation has image isomorphic to \( \text{PGL}_2(\mathbb{F}_{199}) \), from which he concludes that there is a \( \text{PGL}_2(\mathbb{F}_{199}) \)-extension \( K/\mathbb{Q} \) that is unramified outside \( \{2,41\} \).

**Example 8.1.7.** Because \( S_5 \simeq \text{PGL}_2(\mathbb{F}_5) \) and because \( S_5 \) is not a subgroup of \( \text{PGL}_2(\mathbb{C}) \), every imaginary \( S_5 \)-extension of \( \mathbb{Q} \) unramified at 5 arises from an ethereal newform over \( \overline{\mathbb{F}}_5 \) (by Theorem 2.4.2).

For example, the HSM computes newforms

\[
 f_1, f_2 \in S_1(203, \varepsilon_7; \overline{\mathbb{F}}_{25})
\]

that are exchanged by the Frobenius map on \( \mathbb{F}_{25} \). For example,

\[
 f_1(q) = q + 3q^2 + \alpha q^3 + 3q^4 + 3\alpha q^5 + 3\alpha q^6 + (\alpha + 2)q^7 + q^8 + 4q^9 + 4\alpha q^{10} + \cdots
\]

where \( \alpha^2 = 3 \). The representations \( \rho_{f_1} \) and \( \rho_{f_2} \) are isomorphic, and their projective images are both isomorphic to \( \text{PGL}_2(\mathbb{F}_5) \).

One can check by comparing the data \( \{(a_\ell(f_1), \chi(\ell))\}_{\ell \mid 203} \) and tables of number fields [Jones] that the fixed field of \( \ker \tilde{\rho}_{f_1} \) is isomorphic to the splitting field \( K \) of \( X^5 - 29X^2 + 58X - 29 \). The extension \( K/\mathbb{Q} \) has Galois group \( S_5 \) and it is unramified outside of \( \{7,29\} \), as predicted by Theorem 2.4.3.

**Remark 8.1.8.** Note that if \( f \in S_1(N; \overline{\mathbb{F}}_p) \) is an ethereal form, there may exist a multiple \( N_1 \) of \( N \) such that \( \delta^* f \in S_1(N_1; \overline{\mathbb{F}}_p) \) lifts to an element \( \hat{f} \in S_1(N; \mathbb{C}) \). Buzzard exhibits an example of such a form at level 52 in [Buz12]. This can only occur if the projective image of \( \rho_f \) falls under Dickson’s classification.

### 8.2 Detection of Ethereal Characteristics

Let \( N \geq 5 \). Since \( \mathcal{E}(N) \) inherits the action of the diamond operators, we have a decomposition

\[
 \mathcal{E}(N) = \bigoplus_{\chi: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times} \mathcal{E}(N, \chi),
\]

where \( \mathcal{E}(N, \chi) \) is the \( \chi \)-eigenspace of \( \mathcal{E}(N) \). \( \mathcal{E}(N, \chi) \) can be interpreted as the subgroup of \( \mathcal{E}(N) \) contributed by the existence of ethereal forms \( f \in M_1(N, \chi; \mathbb{F}_p) \) for some \( p \subset \mathcal{O}_{\mathbb{F}(\chi)} \) not dividing \( N \).

Fix an odd character \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times \) and let \( K = \mathbb{Q}(\chi) \). An **ethereal characteristic** for the pair \( (N, \chi) \) is a prime \( p \) such that there is a prime ideal \( p \subset \mathcal{O}_K \) over \( p \) for which there exists an ethereal form \( f \in M_1(N, \chi; \mathbb{F}_p) \). The ethereal characteristics for \( (N, \chi) \) are exactly those primes \( p \) dividing the order of the group \( \mathcal{E}(N, \chi) \).
To account for ethereal forms, we would like an algorithm that computes not only a basis for $M_1(N, \chi; \mathbb{C})$, but also the set of ethereal characteristics for $(N, \chi)$. One of the advantages of Algorithm 7.2.6 is that with only a few minor changes it can be modified to compute a close approximation of this set in the process of computing a basis for $M_1(N, \chi; \mathbb{C})$.

**Remark 8.2.1.** A brief word of caution: Even though every character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{F}_p^\times$ lifts to characteristic zero (as in the proof of Proposition 1.6.5), it may have multiple such lifts if $p$ divides the order of $(\mathbb{Z}/N\mathbb{Z})^\times$.

Hence, to check that some form $f \in M_1(N, \chi; \mathbb{F}_p)$ is actually ethereal when $p \mid \phi(N)$, we must verify that it is not an element of

$$\text{im}(M_1(N, \theta\chi; K) \to M_1(N, \chi; \mathbb{F}_p)) \otimes \mathbb{F}_p$$

for each even character $\theta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ with trivial reduction modulo $p$.

When $k \geq 2$, any element of $S_k(N, \chi; \mathbb{F}_p)$ lifts to a cusp form of character $\chi$ except possibly when $\text{char} \mathbb{F}_p = 2, 3$ (see [Kha07] Proposition 4.2), but this restriction on characteristics also does not hold when $k = 1$. For example, there is $f \in S_1(129, \overline{\chi}; \mathbb{F}_7)$ that does not lift to an element of $S_1(129, \varepsilon_3; \mathbb{Z})$ but which does lift to an element of $S_1(129, \varepsilon_3; \mathbb{Z}[[\mu_7]])$ where $\theta$ is a character of order 7 and conductor 43.

Choose a finite nonempty $A \subset M_1(N, \chi^{-1}; \mathbb{C}) \setminus \{0\}$ so that for all $\lambda$, $\lambda(q)$ has coefficients in the algebraic integers, and there exists $n$ so that $a_n(\lambda) = 1$. As before, let $\mathcal{O}_A$ be the ring obtained by adjoining to $\mathbb{Z}[\frac{1}{\chi}]$ the coefficients of the Laurent series $\{1/\lambda(q)\}_{\lambda \in A}$. Note that for every prime $p \subset \mathcal{O}_A$, the reduction $\widetilde{A}$ of $A$ modulo $p$ satisfies $\widetilde{A} \subset M_1(N, \overline{\chi}; \mathbb{F}_p) \setminus \{0\}$ where $\overline{\chi}$ is the reduction of $\chi$ modulo $p$.

If $M$ is a matrix with entries in $\mathcal{O}_A$, we say that a prime $p \subset \mathcal{O}_A$ is a **divisor** of $M$ if $\dim_K \ker M < \dim_{\mathbb{F}_p} \ker \widetilde{M}$, where $\widetilde{M}$ is the reduction of $M$ modulo $p$. Similarly, if $B \subset M_1^{\text{frac}}(N, \chi; \mathcal{O}_A)$ is linearly independent, we say that $p$ is a divisor of $B$ if the reduction $\overline{B}$ modulo $p$ is not linearly independent.

**Remark 8.2.2.** If $M$ is a matrix with coefficients in $\mathcal{O}_A$, then one can compute the divisors of $M$ as follows: Let $r = \text{rank}(M)$. Compute a set of $r \times r$ minors $M'_1, \ldots, M'_s$ of $M$ such that $\text{rank}(M'_i) = r$ for all $i$. The divisors of $M$ must be among the prime ideals dividing the **ideal** $\gcd, \det M'_i$ (see also Remark 8.2.3).

The same sort of argument applies to computing the divisors of $B \subset M_1^{\text{frac}}(N, \chi; \mathcal{O}_A)$: We simply construct a matrix whose entries are the coefficients in the $q$-expansions of the elements of $B$. We must of course work at an appropriate level of precision (compare with Lemma 7.2.4) to be sure of our computation.

**Remark 8.2.3.** Computing the determinant of an $r \times r$ matrix with entries in $K = \mathbb{Q}(\chi)$ directly is rather slow if the degree of $K$ (eq. the order of $\chi$) is large. It is often quicker in practice to employ the following strategy: Let $M \in K^{r \times r}$ and let $\{\sigma_1, \ldots, \sigma_n\}$ be an enumeration of $\text{Gal}(K/\mathbb{Q})$. Compute

$$M^* = M^{\sigma_1} \cdots M^{\sigma_n}$$
so that \( \det(M^*) \in \mathbb{Q} \) (the actual matrix \( M^* \) of course depends on the chosen enumeration and typically does not have rational entries). Assume that we can easily compute the smallest (or any) \( d \) such that \( d \det M^* \in \mathbb{Z} \). By reducing \( M^* \) modulo several primes \( p \subset \mathcal{O}_K \) and taking determinants over the finite field \( \mathbb{F}_p \), we can use the Chinese remainder theorem to reconstruct \( d \det M^* \), and therefore a finite list of rational primes \( p \) over which the divisors of \( M \) must lie.

**Algorithm 8.2.4.** The following procedure on input \((N, \chi, A)\) outputs a list \( L \) that contains all prime ideals \( p \in \mathcal{O}_A \) such that

\[
\dim_{\mathbb{C}} V_\ell^{(0)}(N; \mathbb{C}; A) < \dim_{\overline{\mathbb{F}}_p} V_\ell^{(0)}(N; \overline{\mathbb{F}}_p; \overline{A}).
\]

1. Let \( L \leftarrow \{ \} \) and \( P \leftarrow \text{Sturm}_2(N) \).
2. Run Algorithm 7.2.2 on input \((N, \mathcal{C}, \chi, A, P)\), and on each iteration of Step 5 of that algorithm, append the divisors of the matrix \( M \) and the basis \( B \) to \( L \).
3. Return \( L \).

**Proof.** Suppose that \( p \subset \mathcal{O}_A \) satisfies the inequality in the claim and let \( L \) be the output of this algorithm. We must show that \( p \in L \).

Enumerate \( A = \{ \lambda_1, \ldots, \lambda_n \} \). We may assume the equality \( \dim_{\mathbb{C}} M_2(N, 1; \mathbb{C}) = \dim_{\overline{\mathbb{F}}_p} M_2(N, 1; \overline{\mathbb{F}}_p) \): otherwise \( p \) is a divisor of the initial basis (because of the way \( A \) was chosen), so it is appended to \( L \) in the first iteration of Step 2. Thus, there exists \( t \in [0, n) \) satisfying

\[
\dim_{\mathbb{C}} \bigcap_{i=1}^{t} \lambda_i^{-1} M_2(N, 1; \mathbb{C}) = \dim_{\overline{\mathbb{F}}_p} \bigcap_{i=1}^{t} \lambda_i^{-1} M_2(N, 1; \overline{\mathbb{F}}_p), \quad \text{but}
\]

\[
\dim_{\mathbb{C}} \bigcap_{i=1}^{t+1} \lambda_i^{-1} M_2(N, 1; \mathbb{C}) < \dim_{\overline{\mathbb{F}}_p} \bigcap_{i=1}^{t+1} \lambda_i^{-1} M_2(N, 1; \overline{\mathbb{F}}_p).
\]

The above conditions imply that \( p \) must be a divisor of the matrix \( M \) whose kernel is used to compute a basis for the the intersection

\[
\lambda_{i+1}^{-1} M_2(N, 1; \mathbb{C}) \cap \bigcap_{i=1}^{t} \lambda_i^{-1} M_2(N, 1; \mathbb{C})
\]

in iteration \( t \) of Step 5 in Algorithm 7.2.2 (for more detail, see the analogous argument in the proof of the next algorithm).

**Example 8.2.5.** Note that the prime ideals in the output of Algorithm 8.2.4 do not necessarily lie over ethereal characteristics: \( L \) may include primes \( p \) such that \(|Z(\overline{A})| < |Z(A)|\); these are the characteristics modulo which zeros of elements in \( A \) collide.
For example, at level $7 \cdot 53$, there are two oldforms that correspond to the primitive weight 1 Eisenstein series with character $\varepsilon_7$: The form $\lambda_1$ with $q$-expansion

$$\lambda_1(q) = 1 + 2 \sum_{n=1}^{\infty} \sum_{m|n} \varepsilon_7(m)q^n$$

and the form $\lambda_2$ whose $q$-expansion is $\lambda_1(q^{53})$ (this is the pullback of $\lambda_{\varepsilon_7}$ by the primitive degeneracy of the second kind, see Section 1.1).

Suppose that $[E,P] \in Z(\lambda_1) \cap Z(\lambda_2)$ for some $[E,P] \in X_1(N)_F$ where $F = \bar{\mathbb{F}}_p$ (these forms have no common zeros in characteristic zero). By Example 3.3.1, $\lambda_1([E,P]) = 0$ if and only if $j(E) = 0$ and that $53P$ is killed by one of the endomorphisms $\{2 + \sqrt{-3}, 2 - \sqrt{-3}\}$ (of norm 7) on $E$. On the other hand, $\lambda_2([E,P]) = 0$ if and only if $\lambda_1([E/(7P), P + (7P)]) = 0$, so in particular, the existence of a common zero implies that the curve $E_0/F$ has an endomorphism of norm 53 (where $E_0$ is an elliptic curve with $j$-invariant 0). Because 53 is inert in $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-3}) \hookrightarrow \text{End}(E_0) \otimes_\mathbb{Z} \mathbb{Q}$, it follows that

- $E_0/F$ is supersingular, so $p \equiv 0, 2 \pmod{3}$, and
- $p \leq 212$ (by Lemma 4.3.3).

Now, Algorithm 8.2.4 in this situation with $A = \{\lambda_1, \lambda_2\}$ outputs

$$L = \{3, 5, 13, 17, 47, 53, 131\}.$$

Using Algorithm 7.2.6, we can verify that 13 and 17 are the only etheeral characteristics for $(371, \varepsilon_7)$ in $L$. Thus, the zero sets of $\lambda_1$ and $\lambda_2$ must collide modulo 3, 5, 47, 53, and 131.

**Example 8.2.6.** The tables in Appendix A show that there are no etheeral forms of level $253 = 11 \cdot 23$ and character $\varepsilon_{11}$. There are also no weight 1 cusp forms of this type over $\mathbb{C}$.

Let $\lambda_1 = \varepsilon_{11}$ and let $\lambda_2 = \varepsilon_{253,11}^{23} \lambda_1$ so that $\lambda_1(q) = 1 + 2 \sum_{n \geq 1} \sum_{m|n} \varepsilon_{11}(m)q^n$ and $\lambda_2(q) = \lambda_1(q^{23})$. Both $\lambda_1$ and $\lambda_2$ are nonzero at the cusps of $X_1(253)_\mathbb{C}$. We have

$$\dim_{\mathbb{C}}(\lambda_1^{-1}S_2(253, 1; \mathbb{C}) \cap \lambda_2^{-1}S_2(253, 1; \mathbb{C})) = 2,$$

even though

$$\dim_{\mathbb{C}} S_1(253, \varepsilon_{11}; \mathbb{C}) = 0.$$

It follows $Z(\lambda_1) \cap Z(\lambda_2)$ on $X_1(253)_\mathbb{C}$ must be nontrivial.

Note that $\lambda_1([E,P]) = 0$ implies $\text{End}(E) \simeq \mathbb{Z}[1+\sqrt{-11}]/2$ (see Example 3.3.4), and the prime 23 splits in $\mathbb{Q}(\sqrt{-11})/\mathbb{Q}$, so we cannot restrict collisions of the zero sets as in the previous example.

**Algorithm 8.2.7.** Assume the notation above with $P = \text{Sturm}_{e+3}(N)$. The following procedure on input $(N, \chi, A, \ell)$ returns $(B, L)$ where $B \subset M_1^{\text{frac}}(N, \chi; \mathcal{O}_A)$ is a basis for the image of $M_1(N, \chi; \mathbb{C})$ under $q$-expansion $M_1^{\text{frac}}(N, \chi; \mathcal{O}_A) \to \mathcal{O}_A[[q]]/(q^P)$ and where $L$ is a (finite) list that contains every prime $p \subset \mathcal{O}_A$ such that $p \nmid N$ and for which $M_1(N, \chi; \mathcal{O}_A) \to M_1(N, \chi; \mathbb{F}_p)$ is not surjective.

52
1. Initialize \( L \) as the set of all \( p \subset \mathcal{O}_K \) that do not divide \( N \) and that are invertible in the overring \( \mathcal{O}_A \).

2. Run Algorithm 8.2.4 on input \( (N, \chi, A) \) and append the output to \( L \).

3. Run Algorithm 7.2.6 on input \( (N, C, \chi, A, \ell, P) \) with the following modifications:

   (a) For each \( t \), save the basis \( B_1^{(t)} \) and the matrix \( M^{(t)} \) as constructed by Algorithm 7.2.6.

   (b) For each \( t \), append to \( L \) the divisors \( p \) of \( B_1^{(t)} \).

   (c) For each \( t \), append to \( L \) the divisors \( p \) of \( M^{(t)} \).

4. Return \((B, L)\), where \( B \) is the output of Algorithm 7.2.6 on input \((N, C, \chi, A, \ell, P)\).

**Proof.** The algorithm produces a basis for \( M_1(N, \chi; C) \) by Theorem 7.1.1.

We may assume that \( p \subset \mathcal{O}_A \) is ethereal and that \( p \) was not added to \( L \) in Step 2 or Step 3b. In particular, \( \dim_C V_\ell^{(0)}(N; C; A) = \dim_{\mathbb{F}_p} V_\ell^{(0)}(N; \mathbb{F}_p; \tilde{A}) \).

Let \( B_1^{(i)} \) be the basis for \( V_\ell^{(i)}(N; C; A) \) constructed in the implementation of the algorithm and recall that \( B_1^{(i)} \subset M_1^{\text{frac}}(N, \chi; \mathcal{O}_A) \) for all \( i \). Let \( \tilde{B}_1^{(i)} \) denote the reduction of this basis modulo \( p \). By the Hecke stability theorem, we may fix \( n \geq 1 \) such that \( B_1^{(n)} \) is a basis for \( M_1(N, \chi; C) \). Each \( \tilde{B}_1^{(i)} \) is linearly independent (by our assumption that \( p \) is not added to \( L \) in Step 3b). In particular, for all \( i \in [0, n] \), the span of \( \tilde{B}_1^{(i)} \) is a \( \dim_C V_\ell^{(i)}(N; C; A) \)-dimensional subspace of \( V_\ell^{(i)}(N; \mathbb{F}_p; \tilde{A}) \).

Since \( p \) is ethereal, \( \tilde{B}_1^{(n)} \) does not generate \( M_1(N, \chi; \mathbb{F}_p) \), so

\[
\dim_C V_\ell^{(n)}(N; C; A) = \dim_C M_1(N, \chi; C) < \dim_{\mathbb{F}_p} M_1(N, \chi; \mathbb{F}_p) \leq \dim_{\mathbb{F}_p} V_\ell^{(n)}(N; \mathbb{F}_p; \tilde{A}).
\]

Because we also have \( \dim_C V_\ell^{(0)}(N; C; A) = \dim_{\mathbb{F}_p} V_\ell^{(0)}(N; \mathbb{F}_p; \tilde{A}) \), there is a least \( t \in [0, n] \) satisfying

\[
\dim_C V_\ell^{(t)}(N; C; A) = \dim_{\mathbb{F}_p} V_\ell^{(t)}(N; \mathbb{F}_p; \tilde{A}), \text{ and}
\dim_C V_\ell^{(t+1)}(N; C; A) < \dim_{\mathbb{F}_p} V_\ell^{(t+1)}(N; \mathbb{F}_p; \tilde{A}).
\]

Now, let \( M^{(t)} \) be the matrix over \( \mathcal{O}_A \) constructed in Algorithm 7.2.6 whose entries are the coefficients of the \( q \)-expansions from \( B_1^{(t)} \cup T_\ell B_1^{(t)} \). Note that \( M^{(t)} \) has entries in \( \mathcal{O}_A \). By Lemma 7.2.5,

\[
\dim_K \ker M^{(t)} = \dim_C V_\ell^{(t+1)}(N; C; A).
\]

The Hecke action on \( q \)-expansions and the reduction of \( q \)-expansions commute (by mere inspection of the formula in Proposition 2.3.1), so since \( \tilde{B}_1^{(t)} \) is linearly independent, Lemma 7.2.5 applies also to the reduction \( \tilde{M}^{(t)} \) of \( M^{(t)} \) modulo \( p \), from which we obtain

\[
\dim_{\mathbb{F}_p} \ker \tilde{M}^{(t)} = \dim V_\ell^{(t+1)}(N; \mathbb{F}_p; \tilde{A}).
\]
We conclude that
\[ \dim_K \ker M(t) < \dim_{\mathbb{F}_p} \ker \tilde{M}(t), \]
hence \( p \) is a divisor of \( M(t) \), so it is appended to \( L \) in Step 3c.

### 8.3 Lower bounds on the group \( \mathcal{E}(N, \chi) \)

The extended Hecke stability method is the following procedure: We run Algorithm 8.2.7, and thereby obtain a basis for \( M_1(N, \chi; K) \) and a list \( L \) of primes ideals of \( \mathcal{O}_A \) such that \( \{ p \cap \mathbb{Z} : p \in L \} \) includes the ethereal characteristics for \( (N, \chi) \). For each \( p \in L \), we compute a basis for \( V^{(\infty)}_\ell(N, \chi; \mathbb{F}_p) \) using Algorithm 7.2.6. Being mindful of the situation that can arise when \( p \mid \phi(N) \) (see Remark 8.2.1), and using Proposition 7.3.2 where necessary, this allows us to produce factors of the abelian group \( \mathcal{E}(N, \chi) \).

**Figure.** The extended Hecke stability method.

**Example 8.3.1.** Let us compute the contribution to \( \mathcal{E}(651) \) (away from 2) by the quadratic characters of level \( N \). There are four such characters:

- Let \( \chi = \varepsilon_3 \). An argument similar to that in Example 6.1.1 shows that
  \[ M_1(651, \varepsilon_3; F) = \{ f \in \lambda_{\varepsilon_3}^{-1}M_2(651, 1; F) : T_2f \in \lambda_{\varepsilon_3}^{-1}M_2(651, 1; F) \} \]
  for \( F = \mathbb{Q} \) and all \( F = \mathbb{F}_p \) with \( p \nmid N \). The characteristic zero space is 2-dimensional and it is generated by the Eisenstein series.
Algorithm 8.2.7 with \( A = \{\lambda_{\varepsilon_3}\} \) outputs \( \{5, 245100439\} \), and one checks using the above equation or Algorithm 7.2.6 that 245100439 is an ethereal characteristic for \((651, \varepsilon_3)\) with

\[
\dim_{\mathbb{F}_{245100439}} M_1(651, \varepsilon_3; \mathbb{F}_{245100439}) - \dim_{\mathbb{Q}} M_1(651, \varepsilon_3; \mathbb{Q}) = 2.
\]

The prime 5 is not ethereal for level 651 for the reasons explained in Remark 8.2.1.

- The case \( \chi = \varepsilon_7 \) is similar. In this case we obtain one ethereal characteristic, namely 7759, and

\[
\dim_{\mathbb{F}_{7759}} M_1(651, \varepsilon_7; \mathbb{F}_{7759}) - \dim_{\mathbb{Q}} M_1(651, \varepsilon_7; \mathbb{Q}) = 2.
\]

- Let \( \chi = \varepsilon_{31} \). In this case, Algorithm 8.2.7 returns the list \( L = \{337\} \). Using Algorithm 7.2.6 over \( F = \overline{\mathbb{F}}_{337} \), we see that the space \( V_2^{(1)}(651; \overline{\mathbb{F}}_{337}; \{\lambda_{\varepsilon_{31}}\}) \) is 2-dimensional, and that it is \( T_2 \)-stable. We would like

\[
V_2^{(1)}(651; \overline{\mathbb{F}}_{337}; \{\lambda_{\varepsilon_{31}}\}) = M_1(651, \tilde{\varepsilon}_{31}; \mathbb{F}_{651}).
\]

We have given several ways to prove this equality:

1. Applying Theorem 7.1.1 directly: Using the algorithm of Section 3.3, we find that \( jZ(\lambda_{\varepsilon_{31}}) \) coincides with the root set of the polynomial

\[
3^{32}t^3 + 394086965048982896640t^2 + 23574729187315780314726400t.
\]

Modulo 337 this factors as \( 2t(t - 96)(t - 241) \). The \( j \)-invariants 0, 96, and 241 are not supersingular modulo 337, so \( Z(\lambda_{\varepsilon_{31}}) \cap X_1(651)_{\mathbb{F}_{337}}^{ss} \) is empty.

2. Applying Corollary 7.1.3 with \( n = 2 \): The desired holds because we have \( \frac{1}{12}[\text{SL}_2(\mathbb{Z}) : \Gamma_0(23)] = 2 < 3 \) and \( 337 > \max\{\frac{1024}{337}, 64\} = 64 \).

3. Using Proposition 7.3.2: Let \( \{f_1, f_2\} \) denotes a basis for \( V_2^{(1)}(651; \overline{\mathbb{F}}_{337}; \{\lambda_{\varepsilon_{31}}\}) \). Checking against the basis for \( M_2(651, 1; \mathbb{Z}[\frac{1}{651}]) \) we computed as part of Algorithm 7.2.2, we have \( f_1^2, f_2^2 \in M_2(651, 1; \overline{\mathbb{F}}_{337}) \).

We have \( \dim_{\mathbb{F}_{337}} M_1(651, \tilde{\varepsilon}_{31}; \overline{\mathbb{F}}_{337}) - \dim_{\mathbb{Q}} M_1(651, \varepsilon_{31}; \mathbb{Q}) = 2 \).

- Let \( \chi = \varepsilon_{651} \). Taking \( A \) as in Remark 7.2.8 and applying \( T_2 \)-stability, we find that there are no ethereal characteristics for \((651, \varepsilon_{651})\), though \( \dim M_1(651, \varepsilon_{651}; \mathbb{C}) = 5 \).

The above shows that

\[
(\mathbb{Z}/337\mathbb{Z})^2 \oplus (\mathbb{Z}/7759\mathbb{Z})^2 \oplus (\mathbb{Z}/245100439\mathbb{Z})^2 \hookrightarrow \mathcal{E}(651)
\]

which is a perfectly respectable lower bound on this group.
Example 8.3.2. Above, we have explained how to approximate the set of primes $p$ that divide the group $E(N)$. However, this group may admit cyclic subgroups of order $p^n$ for $n \geq 2$. It is understandably more difficult to detect such elements because linear algebra over $\mathbb{Z}/p^n\mathbb{Z}$ can be rather tricky.

The theory of isogeny graphs laid down in Chapter II was developed only over an algebraically closed field, but because $\overline{\mathbb{F}}_p \hookrightarrow \mathbb{Z}/p^n\mathbb{Z}$ (with this latter ring as defined in [CKW11]), one can argue that a Hecke stability statement such as

$$M_1(N, \chi; \mathbb{F}_p) = \{ f \in \lambda^{-1}M_2(N, 1; \mathbb{F}_p) : T_{\ell}f \in \lambda^{-1}M_2(N, 1; \mathbb{F}_p) \}$$

should imply

$$M_1(N, \chi; \mathbb{Z}/p^n\mathbb{Z}) = \{ f \in \lambda^{-1}M_2(N, 1; \mathbb{Z}/p^n\mathbb{Z}) : T_{\ell}f \in \lambda^{-1}M_2(N, 1; \mathbb{Z}/p^n\mathbb{Z}) \}.$$  

The first instance of this “higher torsion” phenomenon in the purview of our tables (Appendix A) seems to occur at level 309. Computing the Smith normal form of the relevant Hecke stability matrix (instead of divisors as in Remark 8.2.2) seems to imply the existence of an embedding $(\mathbb{Z}/121\mathbb{Z})^2 \hookrightarrow E(309, \varepsilon_3)$.

It is an open question (posed to the author by F. Calegari) whether or not the projective Galois representations $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{PGL}_2(\mathbb{Z}/p^n\mathbb{Z})$ induced by ethereal mod $p^n$ modular forms (via Carayol’s Lemma, see [CKW11]) are unramified at $p$ (i.e., whether or not the conclusion of Theorem 2.4.3 holds in this context).

Remark 8.3.3. The reader may have noticed that the factors of $E(N)$ we have computed above are all square. This is not a coincidence, but rather it is apparently due to the existence of a twisting action on newforms

$$M_1(N, \chi; \mathbb{F}_p) \to M_1(N, \chi^{-1}; \mathbb{F}_p) : f \mapsto f^\chi$$

where $f^\chi$ satisfies $a_\ell(f^\chi) = \chi(\ell)a_\ell(f)$ for all $\ell \nmid N$. This sort of twisting action is well-studied (see [AL78]), but in our particular case, one must check that $f$ and $f^\chi$ have the same level (perhaps using Theorems 2.4.1 and 2.4.2).

Assuming this twisting action exists as described, we observe that the newforms that are fixed by this action are precisely the dihedral forms (see [Kan11]). It is known that dihedral forms in odd characteristic always lift to characteristic forms of the same level (see [Wie04]), so it follows that there are always evenly many ethereal newforms. In particular, when $\varepsilon$ is quadratic, $\varepsilon = \varepsilon^{-1}$, so $|E(N, \varepsilon)|$ is square.

8.4 Complexity of the extended HSM

It is not our intention to provide a deep analysis of the complexity of the extended Hecke stability method. While many of the operations involved are just linear algebra over the field $\mathbb{Q}(\chi)$, there are a number of other operations that are nontrivial from an algorithmic standpoint.
• The extended HSM requires that we compute the auxiliary space $M_2(N, \chi; F)$ to precision $\ell \Sturm_{\ell+3}(N)$ (with $\ell \nmid N$ as small as possible). It is not entirely clear how complex this operation is, but estimates in seem to indicate that for a fixed prime $\ell$, the upper bound on the theoretical complexity of this computation using modular symbols is around $O(N^{4+\epsilon})$. In his thesis [Bru10], Bruin shows that when $N$ is squarefree, this bound can be improved significantly under the generalized Riemann hypothesis.

• Computing the divisors of matrices and bases in Steps 3b and 3b of Algorithm 8.2.7 requires that we evaluate the determinants of large matrices over $\mathcal{O}_A$, take the GCD of these determinants, and then factor that GCD into primes.

Fast algorithms for computing the determinant of an $r \times r$ matrix (such as Gaussian elimination) take about $O(r^3)$ operations, but over a number field, one must remember that these operations are essentially operations on polynomials. Moreover, the memory requirements for this computation can be quite large. Remark 8.2.3 seems to provide an improvement in practice, presumably because arithmetic operations in finite fields are quicker and require less memory than the same operations in number fields.

The size of the factorization problem is unclear, but at the very least we must factor $|\mathcal{E}(N, \chi)|$. We suspect that this quantity grows rather quickly in $N$ (see Example 8.3.1 above and Appendix A). Since ideally we would like a complete description of the group $\mathcal{E}(N, \chi)$, this factorization step cannot be avoided.

It would therefore seem that the runtime of this algorithm is at worst polynomial in $N$ and $|\mathcal{E}(N, \chi)|$, with the degree of that polynomial depending possibly on the degree of $\mathbb{Q}(\chi)/\mathbb{Q}$. 

References


Appendix A

Tables

Ethereal forms by level

The tables that follows describes spaces of ethereal forms of odd levels $N < 750$ and quadratic character. These tables were computed using the extended Hecke stability method with $\ell = 2$.

In these tables, $N$ denotes the level (a factorization of $N$ is provided for reference), $f$ is the conductor of the quadratic character in question. The field “contrib.” describes the subgroup $E(N, \varepsilon_f)$ of $E(N)$; this is denoted using the standard shorthand notation for finite abelian groups.

The field “cert.” describes the certification method used to verify that the $T_2$-stable space consists of modular forms:

- An empty entry denotes certification by direct argument as in Example 6.1.1.
- ‘E’ indicates that $Z(A)$ contained no supersingular points, where $A$ is the standard choice of auxiliary forms (see Remark 7.2.8).
- ‘B’ indicates that the bound of Proposition 7.1.3 was sufficient to prove the desired equality.
- ‘C’ indicates that the basis obtained was certified using the criterion of Proposition 7.3.2.

Unless otherwise mentioned in “notes,” the Galois representations associated to the newforms of the given spaces for $p \geq 7$ are known to have “large” projective image (i.e., the projective image is isomorphic to $\text{PGL}_2(\mathbb{F}_p^n)$ or $\text{PSL}_2(\mathbb{F}_p^n)$ for some $n$). This was verified using the arguments in [Buz12] as well as the criterion in [Ser72]. For forms in characteristics 3 and 5, we are sometimes able to describe the number field $K$ that correspond to the ethereal newforms (by checking against [Jones]); these are given in terms of a quartic or quintic polynomial $f(t)$ whose splitting field is $K$.

It is important to emphasize that these tables list ethereal forms defined over the fields $\mathbb{F}_p$ with $p$ odd, though occasionally we note that there may be “higher torsion,” as in Example 8.3.2; the specific implementation of the extended HSM that generated these tables did not systematically check for this phenomenon.
<table>
<thead>
<tr>
<th>$N$</th>
<th>factn.</th>
<th>$f$</th>
<th>contrib.</th>
<th>cert.</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>133</td>
<td>7 · 19</td>
<td>7</td>
<td>$3^2$</td>
<td></td>
<td>projective image $A_4$ field $t^4 + 3t^2 - 7t + 4$</td>
</tr>
<tr>
<td>141</td>
<td>3 · 47</td>
<td>3</td>
<td>$5^2$</td>
<td></td>
<td>field $t^5 - t^4 - 9t^3 - 17t^2 - 3t + 2$</td>
</tr>
<tr>
<td>159</td>
<td>3 · 53</td>
<td>3</td>
<td>$5^2$</td>
<td></td>
<td>field $t^3 - 2t^2 - 9t^3 - 7t^2 + 12t + 16$</td>
</tr>
<tr>
<td>165</td>
<td>3 · 5 · 11</td>
<td>3</td>
<td>$13^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>195</td>
<td>3 · 5 · 13</td>
<td>3</td>
<td>$23^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>203</td>
<td>7 · 29</td>
<td>7</td>
<td>$5^2$</td>
<td></td>
<td>field $t^5 - 29t^2 + 58t - 29$</td>
</tr>
<tr>
<td>209</td>
<td>11 · 19</td>
<td>11</td>
<td>$3^2$</td>
<td>E</td>
<td>projective image $A_4$ field $t^4 - t^3 - 9t^2 + 6t - 25$</td>
</tr>
<tr>
<td>213</td>
<td>3 · 71</td>
<td>3</td>
<td>$17^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>219</td>
<td>3 · 73</td>
<td>3</td>
<td>$41^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>237</td>
<td>3 · 79</td>
<td>3</td>
<td>$5^2$</td>
<td></td>
<td>projective image $A_5$ field $t^5 - 79t^2 + 474t - 711$</td>
</tr>
<tr>
<td>249</td>
<td>3 · 83</td>
<td>3</td>
<td>$89^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>255</td>
<td>3 · 5 · 17</td>
<td>3</td>
<td>$19^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>267</td>
<td>3 · 89</td>
<td>3</td>
<td>$41^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>273</td>
<td>3 · 7 · 13</td>
<td>7</td>
<td>$23^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>291</td>
<td>3 · 97</td>
<td>3</td>
<td>$73^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>301</td>
<td>7 · 43</td>
<td>43</td>
<td>$3^2$</td>
<td>C</td>
<td>projective image $A_4$ field $t^4 - t^3 - 7t^2 + 9t + 38$</td>
</tr>
<tr>
<td>303</td>
<td>3 · 101</td>
<td>3</td>
<td>$190^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>309</td>
<td>3 · 103</td>
<td>3</td>
<td>$11^2$</td>
<td></td>
<td>the contribution may be $121^2$</td>
</tr>
<tr>
<td>321</td>
<td>3 · 107</td>
<td>3</td>
<td>$73^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>323</td>
<td>17 · 19</td>
<td>19</td>
<td>$13^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>327</td>
<td>3 · 109</td>
<td>3</td>
<td>$281^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>329</td>
<td>7 · 47</td>
<td>7</td>
<td>$3^2$</td>
<td></td>
<td>projective image $S_4$ field $t^4 - t^2 - 3t - 4$</td>
</tr>
<tr>
<td>339</td>
<td>3 · 113</td>
<td>3</td>
<td>$11801^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>341</td>
<td>11 · 31</td>
<td>31</td>
<td>$7^2$</td>
<td>E,C</td>
<td></td>
</tr>
<tr>
<td>345</td>
<td>3 · 5 · 23</td>
<td>3</td>
<td>$829^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>$11^2$</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>357</td>
<td>3 · 7 · 17</td>
<td>3</td>
<td>$19^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>369</td>
<td>3^2 · 41</td>
<td>3</td>
<td>$13^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>371</td>
<td>7 · 53</td>
<td>7</td>
<td>$17^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>381</td>
<td>3 · 127</td>
<td>3</td>
<td>$13^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>385</td>
<td>5 · 7 · 11</td>
<td>7</td>
<td>$89^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>11</td>
<td>$359^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>387</td>
<td>3^2 · 43</td>
<td>3</td>
<td>$17^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>391</td>
<td>17 · 23</td>
<td>23</td>
<td>$7^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>393</td>
<td>3 · 131</td>
<td>3</td>
<td>$7^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$N$</td>
<td>factn.</td>
<td>$f$</td>
<td>contrib.</td>
<td>cert.</td>
<td>notes</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>-----</td>
<td>----------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>407</td>
<td>11 · 37</td>
<td>11</td>
<td>$7^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>411</td>
<td>3 · 137</td>
<td>3</td>
<td>$223^2 · 613^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>413</td>
<td>7 · 59</td>
<td>7</td>
<td>$5297^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>417</td>
<td>3 · 139</td>
<td>3</td>
<td>$37^2 · 227^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>423</td>
<td>3² · 47</td>
<td>3</td>
<td>$5^4 · 13^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>427</td>
<td>7 · 61</td>
<td>7</td>
<td>$12041^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>429</td>
<td>3 · 11 · 13</td>
<td>3</td>
<td>313²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>435</td>
<td>3 · 5 · 29</td>
<td>3</td>
<td>17²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>437</td>
<td>19 · 23</td>
<td>19</td>
<td>83²</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>447</td>
<td>3 · 149</td>
<td>3</td>
<td>$353^2 · 937^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>451</td>
<td>11 · 41</td>
<td>11</td>
<td>17²</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>453</td>
<td>3 · 151</td>
<td>3</td>
<td>2417²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>459</td>
<td>3³ · 17</td>
<td>3</td>
<td>7²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>465</td>
<td>3 · 5 · 31</td>
<td>3</td>
<td>41²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>469</td>
<td>7 · 67</td>
<td>7</td>
<td>181²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>471</td>
<td>3 · 157</td>
<td>3</td>
<td>4523²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>473</td>
<td>11 · 43</td>
<td>11</td>
<td>$23^2 · 101^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>43</td>
<td>$3^4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>477</td>
<td>3² · 53</td>
<td>3</td>
<td>5⁴</td>
<td></td>
<td></td>
</tr>
<tr>
<td>483</td>
<td>3 · 7 · 23</td>
<td>3</td>
<td>$955333^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>6337²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>489</td>
<td>3 · 163</td>
<td>3</td>
<td>$11^2 · 463^2$</td>
<td>$7^2$</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>163</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>495</td>
<td>3² · 5 · 11</td>
<td>3</td>
<td>13¹</td>
<td></td>
<td></td>
</tr>
<tr>
<td>497</td>
<td>7 · 71</td>
<td>7</td>
<td>$23^2 · 89^2$</td>
<td>$3^2$</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>71</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>501</td>
<td>3 · 167</td>
<td>3</td>
<td>$191^2 · 859^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>511</td>
<td>7 · 73</td>
<td>7</td>
<td>1289²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>513</td>
<td>3³ · 19</td>
<td>3</td>
<td>5³</td>
<td></td>
<td></td>
</tr>
<tr>
<td>517</td>
<td>11 · 47</td>
<td>11</td>
<td>$167^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>47</td>
<td>$37^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>519</td>
<td>3 · 173</td>
<td>3</td>
<td>$257^2 · 523^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>527</td>
<td>3 · 5² · 7</td>
<td>31</td>
<td>13²</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>531</td>
<td>3² · 59</td>
<td>3</td>
<td>149²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>537</td>
<td>3 · 179</td>
<td>3</td>
<td>$5^2 · 97^2 · 8713^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>543</td>
<td>3 · 181</td>
<td>3</td>
<td>$67^2 · 193^2$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

projective image $A_4$
field $t^4 - t^3 + 9t + 10$
<table>
<thead>
<tr>
<th>$N$</th>
<th>factn.</th>
<th>$f$</th>
<th>contrib.</th>
<th>cert.</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>549</td>
<td>$3^2 \cdot 61$</td>
<td>3</td>
<td>$5^4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>551</td>
<td>$19 \cdot 29$</td>
<td>19</td>
<td>$43^2$</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>553</td>
<td>$7 \cdot 79$</td>
<td>7</td>
<td>$47^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>559</td>
<td>$13 \cdot 43$</td>
<td>34</td>
<td>$17^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>561</td>
<td>$3 \cdot 11 \cdot 17$</td>
<td>3</td>
<td>$8338651^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>573</td>
<td>$3 \cdot 191$</td>
<td>7</td>
<td>$67^2 \cdot 15731^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>579</td>
<td>$3 \cdot 193$</td>
<td>7</td>
<td>$53^2 \cdot 167^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>583</td>
<td>$11 \cdot 53$</td>
<td>11</td>
<td>$43^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>585</td>
<td>$3^2 \cdot 5 \cdot 13$</td>
<td>3</td>
<td>$23^2 \cdot 53^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>589</td>
<td>$19 \cdot 31$</td>
<td>19</td>
<td>$53^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>591</td>
<td>$3 \cdot 197$</td>
<td>7</td>
<td>$29^2 \cdot 444151^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>595</td>
<td>$5 \cdot 7 \cdot 17$</td>
<td>7</td>
<td>$4447^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>597</td>
<td>$3 \cdot 199$</td>
<td>3</td>
<td>$239^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>603</td>
<td>$3^2 \cdot 67$</td>
<td>3</td>
<td>$11^2 \cdot 557^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>609</td>
<td>$3 \cdot 7 \cdot 29$</td>
<td>3</td>
<td>$112162241^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>611</td>
<td>$13 \cdot 47$</td>
<td>47</td>
<td>$11^2$</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>615</td>
<td>$3 \cdot 5 \cdot 41$</td>
<td>3</td>
<td>$7^2 \cdot 17^2 \cdot 2063^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>623</td>
<td>$7 \cdot 89$</td>
<td>7</td>
<td>$17^2 \cdot 557^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>627</td>
<td>$3 \cdot 11 \cdot 19$</td>
<td>3</td>
<td>$2143^2 \cdot 33161^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>633</td>
<td>$3 \cdot 211$</td>
<td>3</td>
<td>$5^2 \cdot 451933^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>635</td>
<td>$5 \cdot 127$</td>
<td>127</td>
<td>$3^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>637</td>
<td>$7^2 \cdot 13$</td>
<td>7</td>
<td>$41^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>639</td>
<td>$3^2 \cdot 71$</td>
<td>3</td>
<td>$17^2 \cdot 53^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>645</td>
<td>$3 \cdot 5 \cdot 43$</td>
<td>3</td>
<td>$5048773^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>649</td>
<td>$11 \cdot 59$</td>
<td>11</td>
<td>$5^2 \cdot 1483^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>$N$</td>
<td>factn.</td>
<td>$\mathfrak{f}$</td>
<td>contrib.</td>
<td>cert.</td>
<td>notes</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>-------------</td>
<td>----------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>651</td>
<td>$3 \cdot 7 \cdot 31$</td>
<td>3 7 31</td>
<td>$245100439^2$ $7759^2$ $337^2$</td>
<td></td>
<td>E</td>
</tr>
<tr>
<td>657</td>
<td>$3^2 \cdot 73$</td>
<td>3</td>
<td>$41^2 \cdot 71^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>663</td>
<td>$3 \cdot 13 \cdot 17$</td>
<td>3</td>
<td>$61^2 \cdot 457913^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>665</td>
<td>$5 \cdot 7 \cdot 19$</td>
<td>7 35 19 95</td>
<td>$3^4 \cdot 13^2 \cdot 283^2$ $59^2$ $541^2$</td>
<td>C  E  C</td>
<td></td>
</tr>
<tr>
<td>667</td>
<td>$23 \cdot 29$</td>
<td>23</td>
<td>$5^2 \cdot 13^2 \cdot 59^2$</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>669</td>
<td>$3 \cdot 223$</td>
<td>3 223</td>
<td>$11489^2 \cdot 48883^2$</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>671</td>
<td>$11 \cdot 61$</td>
<td>11</td>
<td>$3^2 \cdot 97^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>679</td>
<td>$7 \cdot 97$</td>
<td>7</td>
<td>$83^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>681</td>
<td>$3 \cdot 227$</td>
<td>3 227</td>
<td>$163316303^2$</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>687</td>
<td>$3 \cdot 229$</td>
<td>3</td>
<td>$1140121^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>693</td>
<td>$3^2 \cdot 7 \cdot 11$</td>
<td>3</td>
<td>$5^4$</td>
<td>projective image $A_5$</td>
<td></td>
</tr>
<tr>
<td>695</td>
<td>$5 \cdot 139$</td>
<td>139</td>
<td>$11^2$</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>699</td>
<td>$3 \cdot 233$</td>
<td>3</td>
<td>$41^2 \cdot 89^2 \cdot 223^2 \cdot 1109^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>703</td>
<td>$19 \cdot 37$</td>
<td>19</td>
<td>$47657^2$</td>
<td></td>
<td>B</td>
</tr>
<tr>
<td>705</td>
<td>$3 \cdot 5 \cdot 47$</td>
<td>3 15 47 235</td>
<td>$1433^2 \cdot 74903^2$ $7^4 \cdot 31^4$ $97^2$</td>
<td>E  E  C</td>
<td></td>
</tr>
<tr>
<td>707</td>
<td>$7 \cdot 101$</td>
<td>7</td>
<td>$5^2 \cdot 911683^2$</td>
<td>contribution at $p = 5$ may be $125^2$</td>
<td></td>
</tr>
<tr>
<td>711</td>
<td>$3^2 \cdot 79$</td>
<td>3</td>
<td>$5^4 \cdot 97^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>713</td>
<td>$23 \cdot 31$</td>
<td>23 31</td>
<td>$97^2$</td>
<td></td>
<td>C  C</td>
</tr>
<tr>
<td>715</td>
<td>$5 \cdot 11 \cdot 13$</td>
<td>11</td>
<td>$59^2$</td>
<td></td>
<td>E</td>
</tr>
<tr>
<td>717</td>
<td>$3 \cdot 239$</td>
<td>3</td>
<td>$619^2 \cdot 26921^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>721</td>
<td>$7 \cdot 103$</td>
<td>7</td>
<td>$5^9 \cdot 16871^2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>731</td>
<td>$17 \cdot 43$</td>
<td>43</td>
<td>$47^2$</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>735</td>
<td>$3 \cdot 5 \cdot 7^2$</td>
<td>7</td>
<td>$11^2$</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>737</td>
<td>$11 \cdot 67$</td>
<td>11 67</td>
<td>$7^2 \cdot 47629^2$ $307$</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>741</td>
<td>$3 \cdot 13 \cdot 19$</td>
<td>3 19</td>
<td>$211^2 \cdot 233^2 \cdot 18149^2$ $5^2 \cdot 1877^2$</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>747</td>
<td>$3^2 \cdot 83$</td>
<td>3</td>
<td>$13^2 \cdot 41^2 \cdot 89^4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>749</td>
<td>$7 \cdot 107$</td>
<td>7</td>
<td>$59^2 \cdot 293^2 \cdot 863^2$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

67
Ethereal forms by characteristic

The tables below sort the ethereal forms from the tables above by characteristic rather than by level. For each prime $p$, we list those $(N, f)$ such that there exists an ethereal form $f \in M_1(N, \varepsilon; \mathbb{F}_p)$. For brevity, we restrict our attention to $p < 100$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$(N, f)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>(133, 7), (209, 11), (301, 43), (329, 7), (473, 43), (497, 71), (635, 127), (665, 7), (671, 11)</td>
</tr>
<tr>
<td>5</td>
<td>(141, 3), (159, 3), (203, 7), (237, 3), (423, 3), (477, 3), (513, 3), (537, 3), (549, 3), (609, 7), (633, 3), (649, 11), (667, 23), (669, 223), (693, 3), (707, 7), (711, 3), (721, 7), (741, 19)</td>
</tr>
<tr>
<td>7</td>
<td>(341, 31), (391, 23), (393, 3), (407, 11), (459, 3), (489, 163), (561, 187), (615, 3), (615, 123), (705, 15), (705, 235), (737, 11)</td>
</tr>
<tr>
<td>11</td>
<td>(309, 3), (345, 15), (489, 3), (611, 47), (665, 95), (681, 227), (695, 139), (735, 7)</td>
</tr>
<tr>
<td>13</td>
<td>(165, 3), (323, 19), (369, 3), (381, 3), (423, 3), (495, 3), (527, 31), (645, 43), (665, 7), (667, 23), (747, 3)</td>
</tr>
<tr>
<td>17</td>
<td>(213, 3), (371, 7), (387, 3), (435, 3), (451, 11), (559, 43), (587, 31), (615, 3), (639, 3)</td>
</tr>
<tr>
<td>19</td>
<td>(255, 3), (357, 3), (597, 3)</td>
</tr>
<tr>
<td>23</td>
<td>(273, 7), (473, 11), (497, 7), (585, 3)</td>
</tr>
<tr>
<td>29</td>
<td>(591, 3)</td>
</tr>
<tr>
<td>31</td>
<td>(705, 15)</td>
</tr>
<tr>
<td>37</td>
<td>(417, 3), (517, 47), (595, 35)</td>
</tr>
<tr>
<td>41</td>
<td>(219, 3), (267, 3), (465, 3), (637, 7), (657, 3), (699, 3), (747, 3)</td>
</tr>
<tr>
<td>43</td>
<td>(551, 19), (585, 11)</td>
</tr>
<tr>
<td>47</td>
<td>(553, 7), (731, 43)</td>
</tr>
<tr>
<td>53</td>
<td>(581, 7), (585, 3), (589, 19), (639, 3)</td>
</tr>
<tr>
<td>59</td>
<td>(573, 3), (665, 35), (667, 23), (715, 11), (749, 7)</td>
</tr>
<tr>
<td>61</td>
<td>(561, 11), (663, 3), (713, 31)</td>
</tr>
<tr>
<td>67</td>
<td>(543, 3), (579, 3)</td>
</tr>
<tr>
<td>71</td>
<td>(561, 11), (657, 3)</td>
</tr>
<tr>
<td>73</td>
<td>(291, 3), (321, 3)</td>
</tr>
<tr>
<td>79</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>(437, 19), (657, 3)</td>
</tr>
<tr>
<td>89</td>
<td>(249, 3), (385, 7), (497, 7), (699, 3), (747, 3)</td>
</tr>
<tr>
<td>97</td>
<td>(537, 3), (671, 11), (705, 47), (711, 3), (713, 23)</td>
</tr>
</tbody>
</table>