Hecke stability and weight 1 modular forms

George J. Schaeffer

Received: 6 August 2014 / Accepted: 17 April 2015 / Published online: 23 May 2015
© Springer-Verlag Berlin Heidelberg 2015

Abstract The Galois representations associated to weight 1 eigenforms over $\overline{F}_p$ are remarkable in that they are unramified at $p$, but the effective computation of these modular forms presents challenges. One complication in this setting is that a weight 1 cusp form over $\overline{F}_p$ need not arise from reducing a weight 1 cusp form over $\overline{Q}$. In this article we propose a unified Hecke stability method for computing spaces of weight 1 modular forms of a given level in all characteristics simultaneously. Our main theorems outline conditions under which a finite-dimensional Hecke module of ratios of modular forms must consist of genuine modular forms. We conclude with some applications of the Hecke stability method that are motivated by the refined inverse Galois problem.

Keywords Modular forms · Computational number theory · Galois representations · Inverse Galois theory · Isogeny graphs

Mathematics Subject Classification 11F11 · 11F80 · 11Y40 · 12F12

1 Introduction and motivation

One of the major achievements of modern number theory is the discovery of a correspondence

$$\begin{cases}
\text{cuspial Hecke eigenforms of weight } k \text{ for } \Gamma_1(N) \text{ over } \overline{F}_p \\
\text{representations } \text{Gal}(\overline{Q}/Q) \to \text{GL}_2(\overline{F}_p) \end{cases} \iff \begin{cases}
\text{of ”Serre type” unramified outside } Np 
\end{cases}$$

established by the work of many researchers over the past few decades and codified in theorems of Eichler–Shimura [41], Deligne [11], Deligne and Serre [12], Khare [27], and Khare and Wintenberger [29]. The $\leftarrow$ direction was formerly Serre's conjecture.

The author was partially supported by the NSF under Grants DMS-0838697 and DMS-0854949.

George J. Schaeffer
gschaeff.research@gmail.com

1 Department of Mathematics, UCLA, 520 Portola Plaza, Math Sciences Building 6363, Los Angeles, CA 90095, USA
Given an eigenform \( f \) in \( S_k(N; \overline{\mathbb{F}}_p) \) (the space of weight \( k \) cusp forms for \( \Gamma_1(N) \) over the field \( \overline{\mathbb{F}}_p \) as defined in [26]) on the left side of the correspondence above, one can construct a number field \( K_f \) as follows: Let \( \rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{F}}_p) \) be the representation associated to \( f \) on the right, and let \( \overline{\rho}_f \) be the projectivization of \( \rho_f \). Because \( \rho_f \) is continuous, the image of \( \overline{\rho}_f \) is a finite subgroup \( G \leq \text{PGL}_2(\overline{\mathbb{F}}_p) \), and the fixed field \( K_f \) of ker \( \overline{\rho}_f \) is a \( G \)-extension of \( \mathbb{Q} \) that is unramified outside \( Np \).

This kind of construction is central to our understanding of the refined inverse Galois problem for finite subgroups of \( \text{PGL}_2 \) over \( \mathbb{Q} \). It is particularly relevant to constructing \( \text{PGL}_2(\mathbb{F}_q) \)-extensions of \( \mathbb{Q} \) with controlled ramification (PXL stands for “PGL or PSL”)—these Galois groups are nonsolvable when \( q \geq 4 \), so they are inaccessible to the methods of class field theory.

The weight 1 case of the correspondence above is unusual for several reasons:

I. **A weight 1 cusp form of level \( N \) over \( \overline{\mathbb{F}}_p \) need not arise from reducing such a form over \( \overline{\mathbb{Q}} \).**

When \( p \nmid N \), the reduction map \( S_k(N; \mathbb{Z}[1/N]) \to S_k(N; \overline{\mathbb{F}}_p) \) is surjective provided that \( k \geq 2 \), but when \( k = 1 \), surjectivity of reduction mod \( p \) can fail for finitely many \( p \) per level \( N \) (see [28] Proposition 4.1). The first example of this phenomenon is due to Mestre at \( (N, p) = (1429, 2) \) [17].

Surjectivity of \( S_1(N; \mathbb{Z}[1/N]) \to S_1(N; \overline{\mathbb{F}}_p) \) fails precisely when the cohomology group \( H^1(X_1(N), \omega(-\text{cusps})) \) has nontrivial \( p \)-torsion [28]. The data produced by our method suggest that the size of the torsion subgroup of this cohomology grows rapidly in the index of \( \Gamma_1(N) \) (see Sect. 5.1 of this paper).

One caveat: There are cases in which a given \( f \in S_1(N; \overline{\mathbb{F}}_p) \) is not the reduction of a form in \( S_1(N; \mathbb{Z}[1/N]) \), but instead there is an augmented level \( N' \) such that \( f \) is the reduction of a form in \( S_1(N'; \mathbb{Z}[1/N]) \). This was observed by Buzzard at \( (N, p) = (74, 3) \) [4]. Mestre’s prototype does not lift to a weight 1 form in characteristic zero at any level. It should also be mentioned here that we do not have general dimension formulas for spaces of weight 1 cusp forms, even over \( \mathbb{C} \).

II. **Representations associated to wt. 1 eigenforms over \( \overline{\mathbb{F}}_p \) are unramified at \( p \).**

Accordingly, the number field \( K_f \) is unramified at \( p \) when \( f \) is of weight 1. This is a theorem of Coleman and Voloch [8] with a condition at \( p = 2 \); the condition at \( p = 2 \) was removed by Wiese [46].

III. **Such representations potentially have “large image.”**

Let \( f \in S_1(N; \overline{\mathbb{F}}_p) \) be an eigenform and let \( \rho_f \) be the associated Galois representation. If \( f \) lifts to an eigenform \( f' \in S_1(N'; \overline{\mathbb{Q}}) \) for some level \( N' \) augmenting \( N \), then \( \rho_f \) lifts to an Artin representation \( \rho_{f'} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{C}) \) of conductor dividing \( N' \) by a theorem of Deligne and Serre [12]. It follows that \( \text{Gal}(K_f/\mathbb{Q}) \) is isomorphic to a finite subgroup of \( \text{PGL}_2(\mathbb{C}) \), and in particular, \( \text{Gal}(K_f/\mathbb{Q}) \) is nonsolvable only if it is isomorphic to \( A_5 \) [14].

On the other hand, if the eigenform \( f \) does not lift to a weight 1 form in characteristic zero at any level, then the image of \( \overline{\rho}_f \) is not necessarily isomorphic to a finite subgroup of \( \text{PGL}_2(\mathbb{C}) \). Given the \( q \)-expansion of \( f \) to reasonably high precision, one can verify rather quickly that \( \text{Gal}(K_f/\mathbb{Q}) \) contains a copy of \( \text{PSL}_2(\mathbb{F}_q) \) (as in [38] or [4]); if \( q \geq 4 \) then \( K_f \) must be a Galois number field with a nonsolvable Galois group, ramified only at primes dividing \( N \) (by II).

Mestre’s example yields a \( \text{PGL}_2(\mathbb{F}_8) \)-extension of \( \mathbb{Q} \) ramified only at 1429. In Sect. 5.3 we will show (among other examples) that there exists a \( \text{PGL}_2(\mathbb{F}_{74873}) \)-extension of \( \mathbb{Q} \) ramified only at 7.
IV. Known methods for computing $S_1(N; \overline{\mathbb{F}}_p)$ require computing auxiliary spaces of higher weight.

To compute a space $V$ of modular forms over a ring $R$ is to give an algorithm that produces on input $P \in \mathbb{Z}_{\geq 0}$ a generating set for the image of the truncated $q$-expansion map $V \to R[[q]]/(q^P)$ (at some fixed cusp). Because of (III.) and because there are already algorithms for computing forms of higher weights [43], our main focus in this paper is computing spaces of the form $S_1(N, \chi; F)$ where $F = \overline{\mathbb{Q}}$ or $F = \overline{\mathbb{F}}_p$ with $p \nmid N$, and where $\chi$ is an odd Dirichlet character of level $N$ taking values in $F$.

As observed by Edixhoven, one can compute $S_1(N, \chi; \overline{\mathbb{F}}_p)$ for a given value of $p$ via the exact sequence

$$0 \to S_1(N, \chi; \overline{\mathbb{F}}_p) \overset{f(q) \to f(q^p)}{\to} S_p(N, \chi; \overline{\mathbb{F}}_p) \overset{f(q) \to qf'(q)}{\to} S_{p+2}(N, \chi; \overline{\mathbb{F}}_p)$$

(see [17]), but the complexity of this method depends on the choice of $p$—one must compute the auxiliary space $S_p(N, \chi; \overline{\mathbb{F}}_p)$ whose dimension is roughly $\frac{1}{12} p^2$. For this reason and (I.) we are motivated to formulate a method for computing weight 1 modular forms that is “characteristic-free.”

Ideas in this direction can be found in [3,20], and [4]. In [4], the author computes (for all relevant $F$, as we will do in Sect. 4.3) an intersection of the form

$$\bigcap_i g_i^{-1}S_{k_i+1}(N, \chi \theta_i; F)$$

where $g_i$ is a weight $k_i$ modular form of type $(N, \theta_i)$. This intersection is equal to the target space $S_1(N, \chi; F)$ provided that all the auxiliary forms $g_i$ do not simultaneously vanish at any point of $X_1(N)(F)$. If one chooses the forms $g_i$ carefully, collisions between their zeros mod $p$ occur for only finitely many $p$, but these cases must be identified and addressed somehow.

The method we present in what follows builds on the intersection idea above; computing a space of the form $\lambda^{-1}S_2(N, 1; \mathbb{Q})$ where $\lambda$ is a weight 1 Eisenstein series of type $(N, \chi^{-1})$ is typically our first step. One advantage of our method is that for a given level $N$, $S_2(N, 1; \mathbb{Q})$ is essentially the only auxiliary space of cusp forms that must be computed. Another advantage is that our computation of $S_1(N, \chi; \overline{\mathbb{F}}_p)$ is guaranteed for sufficiently large $p$, with effective bounds.

In [17], 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 goal of this article is the development of the Hecke stability method (HSM), a procedure for computing and analyzing weight 1 modular forms in a way that takes the issues above into account. The HSM addresses and—in most cases—solves the problem posed by Edixhoven.

1.1 Outline

In Sect. 2 we outline the central ideas of the Hecke stability method and state our main results. Section 3 contains an analysis of isogeny graphs and the proofs of the Hecke stability theorems (Theorems 2.1 and 2.3). In Sect. 4 we prove Theorem 2.5 by explaining the practicalities of computing weight 1 modular forms using Hecke stability.
Finally, in Sect. 5 we give some conjectures, examples, and applications that arise from the Hecke stability method.

# 2 Hecke stability and main results

## 2.1 Hecke stability in general

For a fixed level \( N \geq 1 \) and a field \( F \) in which \( N \) is nonzero, we construct the \( F \)-algebra \( \mathcal{M}(N; F) = \bigoplus_{k \geq 0} \mathcal{M}_k(N; F) \) of (Katz) modular forms for \( \Gamma_1(N) \) graded by weight. The space of modular ratios for \( \Gamma_1(N) \) over \( F \), denoted \( \mathcal{M}^*(N; F) \), is the \( \mathbb{Z} \)-graded \( F \)-algebra generated by ratios of homogeneous elements from \( \mathcal{M}(N; F) \). We treat \( \mathcal{M}(N; F) \) as a subalgebra of \( \mathcal{M}^*(N; F) \) in the obvious fashion (see Sect. 3.1 for a more precise definition of this space).

As one might expect, much of the theory of modular forms carries over to the setting of modular ratios. In particular, the action of the Hecke algebra \( \mathcal{T} \) on this space.

The Hecke stability method depends on characterizing finite-dimensional Hecke submodules \( V \subseteq \mathcal{M}^*(N; F) \). The idea is that such spaces ought to consist of modular forms, but because of complications that arise on the supersingular locus of \( X_1(N) \) when \( \text{char}(F) > 0 \) (see Sect. 3.3 and Remark 4.11) this is not entirely true.

**Theorem 2.1** Let \( N \geq 1 \), let \( F \) be a field in which \( N \) is nonzero, and let \( \ell \) be any prime that does not divide \( N \) and that is not the characteristic of \( F \).

Suppose that \( V \) is a finite-dimensional subspace of \( \mathcal{M}^*(N; F) \) and that the Hecke operator \( T_{\ell} \) acts on \( V \).

\( a. \) If \( \text{char}(F) = 0 \), then \( V \) is a subspace of \( \mathcal{M}(N; F) \).

\( b. \) If \( \text{char}(F) = p > 0 \), there exists \( r \geq 0 \) such that \( A^r V \subseteq \mathcal{M}(N; F) \) where \( A \) is the characteristic \( p \) Hasse invariant. Therefore, if \( f \in V \) and \( f(\tau) = \infty \) for some \( \tau \in X_1(N)(F), \) \( \tau \) is supersingular.

To make the theorem above a practical tool for computing weight 1 modular forms mod \( p \), we need conditions under which the exponent \( r \) in claim (b.) is zero.

**Remark 2.2** If \( F' \) is any subfield of \( F \), then \( \mathcal{M}(N; F') = \mathcal{M}^*(N; F') \cap \mathcal{M}(N; F) \). The forward inclusion is obvious. For the other direction, if \( f \in \mathcal{M}^*(N; F') \) then the \( q \)-expansion of \( f \) has coefficients in \( F' \); because \( f \in \mathcal{M}(N; F) \) this implies that \( f \in \mathcal{M}(N; F') \) by the \( q \)-expansion principle (see [26] Corollary 1.6.2).

It will therefore suffice to prove Theorem 2.1 (and Theorem 2.3) under the assumption that \( F \) is algebraically closed.

## 2.2 Hecke stability and computing weight 1 modular forms

In light of (II.) and (III.) from the introduction, we are principally interested in computing spaces of the form \( S_1(N, \chi; F) \) where \( F \) is an algebraic extension of \( \mathbb{Q} \) or \( \mathbb{F}_p \) and \( \chi : (\mathbb{Z}/N\mathbb{Z})^* \to F^* \) is an odd character. Because of (I.) and (IV.), we want our method to depend as little as possible on the choice of \( F \).

The Hecke stability method (HSM) for computing \( S_1(N, \chi; F) \) proceeds as follows: Fix a finite nonempty \( A \subseteq \mathcal{M}_1(N, \chi^{-1}; F) - \{0\} \) whose elements can be easily computed; \( A \)
could for example consist of explicit weight 1 Eisenstein series. For each \( \lambda \in \Lambda \) there is an injective map

\[
[\lambda^{-1}] : S_2(N, 1; F) \to \text{M}_1^*(N, \chi; F) : g \mapsto g / \lambda,
\]

where \( \text{M}_1^*(N, \chi; F) \) is a space of modular ratios with modularity properties like the modular forms in \( \text{M}_1(N, \chi; F) \); in particular, \( \text{M}_1(N, \chi; F) = \text{M}(N; F) \cap \text{M}_1^*(N, \chi; F) \). Let \( V'_A(F) = \bigcap_{\lambda \in A} \text{im}[\lambda^{-1}] \). This is a finite-dimensional subspace of \( \text{M}_1^*(N, \chi; F) \) containing \( S_1(N, \chi; F) \). Elements of \( V'_A(F) \) can have poles, but these are limited to the (finite) set

\[
Z(\Lambda) = \{ \tau \in X_1(N)(\bar{F}) : \lambda(\tau) = 0 \text{ for all } \lambda \in \Lambda \}.
\]

Next, fix a prime \( \ell \) such that \( \ell \nmid N \) and \( \ell \neq \text{char}(F) \). The maximal \( T_\ell \)-stable subspace of \( V'_A(F) \), denoted by \( V'_{A,\ell}(F) \), contains the target space \( S_1(N, \chi; F) \). By Theorem 2.1 (and the remark that follows it), if \( Z(\Lambda) \) contains no supersingular points of \( X_1(N)(\bar{F}) \) we have the desired inclusions

\[
S_1(N, \chi; F) \subseteq V'_{A,\ell}(F) \subseteq \text{M}_1(N, \chi; F).
\]

Unfortunately, the assumption that \( Z(\Lambda) \) contains no supersingular points is rather strong and also somewhat expensive to verify in practice (see Remark 4.7). In fact, there are levels \( N \) for which this assumption automatically fails over \( F = \bar{F}_p \) for half of all primes \( p \) due to the vanishing of low-weight modular forms above elliptic points of \( X_0(N) \) forced by Riemann–Roch. The main focus of Sect. 3 is weakening this hypothesis on \( Z(\Lambda) \), and the theorem below summarizes the results of our efforts.

**Theorem 2.3** Let \( N \geq 1 \), let \( F \) be a field in which \( N \) is nonzero, and let \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \bar{F}^\times \) be an odd character. Fix a prime \( \ell \) such that \( \ell \nmid N \) and \( \ell \neq \text{char}(F) \), let \( \Lambda \) be a nonempty finite subset of \( \text{M}_1(N, \chi^{-1}; F) = \{0\} \), and define \( V'_{A,\ell}(F) \) and \( Z(\Lambda) \) as above.

We have \( V'_{A,\ell}(F) \subseteq \text{M}_1(N, \chi; F) \) if any one of the following conditions holds:

i. The characteristic of \( F \) is 0.

ii. The characteristic of \( F \) is \( p > 0 \) and \( Z(\Lambda) \) contains no supersingular points of \( X_1(N)(\bar{F}) \).

iii. The characteristic of \( F \) is \( p > 0 \) and there exist \( M \mid N \) and \( r \geq 2 \) satisfying \( \max\{\frac{4}{M} \ell^{4r}, 4\ell^{2r}\} \) and

\[
|\{ \tau \in \delta_{N,M} Z(\Lambda) : \tau \text{ is supersingular and non-elliptic} \}| < \ell^{[r/2]} + \ell^{[r/2]-1},
\]

where \( \delta_{N,M} : X_1(N)(\bar{F}) \to X_0(M)(\bar{F}) \) is a modular degeneracy map (see Sect. 3.2) and \( W_M \) is the set of elliptic points on \( X_0(M)(\bar{F}) \).

It is important to note that the space \( V'_{A,\ell}(F) \) is easy to compute and that the auxiliary computations involved do not depend in a crucial way on the choice of \( F \):

- A basis for \( S_2(N, 1; \mathbb{Z}[\frac{1}{N}]) \) can be computed to arbitrarily high precision by several methods (modular symbols [43], the method of graphs [31], etc.). Because reduction mod \( p \) is surjective for weight 2 cusp forms with character when \( p \neq 2, 3 \) this also yields bases for \( S_2(N, 1; \mathbb{F}_p) \) for all \( p \nmid 6N \). When \( p = 2 \) or \( p = 3 \) one must also account for the Hecke eigenspaces associated to representations induced from \( \mathbb{Q}(\sqrt{-1}) \) or \( \mathbb{Q}(\sqrt{-3}) \), respectively (see Proposition 1.10 of [16] or Proposition 4.2 of [28]).

- A standard choice for \( \Lambda \) is a finite set of weight 1 Eisenstein series for the character \( \chi^{-1} \). Such series can be computed directly as \( \ell \)-expansions over an extension of \( \mathbb{Z}[\chi] \) inverting finitely many (explicitly computable) primes [13].
The action of $T_{\ell}$ on modular ratios is integral and admits a simple interpretation on $q$-expansions (see Sect. 3.1).

The computation of $V'_{A,\ell}(F)$ therefore amounts to computing $S_2(N, 1; \mathbb{Z}[\frac{1}{N}])$ (once per level accounting for the caveats at $p = 2, 3$), a suitable $\Lambda$ (once per character), and performing some linear algebra in $F(q)$. Of course, in actual implementations, we work in $F(q)/(q^P)$ for $P$ sufficiently large; a lower bound on the precision $P$ required to unequivocally compute $V'_{A,\ell}(F)$ is in $O(\ell^2 N)$ and this bound does not depend on $F$ (see Lemma 4.6).

Remark 2.4 The perhaps unusual bounds in condition (iii.) of Theorem 2.3 are stated in order to be as general as possible; there are specific situations in which these bounds can be significantly improved (see Example 4.8 and Remark 4.10).

If we assume no a priori knowledge of $Z(\Lambda)$, then, taking $M$ to be the conductor of $\chi$, the requirements of (iii.) and a standard bound on $|\delta_{N,M}Z(\Lambda)|$ coming from Riemann–Roch on $X_0(M)$ imply that the desired inclusion holds for all $p$ larger than some bound of order $O(M^7)$.

Even when such bounds do not apply in practice, one can often certify the hypothesis $V'_{A,\ell}(F) \subseteq M_1(N, \chi; F)$ once $V'_{A,\ell}(F)$ has been computed (see Sect. 4.6).

2.3 Detection of torsion cohomology, computing in all characteristics

Because of the phenomenon described in (I.), we also require a procedure for listing those primes $p \nmid N$ for which the reduction map $S_1(N; \mathbb{Z}[\frac{1}{N}]) \rightarrow S_1(N; \mathbb{F}_p)$ is not surjective. As alluded to in the introduction, these are the primes such that $H^1(X_1(N), \omega(-\text{cusps}))$ has nontrivial $p$-torsion where $\omega$ is the sheaf of weight 1 Katz modular forms for $I_1(N)$.

It suffices to compute for each $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \bar{\mathbb{Q}}^\times$ a list $L_\chi$ containing all those prime ideals $p \subseteq \mathbb{Z}[\frac{1}{N}, \chi]$ for which $S_1(N, \chi; \mathbb{Z}[\frac{1}{N}, \chi]) \rightarrow S_1(N, \chi; \kappa_p)$ is not surjective (here $\kappa_p = \mathbb{Z}[\frac{1}{N}, \chi]/p$ and $\chi$ is also used to denote the character $(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \kappa_p^\times$ obtained by reducing $\chi$ modulo $p$).

For each character $\chi$ of level $N$, a full implementation of the Hecke stability method in all characteristics therefore requires two passes and a certification step:

- In the first pass we compute $M_1(N, \chi; \mathbb{Q}(\chi))$ using Hecke stability (as outlined in Sect. 2.2 and detailed in Sect. 4.2) and Theorem 2.3. This also produces a finite list $L_\chi$ of primes of $\mathbb{Q}(\chi)$ containing all $p$ at which reduction $S_1(N, \chi; \mathbb{Z}[\frac{1}{N}, \chi]) \rightarrow S_1(N, \chi; \kappa_p)$ is not surjective (see Sect. 4.3).
- In the second pass, for each $p \in L_\chi$, we use Hecke stability again to compute a finite-dimensional $T_{\ell}$-stable $V'(\kappa_p) \subseteq M_1^*(N, \chi; \kappa_p)$ containing $S_1(N, \chi; \kappa_p)$.
- Finally, for each $p \in L_\chi$, we must certify the Hecke stability hypothesis, the statement “$V'(\kappa_p) \subseteq M_1(N, \chi; \kappa_p)$,” by verifying one of the conditions of Theorem 2.3 or by some alternate method (see Sect. 4.6).

Putting all of our computational work together, we have the following theorem:

**Theorem 2.5** There is an algorithm that on input $(N, \chi, \ell, P)$ (with $N, \chi, \ell$ as above and $P \geq 0$) outputs the following:

- A basis for $M_1(N, \chi; \mathbb{Q}(\chi))$ computed to precision $P$;
- A (finite) list $L_\chi$ of primes $p \subseteq \mathbb{Z}[\frac{1}{N}, \chi]$ containing all those $p$ for which
  
  \[ S_1(N, \chi; \mathbb{Z}[\frac{1}{N}, \chi]) \rightarrow S_1(N, \chi; \kappa_p) \]

  is not surjective;

\[ \square \]
– For all \( p \in L \chi \) a basis for a space \( V'(\kappa_p) \) that is \( T_\ell \)-stable and that satisfies
\[
S_1(N, \chi; \kappa_p) \subseteq V'(\kappa_p) \subseteq M_1^*(N, \chi; \kappa_p); \text{ and}
\]
– Certificates that guarantee the inclusion \( V'(\kappa_p) \subseteq M_1(N, \chi; \kappa_p) \) for each \( p \in L \chi \) when possible.

### 3 Proof of the Hecke stability theorems

Throughout this section, fix a level \( N \geq 1 \) and a field \( F \) such that \( N \) is nonzero in \( F \). For simplicity of exposition, we assume throughout this section that \( F \) is algebraically closed (see Remark 2.2).

To prove Theorems 2.1 and 2.3 we will show that if \( V \subseteq M^*(N; F) \) is finite-dimensional and stable under the action of \( T_\ell \), then there is a lower bound \( B \) on the size of the set
\[
\Pi(V) = \{ \tau \in X_1(N)(F) : \text{there exists } f \in V \text{ with } f(\tau) = \infty \},
\]
provided that it is nonempty. With notation as in Sect. 2.2, we have \( |\Pi(V'_A,\ell)(F))| \leq |Z(\Lambda)| \). Therefore, if we can prove that \( B > |Z(\Lambda)| \) in a given situation, we would have \( |\Pi(V'_A,\ell)(F))| = 0 \), so \( V'_A,\ell(F) \) would necessarily consist of modular forms.

#### 3.1 Modular ratios

The space of modular ratios \( M^*(N; F) \) is the \( \mathbb{Z} \)-graded \( F \)-algebra generated by ratios of homogeneous elements from \( M(N; F) \). We denote the weight \( k \) component of \( M^*(N; F) \) by \( M_k^*(N; F) \).

Much of the theory of modular forms from [26] applies to \( M^*(N; F) \):
– Formally, a modular ratio over \( F \) of weight \( k \) is a global section of \( \omega_F^k \otimes K \) on the modular curve \( X_1(N) \), where \( \omega \) is the sheaf of weight 1 Katz modular forms on \( X_1(N) \) and \( K \) is the sheaf of rational functions on \( X_1(N) \): For example, when \( N \geq 3 \), there exists a nonzero \( \lambda \in M_2(N; F) \), so if \( f \in M_k^*(N; F) \), then \( f = (\lambda^2 \lambda q^k) \) expresses \( f \) as a product of a weight \( k \) modular form for \( \Gamma_1(N) \) and a rational function on \( X_1(N) \).
– At each cusp of \( X_1(N)(F) \) there is a \( q \)-expansion map \( M^*(N; F) \to F \ll q^{1/2} \) obtained by evaluating modular ratios at the corresponding Tate object. In practice, we work with an implicit choice of cusp such that the image of \( q \)-expansion lies in \( F \ll \ll q^{1/2} \). If \( f \) and \( g \) are homogeneous modular forms, we have \( (f/g)(q) = f(q)/g(q) \).
– \( M^*(N; F) \) inherits the action of the diamond and Hecke operators on \( M(N; F) \). These can also be defined in the usual way via degeneracy maps, and they have the expected interpretation on “test objects” as in equation (*) of the next section.
– For each character \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times \) we denote by \( M^*(N, \chi; F) \) the subspace of \( M^*(N; F) \) on which the diamond operator \( \langle d \rangle \) acts as multiplication by \( \chi(d) \) for each \( d \in (\mathbb{Z}/N\mathbb{Z})^\times \).
– If \( \lambda \in M_j(N, \chi; F) \to \{0\} \), there is an injection
\[
[\lambda^{-1}] : M_k(N, \chi; F) \to M^*_k(N, \chi \theta^{-1}; F)
\]
that takes any \( g \in M_k(N, \chi; F) \) to \( g/\lambda \).
– If \( f \in M_k^*(N, \chi; F) \) and \( \ell \) is a prime, then the \( q \)-expansion of \( T_\ell f \) (at any cusp) satisfies
\[
(T_\ell f)(q) = \sum_{n \in \mathbb{Z}} a_{\ell n/N}(f) q^{n/N} + \chi(\ell) q^{k-1} \sum_{n \in \mathbb{Z}} a_{n/N}(f) q^{\ell n/N}.\]
where \(a_r(f)\) is the coefficient of \(q^r\) in the \(q\)-expansion of \(f\) (at that same cusp). The proof of this formula is identical to the version for modular forms found in [26].

**Lemma 3.1** Suppose that \(f \in M^*_\ell(N, \chi; F)\) for some weight \(k\) and character \(\chi\), and that \(\ell\) is a prime satisfying \(\ell \nmid N\) and \(\ell \neq \text{char}(F)\).

a. If \(\tau \in X_1(N)(F)\) is a cusp and \(\text{ord}_\tau(f) < 0\), then \(\text{ord}_\tau(T_\ell f) = \ell \cdot \text{ord}_\tau(f)\).

b. If \(V \subseteq M^*(N; F)\) is finite-dimensional and stable under the action of \(T_\ell\), then

\[
\Pi(V) = \{ \tau \in X_1(N)(F) : \text{there is } f \in V \text{ such that } f(\tau) = \infty \}
\]

contains no cusps.

**Proof** Claim (a.) follows from the \(q\)-expansion formula above since \(\chi(\ell)^{\ell-1} \neq 0\). From (a.) we see that if \(\text{ord}_\tau(f) < 0\) then \(\{\text{ord}_\tau(T_\ell^n f)\}_{n \geq 0}\) is unbounded below, so any \(T_\ell\)-stable subspace containing \(f\) must be infinite-dimensional; this proves (b.) \(\square\)

### 3.2 Isogeny graphs and Hecke operators

The \(F\)-points on the modular curve \(Y_1(N) = X_1(N)-(\text{cusps})\) represent isomorphism classes of \(\Gamma_1(N)\)-structures over \(F\), and the Hecke operator \(T_\ell\) encodes an isogeny graph on these points.

A \(\Gamma_1(N)\)-structure over \(F\) is a pair \((E, P)\) where \(E/F\) is an elliptic curve and \(P \in E(F)\) has order \(N\). A \(\Gamma_0(N)\)-structure over \(F\) is a pair \((E, C)\) where \(E/F\) is an elliptic curve and \(C\) is a cyclic subgroup of \(E(F)\) satisfying \(|C| = N\). An isogeny of \(\Gamma_1(N)\)-structures \(\varphi : (E_1, \sigma_1) \to (E_2, \sigma_2)\) is an isogeny \(\varphi : E_1 \to E_2\) of elliptic curves such that \(\varphi(\sigma_1) = \sigma_2\).

We consider two isogenies \(\varphi\) and \(\psi\) to be isomorphic, denoted \(\varphi \simeq \psi\), if there are isomorphisms \(\iota_1\) and \(\iota_2\) of \(\Gamma_1(N)\)-structures that make

\[
\begin{array}{ccc}
(E_1, \sigma_1) & \varphi & (E_2, \sigma_2) \\
\downarrow \iota_1 & & \downarrow \iota_2 \\
(E'_1, \sigma'_1) & \psi & (E'_2, \sigma'_2)
\end{array}
\]

commute. We say that the isogenies \(\varphi\) and \(\psi\) are homotopic if either \(\varphi \simeq \psi\) or \(\hat{\varphi} \simeq \hat{\psi}\) (where \(\hat{\varphi}\) is the isogeny dual to \(\varphi\)); the homotopy class of \(\varphi\) will be denoted \([\varphi]\). Our justification for distinguishing between isomorphism and homotopy of isogenies will become clear later on.

Broadly speaking, an isogeny graph is a graph whose vertices are isomorphism classes of level structures and whose arcs are equivalence classes of isogenies between them. Fix \(M \mid N\) and let \(\ell\) be a prime that does not divide \(N\) and that is not the characteristic of \(F\). We will be working with the three isogeny graphs, summarized in Table 1.

A priori, all of these graphs are directed and all of them may have loops and parallel arcs with the same origin and destination (they are directed pseudographs). Because \(F\) is algebraically closed, we may identify the vertex set of \(G_\ell(\Gamma_1(N); F)\) with \(Y_1(N)(F)\) and the vertex sets of \(G_\ell(\Gamma_0(M); F)\) and \(G_\ell'(\Gamma_0(M); F)\) with \(Y_0(M)(F)\). Because of our assumptions on \(\ell\), every vertex of \(G_\ell(\Gamma_1(N); F)\) and \(G_\ell'(\Gamma_0(M); F)\) has outdegree \(\ell + 1\).

The adjacency relation of the isogeny graph \(G_\ell(\Gamma_1(N); F)\) is linked to the action of the Hecke operator \(T_\ell\) on \(M^*(N; F)\) (see also [31]). If \(f \in M^*(N; F)\), \((E, P)\) is a \(\Gamma_1(N)\)-structure over \(F\), and \(\omega\) is a nonvanishing differential on \(E\), then we can evaluate the modular ratio \(T_\ell f\) on the test object \((E, P, \omega)\) by “averaging” \(f\) over the \(\ell\)-isogenous test objects:
Let \( \Pi(\Gamma_1(N); F) \) be the quotient isogeny \([19,26]\). In particular, if \( \Pi\) is a surjective graph homomorphism such that

\[
\det_{\Pi(\Gamma_1(N); F)}(\tau, \tau') = 1,
\]

then \((T_\ell f)(\tau) = \infty\) (above, \(\deg_G(v, w)\) is the number of arcs \(v \to w\) in the directed graph \(G\)). This motivates the following definition:

**Definition 3.2** Let \( G \) be a directed graph. A subset \( P \subseteq G \) of vertices is called a **polar condition** on \( G \) if for all vertices \( v \in G \),

\[
\deg(v, P) = \sum_{w \in P} \deg(v, w) = 1
\]
only only if \( v \in P \).

By the observation preceding Definition 3.2,

**Proposition 3.3** Let \( V \subseteq M^*(N; F) \) and let

\[
\Pi(V) = \{ \tau \in X_1(N)(F) : \text{there exists } f \in V \text{ with } f(\tau) = \infty \}.
\]

If \( V \) is \( T_\ell \)-stable and \( \Pi(V) \) is nonempty, then \( \Pi(V) \subseteq Y_1(N)(F) \) (by Lemma 3.1) and \( \Pi(V) \) is a polar condition on \( G_\ell(\Gamma_1(N); F) \).

Ultimately we want to bound \(|\Pi(V)|\) from below using the fact that it is a polar condition, but working with \( \Gamma_1(N)\)-structures directly is awkward because adjacency in \( G_\ell(\Gamma_1(N); F) \) is not a symmetric relation. Instead, we will pass to the isogeny graphs on \( Y_0(M)(F) \) via the **modular degeneracy map** \( \delta_{N,M} : Y_1(N) \to Y_0(M) \) interpreted on level structures as \((E, P) \mapsto \langle E, \langle N \rangle P \rangle\). This degeneracy induces a surjective graph homomorphism \( G_\ell(\Gamma_1(N); F) \to G_\ell(\Gamma_0(M); F) \) by taking the arc \( \tau \to \tau' \) represented by some isogeny \( \phi \) to the arc \( \delta_{N,M}(\tau) \to \delta_{N,M}(\tau') \), represented by the same isogeny. We first need to show that the image of \( \Pi(V) \) under \( \delta_{N,M} \) is a polar condition on \( G_\ell(\Gamma_0(M); F) \) (provided that it is nonempty).

**Lemma 3.4** Let \( r \geq 1 \), let \( G \) and \( G' \) be directed graphs and let \( P \) be a polar condition on \( G \). Suppose \( \delta : G \to G' \) is a surjective graph homomorphism such that

i. For all vertices \( v \in G \), \( \delta : \text{arcs}_G(v, G) \to \text{arcs}_{G'}(\delta(v), G') \) is a bijection; and

### Table 1: Isogeny graphs

| Vertices             | Arcs                  |
|----------------------|-----------------------|
| \( G_\ell(\Gamma_1(N); F) \) | Isomorphism classes of \( \Gamma_1(N) \)-structures Isomorphism classes of \( \ell \)-isogenies |
| \( G_\ell(\Gamma_0(M); F) \) | Isomorphism classes of \( \Gamma_0(M) \)-structures Isomorphism classes of \( \ell \)-isogenies |
| \( G'_\ell(\Gamma_0(M); F) \) | Isomorphism classes of \( \Gamma_0(M) \)-structures Homotopy classes of \( \ell \)-isogenies |

\[
(T_\ell f)(E, P, \omega) = \frac{1}{\ell} \sum_{H \leq E/\ell} f(E/H, \varphi_H(P), \varphi_{H*}\omega)
\]

where \( H \) ranges over the (cyclic) subgroups of \( E(F) \) having order \( \ell \) and \( \varphi_H : E \to E/H \) is the quotient isogeny \([19,26]\). In particular, if \( \tau \in Y_1(N)(F) \) and

\[
\sum_{\tau' \in Y_1(N)(F)} \deg_{G_\ell(\Gamma_1(N); F)}(\tau, \tau') = 1,
\]

then \((T_\ell f)(\tau) = \infty\) (above, \(\deg_G(v, w)\) is the number of arcs \(v \to w\) in the directed graph \(G\)).
**ii. Adjacency in \( G' \) “lifts along fibers of \( \delta \)”:** For all vertices \( V', w' \in G' \),
\[
\deg_{G'}(V', w') \geq 1 \Rightarrow \forall w \in \delta^{-1}(w') \exists v \in \delta^{-1}(V') \deg_{G}(v, w) \geq 1.
\]

That is, any diagram of the form
\[
\begin{array}{c}
w \\
\delta \\
V' \\
\end{array} \quad \begin{array}{c}
v \quad \searrow \quad w \\
\delta \downarrow \\
V' \quad \searrow \quad w'
\end{array}
\]
can be completed to a diagram of the form
\[
\begin{array}{c}
w \\
\delta \\
V' \\
\end{array} \quad \begin{array}{c}
v \quad \searrow \quad w \\
\delta \downarrow \\
V' \quad \searrow \quad w'
\end{array}
\]

Then \( \delta(P) \) is a polar condition on \( G' \).

**Proof** Let \( V' \in G' \). If \( \deg_{G'}(V', \delta(P)) = 1 \), there exists \( w' \in \delta(P) \) such that \( \deg_{G'}(V', w') = 1 \). Fix \( w \in \delta^{-1}(w') \) such that \( w \in P \). By (ii.), there exists \( v \in \delta^{-1}(V') \) such that \( \deg_{G}(v, w) \geq 1 \). Since \( w \in P \), \( \deg_{G}(v, P) \geq 1 \).

On the other hand, because \( \delta : \text{arcs}_{G}(v, G) \rightarrow \text{arcs}_{G'}(V', G') \) is a bijection, \( \delta : \text{arcs}_{G}(v, P) \rightarrow \text{arcs}_{G'}(V', \delta(P)) \) is injective, so \( \deg_{G}(v, P) \leq \deg_{G}(V', \delta(P)) = 1 \). Thus \( \deg_{G}(v, P) = 1 \), so since \( P \) is a polar condition, we have \( v \in P \). Therefore, \( V' \in \delta(P) \), and this proves that \( \delta(P) \) is also a polar condition. \( \square \)

**Proposition 3.5** Let \( V \) be a subspace of \( M^*(N; F) \) and define \( \Pi(V) \) as in Proposition 3.3.

If \( V \) is stable under the action of \( T_{\ell} \) and \( \Pi(V) \) is nonempty, then \( \delta_{N,M} \Pi(V) \) is a polar condition on \( G_{\ell}(\Gamma_0(M); F) \).

**Proof** We need only prove that \( \delta_{N,M} : G_{\ell}(\Gamma_1(N); F) \rightarrow G_{\ell}(\Gamma_0(M); F) \) satisfies conditions (i.) and (ii.) of Lemma 3.4. It has property (i.) by construction. To prove that it has property (ii.), it is sufficient to show that given an \( \ell \)-isogeny of \( \Gamma_0(M) \)-structures \( \varphi : (E_1, C_1) \rightarrow (E_2, C_2) \) and \( P_1 \in E_1[N] \) with \( C_2 = (N \mod P_2) \), there exists \( P_1 \in E_1[N] \) such that
\[
\begin{array}{c}
(E_1, P_1) \xrightarrow{\varphi} (E_2, P_2) \\
\delta_{N,M} \\
(E_1, C_1) \xrightarrow{\varphi} (E_2, C_2)
\end{array}
\]
commutes. One easily verifies that \( P_1 = m \hat{\varphi}(P_2) \) where \( m \) satisfies \( \ell m \equiv 1 \mod N \) works. \( \square \)

A minor disadvantage of working with isogeny graphs on \( \Gamma_0(M) \)-structures is that \( Y_0(M)(F) \) may contain (finitely many) elliptic points—points that represent \( \Gamma_0(M) \)-structures over \( F \) whose automorphism groups are strictly larger than \( \{ \pm 1 \} \). If \( (E, C) \) represents an elliptic point, then there could be \( \varphi, \psi : (E, C) \rightarrow (E', C') \) such that \( \varphi \neq \psi \) but \( \hat{\varphi} \simeq \hat{\psi} \). This means that \( \varphi \) and \( \psi \) are homotopic but not isomorphic.

The isogeny graph \( G'_{\ell}(\Gamma_0(M); F) \) (the last graph listed in Table 1) circumvents this issue: Dualization of isogenies is a direction-reversing involution on the arc set of the graph \( G'_{\ell}(\Gamma_0(M); F) \), so we may consider it as an undirected graph whose edges are orbits \([\varphi], [\hat{\varphi}]\) under the action of dualization. It is necessary to distinguish between loops \([\varphi] : \tau \rightarrow \tau \) that are equal to their own duals (self-dual loops) from those that are not (see Remark 3.9). Every non-elliptic vertex of \( G'_{\ell}(\Gamma_0(M); F) \) has degree \( \ell + 1 \) (note that a self-dual loop contributes 1 to the degree of its vertex and a non-self-dual loop contributes 2).

Let \( W_M \) denote the set of elliptic points on \( Y_0(M)(F) \).
Lemma 3.6  a. If \( P \) is a polar condition on \( G_\ell (\Gamma_0(M); F) \), then \( P \) is a polar condition on \( G'_\ell (\Gamma_0(M); F) \) as well.

b. If \( P' \) is a polar condition on \( G'_\ell (\Gamma_0(M); F) \), then there is a polar condition \( P \) on \( G_\ell (\Gamma_0(M); F) \) such that \( P - W_M = P' - W_M \).

Proof  These follow from the fact that \( G'_\ell (\Gamma_0(M); F) \) is a subgraph of \( G_\ell (\Gamma_0(M); F) \), and the complement of this subgraph consists of (finitely many) arcs based at elliptic points of \( Y_0(M)(F) \).

\[ \square \]

3.3 Structure theory of isogeny graphs on \( Y_0(M) \)

To every \( \tau \in Y_0(M)(F) \) we assign an abstract ring \( \text{End}(\tau) \) such that for every \( \Gamma_0(M) \)-structure \( (E, C) \) representing \( \tau \),

\[ \text{End}(\tau) \cong \text{End}(E, C) = \{ \alpha \in \text{End}(E) : \alpha(C) \subseteq C \} \]

The ring \( \text{End}(\tau) \) is equipped with a conjugation operation \( \alpha \mapsto \bar{\alpha} \) (corresponding to isogeny dualization) and a multiplicative norm \( N : \text{End}(\tau) \to \mathbb{Z}_{\geq 0} : \alpha \mapsto \alpha \bar{\alpha} \) (corresponding to isogeny degree). By the elementary classification of endomorphisms of elliptic curves, \( \text{End}(\tau) \) is isomorphic to \( \mathbb{Z} \), an order of an imaginary quadratic number field, or an Eichler order of a quaternion algebra. If \( \text{End}(\tau) \) is commutative, we call \( \tau \) ordinary, and we call \( \tau \) supersingular otherwise.

Lemma 3.7  Let \( \tau, \tau' \in Y_0(M)(F) \). If \( \alpha \in \text{End}(\tau) \) and there is a homotopy class \( [\varphi] : \tau \to \tau' \), then \( \mathbb{Z}[D\alpha] \hookrightarrow \text{End}(\tau') \) where \( D = \deg \varphi \).

Proof  Choose representatives \( \varphi : (E, C) \to (E', C') \) for \( [\varphi] : \tau \to \tau' \), let \( \alpha \in \text{End}(E, C) \), and consider the diagram

\[ (E', C') \xrightarrow{\varphi} (E, C) \xrightarrow{\alpha} (E, C) \xrightarrow{\varphi} (E', C'). \]

Let \( \beta = \varphi \alpha \varphi \in \text{End}(E', C') \). The conclusion is trivial if \( \alpha \in \mathbb{Z} \), so assume otherwise.

Fix any prime \( \nu \) different from the characteristic of \( F \). Applying the Tate\(_\nu \) functor to the diagram above and choosing bases for \( \text{Tate}_\nu(E) \) and \( \text{Tate}_\nu(E') \) allows us to identify the isogenies above with \( 2 \times 2 \) matrices over \( \mathbb{Z}_\nu \).

Since \( \beta \notin \mathbb{Z} \), the minimal polynomial of \( \beta \) is equal to the characteristic polynomial of \( \text{Tate}_\nu(\varphi \alpha \varphi) \). The trace and determinant of a matrix product are invariant under cyclic permutations of the terms, so this is also equal to the characteristic polynomial of \( \text{Tate}_\nu(\varphi \alpha \varphi) = D \text{Tate}_\nu(\alpha) \). It follows that \( \beta \) and \( D\alpha \) have the same minimal polynomial, so \( \mathbb{Z}[D\alpha] \hookrightarrow \text{End}(\tau') \), as claimed. \( \square \)

Let \( G \) be an undirected subgraph of \( G'_\ell (\Gamma_0(M); F) \) and let \( \tau, \tau' \) be vertices of \( G \). The above lemma implies that if \( d = \text{dist}_G(\tau, \tau') \), then for all \( \alpha \in \text{End}(\tau), \mathbb{Z}[\ell^d\alpha] \hookrightarrow \text{End}(\tau') \).

This hints at a structural relationship between the graph \( G \) and the multiplicative monoid

\[ \text{End}(\tau) = \{ \alpha \in \text{End}(\tau) : N(\alpha) \in \ell^{\mathbb{Z}_{\geq 0}} \}, \]

a relationship we will develop and exploit heavily in what follows.

To simplify the next construction, fix representative \( \Gamma_0(M) \)-structures for each vertex of \( G \) and choose compatible representative \( \ell \)-isogenies for each arc of \( G \). We demand that if \( \varphi \) is chosen as a representative for an arc, then \( \varphi \) must be chosen as the representative of the
dual arc, so that every edge has the form \([\varphi, \tilde{\varphi}]\). For the moment we will identify \(G\) with the graph obtained via this choice of representatives. If

\[
x : (E_1, C_1) \xrightarrow{\psi_1} (E_2, C_2) \to \cdots \to (E_n, C_n) \xrightarrow{\psi_n} (E_1, C_1)
\]

is a directed cycle in \(G\) based at \((E_1, C_1)\), we set

\[
\xi_{(E_1, C_1)}(x) = \tilde{\varphi}_1 \cdots \tilde{\varphi}_n \in \text{End}(E_1, C_1).
\]

By convention, \(\xi_{(E_1, C_1)}(x) = 1\) if and only if \(x\) is the trivial cycle based at \(\tau\). We therefore obtain for each vertex \((E, C)\) a monoid homomorphism

\[
\xi_{(E, C)} : \text{[directed cycles in } G\text{ based at } (E, C)] \to \text{End}(E, C)
\]

where the operation on the left is concatenation (if \(a\) and \(b\) are paths with \(a\) ending at the origin of \(b\), then \(ab\) denotes the path obtained by first following \(a\) and then following \(b\)).

Forgetting our choices of representatives for the elements of \(G\), we obtain a family of monoid homomorphisms \(\{\xi_\tau\}_\tau\), where for each vertex \(\tau\), \(\xi_\tau\) is a map from directed cycles in \(G\) based at \(\tau\) to elements of the monoid \(\text{End}_\ell(\tau)\) defined above. Because of the many choices involved in the above construction, we explicitly avoid asserting any sort of canonicity for \(\{\xi_\tau\}_\tau\).

**Theorem 3.8** Let \(G\) be an undirected subgraph of \(\mathcal{G}_\ell(M; F)\). There is a family \(\{\xi_\tau\}_\tau\) of monoid homomorphisms indexed by the vertices of \(G\) such that

\[
\xi_\tau : \text{[directed cycles in } G\text{ based at } \tau]\to \text{End}_\ell(\tau)
\]

satisfying the following claims: If \(x\) is a directed cycle in \(G\) based at \(\tau\), then

a. \(\text{N}(\xi_\tau(x)) = \ell^{|x|}\) where \(|x|\) is the length of \(x\);

b. If \(\xi_\tau(x)\) is irreducible then \(x\) is irreducible;

c. For any other \(\tau'\) lying on \(x\), either \(\xi_\tau(x) \in \mathbb{Z}\) and \(\xi_\tau(x) = \pm \xi_\tau'(x)\), or \(\xi_\tau(x) \notin \mathbb{Z}\) and there exists an irreducible quadratic polynomial \(h \in \mathbb{Z}[t]\) such that \(h(\xi_\tau(x)) = h(\xi_\tau'(x)) = 0\);

d. \(\xi_\tau(x) \in \mathbb{Z}\) if and only if \(x\) is contractible; and

e. Each \(\xi_\tau\) induces an injective group homomorphism

\[
\tilde{\xi}_\tau : \pi_1(G, \tau) \to \frac{\text{End}_\ell(\tau)}{\mathbb{Z} \cap \text{End}_\ell(\tau)}.
\]

**Remark 3.9** We pause here for some remarks related to claim (e.) above. First of all, the monoid quotient given there is a group; inversion is induced by conjugation in \(\text{End}(\tau)\).

Secondly, self-dual loops in \(G\) contribute 2-torsion to \(\pi_1(G, \tau)\): If \(G\) is connected and \(T\) is a spanning tree for \(G\), then \(G - T\) consists of edges (finitely many, in this setting). Let \(s\) be the number of self-dual loops in \(G - T\), and let \(t\) be the number of all other edges. We have \(\pi_1(G, \tau) \simeq (\mathbb{Z}/2\mathbb{Z})^s \ast \mathbb{Z}^t\). Note that \(\pi_1(G, \tau)\) contains an element of order 2 only if \(\text{End}_\ell(\tau) \otimes \mathbb{Q}\) contains a square root of \(-\ell\).

Thirdly, if \(G\) is a connected component and \(G\) contains no elliptic points, then the group homomorphism \(\tilde{\xi}_\tau\) is actually an isomorphism for each \(\tau \in G\).

**Proof** Let \(\{\xi_\tau\}_\tau\) be the family of monoid homomorphisms constructed before the statement of the theorem. Claim (a.) and the contrapositive of claim (b.) both follow directly from the construction.

Claim (c.) is proven by applying an appropriately chosen Tate functor to \(x\) and remembering (as in the proof of Lemma 3.7) that the characteristic polynomial of a product of 2 \(\times\) 2 matrices is invariant under cyclic permutations of the terms.
Claim (d.) is proven by induction on $|x|$ in a series of if and only if statements. The case $|x| = 0$ is trivial so assume $|x| > 0$. The following are equivalent:

i. $x$ is contractible,

ii. There exist $\tau', \tau'' \in Y_0(M)(F)$ and an arc $[\varphi]: \tau' \to \tau''$ such that $x$ has the form

\[
x : \tau \to \cdots \to \tau' [\varphi] \to \tau'' [\varphi'] \to \tau' \to \cdots \to \tau
\]

where $y = ab$ is contractible, and

iii. $\xi_\tau(x) \in \mathbb{Z}$.

(i. $\iff$ ii.) follows from the construction of $G_\ell(M; F)$ as an undirected graph and a routine characterization of contractible cycles on an undirected graph. (ii. $\implies$ iii.) follows from claim (c.), the fact that $\xi_\tau([\varphi][\varphi']) = \ell$, and the inductive hypothesis.

It remains to prove (iii. $\implies$ ii.) If $\xi_\tau(x) \in \mathbb{Z} \cap \text{End}_\ell(\tau)$ and $|x| > 0$, then $\ell \mid \xi_\tau(x)$ in $\text{End}_\ell(\tau)$. Fix representatives as in the discussion preceding the theorem and suppose that

\[
x : (E_1, C_1) \to \cdots \to (E_n, C_n) \to (E_1, C_1)
\]

where for each $i$, $(E_i, C_i)$ represents $\tau_i$, and $\tau_1 = \tau$. The endomorphism $\xi_{(E_1,C_1)}(x) = \hat{\psi}_1 \cdots \hat{\psi}_n$ of $(E_1, C_1)$ is divisible by $\ell$, so its kernel contains $E_1[\ell]$. For $k$ with $0 \leq k < n$, let $\eta_k = \hat{\psi}_{n-k} \cdots \hat{\psi}_n$. Since $\ker(\eta_0)$ is cyclic but $\ker(\eta_{n-1})$ is not, there is a least $k$ such that $\ker(\eta_k)$ is not cyclic. Then $\ker(\hat{\psi}_{n-k} \hat{\psi}_{n-k+1}) = E_{n-k+2}[\ell]$, so $\hat{\psi}_{n-k} \hat{\psi}_{n-k+1}$ is multiplication by $\ell$ on the underlying elliptic curve of the $\Gamma_0(M)$-structure $(E_{n-k+2}, C_{n-k+2}) = (E_{n-k}, C_{n-k})$. It follows from how we chose representatives that $\hat{\psi}_{n-k+1} = \hat{\psi}_{n-k}$. Taking isomorphism classes of vertices and homotopy classes of arcs yields vertices $\tau' = \tau_{n-k}$, $\tau'' = \tau_{n-k+1}$, and an arc $[\varphi] = [\psi_{n-k}] : \tau' \to \tau''$ with the desired properties. Finally, to prove that the remainder cycle

\[
y : \tau_1 \to \cdots \to \tau_{n-k} [\psi_{n-k-1}] \to \tau_{n-k} [\psi_{n-k+2}] \to \tau_{n-k+3} \to \cdots \to \tau_1
\]

is contractible, note that $\xi_{\tau_1}(x) \in \mathbb{Z}$ implies $\xi_{\tau_{n-k}}(x) \in \mathbb{Z}$ by (c.), so since $\xi_{\tau_{n-k}}(x) = \ell \xi_{\tau_{n-k}}(y)$, it follows that $\xi_{\tau_{n-k}}(y) \in \mathbb{Z}$. Because $|y| < |x|$, $y$ is contractible by the inductive hypothesis.

Claim (e.) follows immediately from claim (d.).

If $G$ is a connected component of $G'_\ell(\Gamma_0(M); F)$ then either every vertex of $G$ is ordinary or every vertex of $G$ is supersingular. We may therefore distinguish between the ordinary components and the supersingular components of $G'_\ell(\Gamma_0(M); F)$.

- By Theorem 3.8.e, an ordinary component $G$ has at most one cycle, and the regularity of $G$ (away from elliptic points) implies that $G$ is infinite (it is either an infinite tree or an infinite volcano).
- There is a supersingular component iff $\text{char}(F) = p > 0$, in which case the supersingular component is unique. In contrast with the ordinary components, the supersingular component of $G'_\ell(\Gamma_0(M); F)$ is finite, and its structure can be rather complicated.

We will show that despite their apparent complexity, supersingular components of isogeny graphs resemble ordinary components “locally.” The key is the following lemma of Goren and Lauter.

**Lemma 3.10** (Goren–Lauter lemma) Let $\tau \in Y_0(M)(F)$ and let $p = \text{char}(F) > 0$. If $\alpha, \beta \in \text{End}(\tau)$ satisfy $\alpha \beta \neq \beta \alpha$, then $4N(\alpha)N(\beta) \geq Mp$. 

\[\text{Springer}\]
Proof If End(τ) is not commutative, then τ is supersingular and End(τ) is an Eichler order of level M in a quaternion algebra ramified at p and ∞; the discriminant of such an order is \( (Mp)^2 \). The proof now proceeds as in Section 2.1 of [21], which treats the case \( M = 1 \).

For example, if \( x \) and \( y \) are directed cycles based at \( τ \) in the supersingular component \( G \) of \( G'_\ell (\Gamma_0(M); F) \), and the homotopy classes of \( x \) and \( y \) do not commute in \( \pi_1(G, \tau) \), then combining the Goren–Lauter lemma with Theorem 3.8 yields

\[
\text{Lemma 3.11 Let } \tau \in Y_0(M)(F) \text{ and } r \geq 0, \text{ let } N'_\ell (\tau) \text{ be the subgraph of } G'_\ell (\Gamma_0(M); F) \text{ obtained by taking the union of all paths of length } \leq r \text{ originating from } \tau. \text{ We consider } N'_\ell (\tau) \text{ as being rooted at } \tau.
\]

\[a. \ N'_\ell (\tau) \text{ contains at most one simple cycle,} \]
\[b. \ N'_\ell (\tau) \text{ contains at most one elliptic point,} \]
\[c. \ If N'_\ell (\tau) \text{ contains both a cycle and an elliptic point, then the cycle is a loop based at the elliptic point, and} \]
\[d. \ If \tau' \in N'_\ell (\tau) \text{ is non-elliptic and } \text{dist}(\tau, \tau') < r, \text{ then } \text{deg}_N(\tau') = \ell + 1.\]

Proof If \( p \leq 3 \), the inequality \( p > \max \{ \frac{4}{M} \ell^4r, 4\ell^{2r} \} \) is never satisfied. Thus, we will assume without loss that either \( \tau \) is ordinary or that \( \tau \) is supersingular and char(\( F \)) \( \neq 2, 3 \). Let \( G \) denote the connected component of \( \tau \).

(a.) If \( G \) is acyclic or has only one simple cycle, then we are done, so assume that \( G \) has two or more simple cycles (in which case \( \tau \) is supersingular). Let \( \ell \geq 0 \) be least so that \( N'_\ell (\tau) \) contains at least two distinct simple cycles. Then, there exist directed cycles \( x \) and \( y \) based at \( \tau \) of length \( \leq 2\ell \) whose homotopy classes do not commute in \( \pi_1(G, \tau) \). Applying \( \xi_\tau \) to \( x \) and \( y \) yields elements \( \alpha, \beta \in \text{End}(\tau) \) such that \( \alpha \beta \neq \beta \alpha \) and \( N(\alpha), N(\beta) \leq \ell^{2\ell} \). By Lemma 3.10, we have \( M\ell \leq 4\ell^{4s} \). Thus, if \( p > \frac{4}{M} \ell^4r \) we must have \( r < s \), so \( N'_\ell (\tau) \) contains at most one simple cycle.

(b.) Suppose that \( \tau_1, \tau_2 \in G \) are distinct elliptic vertices. Because char(\( F \)) \( \neq 2, 3 \), the group End(\( \tau_i \)) \( ^{\times} \) is cyclic of order 4 or 6. Set \( w(\tau_i) = \frac{1}{2} \text{End}(\tau_i)^{\times} | (i = 1, 2) \) and let \( d = \text{dist}(\tau_1, \tau_2) \). We have two cases:

- 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 Lemma 3.7, there is an embedding \( \mathbb{Z}[\ell^d u_1] \hookrightarrow \text{End}(\tau_2) \). Since \( u_1 \) and \( u_2 \) cannot commute in the quaternion algebra \( \text{End}(\tau_2) \otimes \mathbb{Q}, \ell^d u_1 \) and \( u_2 \) do not commute in \( \text{End}(\tau_2) \), so \( \tau \) is supersingular. It follows from the Goren–Lauter lemma that \( 4\text{N}(\ell^d u_1)\text{N}(u_2) = 4\ell^{2d} \geq M\ell \), and therefore \( d > 2r \) (because \( M\ell > 4\ell^{4r} \)). This proves that at most one of \( \tau_1, \tau_2 \) is a vertex of \( N'_\ell (\tau) \).

- If \( w(\tau_1) = w(\tau_2) \), then there exists an elliptic curve \( E/F \) with \( j(E) \in [0, 1728] \) and distinct subgroups \( C_1, C_2 \subseteq E(F) \) cyclic of order \( M \) such that \( E(C_i) \) represents \( \tau_i \) \((i = 1, 2)\). Following a path \( \tau_1 \to \tau_2 \) of minimal length \( d \) in \( G \) yields an endomorphism \( \varphi \) of the elliptic curve \( E \) of norm \( \ell^d \) such that \( \varphi(C_1) = C_2 \). Let \( u \) generate the group \( \text{End}(E)^{\times} = \text{End}(E, C_1)^{\times} \). Since \( u(C_1) \subseteq C_1 \) but \( \varphi(C_1) \not\subseteq C_1 \), we have \( \varphi \not\subseteq \mathbb{Z}[u] \). Because \( \mathbb{Z}[u] \) is a maximal quadratic order, it follows that \( \varphi \)
and \( u \) do not commute in \( \text{End}(E) \). Thus, \( \tau \) is supersingular and the Goren–Lauter lemma (with \( M = 1 \) because \( \varphi \) is just an endomorphism of elliptic curves) yields 
\[ 4N(\varphi)N(u) = 4\ell^d \geq p, \]
Thus \( d > 2r \) (because \( p > 4\ell^{2r} \)), and again we conclude that at most one of \( \tau_1, \tau_2 \) is a vertex of \( N_\ell^r(\tau) \).

(c.) Let \( x \) and \( \tau' \) denote the unique simple cycle and the unique elliptic point on \( N_\ell^r(\tau) \), respectively. If \( a : \tau' \to \tau'' \) is a path of minimal length \( d \) from \( \tau' \) to a vertex \( \tau'' \) on the cycle \( x \), then \( y = ax\tilde{a} \) is a directed cycle in \( N_\ell^r(\tau) \) based at \( \tau' \) (with either direction assigned to \( x \)). Let \( \alpha = \xi_{\tau'}(ax\tilde{a}) \), so \( N(\alpha) = \ell|x|^2+2d \) where \( |x| \leq 2r \) and \( d \leq 2r \).

Fix a generator \( u \) for \( \text{End}(\tau')^\times \). If \( au \neq ua \), then by Lemma 3.10,
\[ 4N(\alpha)N(u) = 4\ell|x|^2+2d \geq Mp > 4\ell^{4r} \]
which is impossible because \( |x| + 2d \leq 4r \).

Therefore, we must have \( au = ua \), so \( \alpha \in \mathbb{Z}[u] \) (because \( \mathbb{Z}[u] \) is a maximal order). Now, \( \ell | \alpha \) in \( \mathbb{Z}[u] \); otherwise there would be a pair of consecutive dual edges in \( y \) as in the proof of Theorem 3.8.d, contradicting either the minimality of \( d \) or the simplicity of \( x \). It follows that \( \alpha \) is neither a positive power of \( \ell \) nor an associate of such an element, so since \( N(\alpha) \) is a positive power of \( \ell \), \( \ell \) must be split or ramified in \( \mathbb{Z}[u] \). Because \( \mathbb{Z}[u] \) has class number 1, there exists \( \pi \in \mathbb{Z}[u] \subseteq \text{End}_\ell(\tau') \) with \( N(\pi) = \ell \), and the homotopy class of \( \pi \) (viewed as an \( \ell \)-isogeny) is a loop \([\pi] : \tau' \to \tau'\). By the uniqueness of \( x \), \( x = [\pi] \).

Claim (d.) follows from the fact that all non-elliptic vertices in \( G'_\ell(\Gamma_0(M); F) \) have degree \( \ell + 1 \). \( \square \)

### 3.4 Lower bounds on polar conditions

The next step is to use Lemma 3.11 to formulate lower bounds on polar conditions on \( G'_\ell(\Gamma_0(M); F) \).

For \( n \geq 2 \) and \( i > -n \), let \( T(n, i) \) denote the infinite rooted tree such that the root has degree \( n + i \) and every other vertex has degree \( n \). If \( r \geq 0 \), let \( T^r(n, i) \) be the subgraph of \( T(n, i) \) induced on the vertex set \( \{ v : \text{dist}_{T(n, i)}(v_0, v) \leq r \} \) where \( v_0 \) is the root of \( T(n, i) \). The graph \( T^r(n, i) \) is a full rooted tree of depth \( r \).

When \( T \) is a tree, we say that a nonempty vertex subset \( Q \subseteq T \) is quasipolar if for all vertices \( v \in T \) the condition \( \deg(v, Q) = 1 \) implies that \( v \in Q \) or that \( v \) is a leaf of \( T \). If \( P \) is a polar condition on \( T(n, i) \), then \( P \cap T^r(n, i) \) is quasipolar on \( T^r(n, i) \); conversely, if \( Q \subseteq T^r(n, i) \) is quasipolar, there exists a polar condition \( P \subseteq T(n, i) \) such that \( Q = P \cap T^r(n, i) \). We define
\[ b^r(n, i) = \min_{P \subseteq T(n, i)} |P \cap T^r(n, i)| = \min_{Q \subseteq T^r(n, i)} |Q| \]
where \( P \) ranges over all polar conditions on \( T(n, i) \) that contain the root and \( Q \) ranges over all quasipolar subsets of \( T^r(n, i) \) that contain the root.

**Lemma 3.12** If \( r \geq 0, n \geq 2, \) and \( i > -n \), we have
\[ b^r(n, i) = 1 + (n + i) \sum_{j=0}^{\lfloor r/2 \rfloor-1} (n - 1)^j. \]
Proof First, we claim that the right hand side is a lower bound on \( b^r(n,i) \). This is trivial when \( r = 0 \) or \( r = 1 \). Suppose that \( r \geq 2 \) and that \( P \) is a polar condition on \( T(n,i) \) that contains the root. If \( v \) is any vertex of \( T^r(n,i) \) let \( T[v] \) denote the subtree of \( T^r(n,i) \) rooted at \( v \) and containing all descendants of \( v \). Let \( v_1, \ldots, v_{n+i} \) denote the children of the root \( v_0 \) and observe that for each \( k \), either \( v_k \in P \) or \( v'_k \in P \) for some child \( v'_k \) of \( v_k \). In the former case, \( T[v_k] \simeq T^{r-1}(n,-1) \) and \( |P \cap T[v_k]| \geq b^{r-1}(n,-1) \); in the latter case, \( T[v'_k] \simeq T^{r-2}(n,-1) \) and \( |P \cap T[v'_k]| \geq |P \cap T[v_k]| \geq b^{r-2}(n,-1) \). Since \( b^{r-1}(n,-1) \geq b^{r-2}(n,-1) \) and \( v_0 \in P \), it follows that

\[
|P \cap T^r(n,i)| = 1 + \sum_{k=1}^{n+i} |P \cap T[v_k]| \geq 1 + (n+i)b^{r-2}(n,-1),
\]

and our claim follows by induction.

On the other hand, a straightforward construction yields a polar condition \( P \) on \( T(n,i) \) with

\[
|P \cap \{ v : \text{dist}_{T(n,i)}(v_0,v) = r \}| = \begin{cases} 
1 & \text{if } r = 0, \\
(n+i)(n-1)^{r/2-1} & \text{if } r \text{ is even and } r \geq 2, \\
0 & \text{if } r \text{ is odd,}
\end{cases}
\]

from which we conclude that the right hand side is also an upper bound on \( b^r(n,i) \). \( \square \)

A graph containing a unique simple cycle is called a volcano (see for example [2]); the crater of a volcano is its unique simple cycle. For \( n \geq 3 \) and \( c \geq 1 \) let \( \mathcal{V}(n,c) \) denote the infinite \( n \)-regular volcano with a crater of length \( c \), rooted at some vertex \( v_0 \) on the crater (the particular choice of root being otherwise unimportant). For \( r \geq 0 \), let \( \mathcal{V}^r(n,c) \) be the subgraph of \( \mathcal{V}(n,c) \) induced on the vertex set \( \{ v : \text{dist}_{\mathcal{V}(n,c)}(v_0,v) \leq r \} \).

Lemma 3.13 Let \( r \geq 0 \), \( n \geq 3 \), and \( c \geq 3 \). Suppose that \( P \) is a polar condition on \( \mathcal{V}(n,c) \) containing the root \( v_0 \). If \( r \geq 2 \), then

\[
|P \cap \mathcal{V}^r(n,c)| \geq (n-1)^{\lceil r/2 \rceil} + (n-1)^{\lfloor r/2 \rfloor - 1}
\]

Proof Let \( x \) be the crater of \( \mathcal{V}(n,c) \).

![Fig. 1 A typical isogeny graph](image-url)
For any vertex \( v \) of \( V^r(n, c) \) let \( T[v] \) denote the subtree of \( V^r(n, c) \) rooted at \( v \) and containing all descendants of \( v \) (in Fig. 1, \( T' = T[v_0] \)); formally, \( T[v] \) is the subgraph induced on the vertex set

\[
\{ w : \text{dist}(w, x) \geq \text{dist}(v, x) \text{ and every path } w \to x \text{ contains } v \}
\]

where \( x \) is the crater of \( V(n, c) \).

Let \( T' = T[v_0] \) (as in Fig. 1) and note that \( T' \simeq T^r(n, -2) \).

Choose vertices \( v_1 \) and \( v_2 \) on the crater so that there is a path \( v_0 \to v_1 \to v_2 \) of length 2 (as in the figure). Remembering that \( v_0 \in P \), we define \( T'' \) according to three cases:

i. If \( v_1 \in P \), let \( T'' = T[v_1] \). In this case \( T'' \simeq T^r-1(n, -2) \).

ii. If \( v_1 \notin P \), and there exists a child \( v'_1 \) of \( v_1 \) on \( T[v_1] \) such that \( v'_1 \in P \), let \( T'' = T[v'_1] \), so \( T'' \simeq T^r-2(n, -1) \).

iii. Otherwise we must have \( v_2 \in P \) since \( P \) is a polar condition and \( v_0 \in P \). In this case, let \( T'' = T[v_2] \), so \( T'' \simeq T^r-2(n, -2) \).

In each of these cases, \( P \cap T' \) and \( P \cap T'' \) are quasipolar and contain the roots of \( T' \) and \( T'' \), respectively. Thus,

\[
|P \cap V^r(n, c)| \geq |P \cap T'| + |P \cap T''| \geq b^r(n, -2) + \begin{cases} b^{r-1}(n, -2) & \text{in case (i.)}, \\ b^{r-2}(n, -1) & \text{in case (ii.)}, \\ b^{r-2}(n, -2) & \text{in case (iii.)}. \end{cases}
\]

The bound in case (iii.) is the weakest, so Lemma 3.12 yields

\[
|P \cap V^r(n, c)| \geq b^r(n, -2) + b^{r-2}(n, -2) = (n - 1)^{\lceil r/2 \rceil} + (n - 1)^{\lceil r/2 \rceil - 1}.
\]

\[\square\]

**Lemma 3.14** Let \( G \) be a connected component of \( G'_\ell(\Gamma_0(M); F) \) and let \( P \) be a polar condition on \( G \). Suppose either that \( G \) is ordinary or that \( G \) is supersingular and \( p = \text{char}(F) \) satisfies \( p > \max\{\frac{4}{M}\ell^8, 4\ell^4\} \).

There exists \( \tau \in P \) such that \( \tau \) is not elliptic and \( \tau \) lies on no cycles of length \( \leq 2 \).

**Proof** Fix \( \tau_0 \in P \) and assume without loss that \( \tau_0 \) is either elliptic or that it lies on a cycle of length \( \leq 2 \). Applying Lemma 3.11 with \( r = 2 \) and some simple arguments using the fact that \( P \) is a polar condition (like those in the proof of Lemma 3.13) yield \( \tau \in P \) with the desired properties. \[\square\]

**Lemma 3.15** Let \( G \) be a connected component of \( G'_\ell(\Gamma_0(M); F) \) and let \( P \) be a polar condition on \( G \).

a. If \( G \) is ordinary then \( P \) is infinite.

b. If on the other hand \( G \) is supersingular and \( p = \text{char}(F) \), then for all \( r \geq 2 \) satisfying

\[
\max\{\frac{4}{M}\ell^{4r}, 4\ell^{2r}\} < p \text{ we have } |P - W_M| \geq \ell^{\lceil r/2 \rceil} + \ell^{\lceil r/2 \rceil - 1} \text{ where } W_M \text{ is the set of elliptic points on } Y_0(M)(F).
\]

**Proof** By Lemma 3.6 it is sufficient to prove the claim upon replacing \( G'_\ell(\Gamma_0(M); F) \) with the undirected graph \( G'_\ell(\Gamma_0(M); F) \).

Let \( G \) be a connected component of \( G'_\ell(\Gamma_0(M); F) \), let \( r \geq 2 \), and assume either that \( G \) is ordinary or that \( G \) is supersingular and \( p > \max\{\frac{4}{M}\ell^{4r}, 4\ell^{2r}\} \).

By Lemma 3.14 we may choose \( \tau \in P \) such that \( w(\tau) = 1 \) and such that \( \tau \) does not lie on any cycles of length \( \leq 2 \). Let \( G_0 = N^r_\ell(\tau) \). Following Lemma 3.11 there are four cases:
\( (G_0 \text{ contains no cycles and no elliptic points.}) \) In this case, \( G_0 \) is isomorphic to \( T' (\ell + 1, 0) \) as a rooted graph and \( P \cap G_0 \) is quasipolar on \( G_0 \), so \( |P \cap G_0| \geq b'(\ell + 1, 0) \). Applying Lemma 3.12 yields
\[
|P \cap G_0| \geq \ell^{(r/2)} + \ell^{(r/2)-1}
\]
and \( P \cap G_0 \) contains no elliptic points.

\( (G_0 \text{ contains a cycle } x \text{ and } \tau \in x.) \) In this case, \( G_0 \) is isomorphic to \( V' (\ell + 1, |x|) \) as a rooted graph and \( P \cap G_0 \) extends to a polar condition on \( V(\ell + 1, |x|) \). Since \( |x| \geq 3 \), Lemma 3.13 guarantees that \( |P \cap G_0| \geq \ell^{(r/2)} + \ell^{(r/2)-1} \) and Lemma 3.11 guarantees that \( P \cap G_0 \) contains no elliptic points.

\( (G_0 \text{ contains a cycle } x \text{ and } \tau \neq x.) \) Because \( G_0 \) contains exactly one cycle, there is a unique shortest path \( a : \tau \to x \). Let \( e \) be the first edge on this path, and consider \( G_0 - \{e\} \). The connected component \( G_1 \) of \( G_0 - \{e\} \) containing and rooted at \( \tau \) is isomorphic as a rooted graph to \( T'(\ell + 1, -1) \). \( P \cap G_1 \) is quasipolar on \( G_1 \), so by Lemma 3.12,
\[
|P \cap G_0| \geq |P \cap G_1| \geq b'(\ell + 1, -1) \geq \ell^{(r/2)} + \ell^{(r/2)-1}
\]
and \( P \cap G_1 \) contains no elliptic points (by Lemma 3.11).

\( (G_0 \text{ contains an elliptic point } \tau'). \) Since \( \tau \neq \tau' \), we may proceed as in the previous case with \( \tau' \) replacing \( x \).

We conclude in every case that \( |P \cap G - W_M| \geq \ell^{(r/2)} + \ell^{(r/2)-1} \). This proves (b.) directly and it proves (a.) by taking \( r \to \infty \).

**Proof (of Theorem 2.1)** (We continue to assume \( F \) is algebraically closed, see Remark 2.2.) Suppose that \( V \subseteq M^*(N; F) \) is stable under the action of the Hecke operator \( T_\ell \). The vertex set \( \delta_{N, N} \Pi(V) \) is a polar condition on \( G_\ell(\Gamma_0(N); F) \) by Proposition 3.3.

If there is a cusp \( \tau \in X_0(N)(F) \) and \( f \in V \) such that \( f(\tau) = \infty \), then \( V \) is infinite-dimensional by Lemma 3.1. If there is an ordinary \( \tau \in Y_0(N)(F) \) and \( f \in V \) such that \( f(\tau) = \infty \), then an ordinary component \( G \) of \( G_\ell(\Gamma_0(N); F) \) meets the polar condition \( \delta_{N, N} \Pi(V) \). Since \( G \cap \delta_{N, N} \Pi(V) \) is a polar condition on the ordinary component \( G \), it is infinite (Lemma 3.15.a). It follows that \( \Pi(V) \) is infinite, so \( V \) is infinite-dimensional. This proves Theorem 2.1.a.

By the preceding argument, if \( V \) is finite-dimensional and \( T_\ell \)-stable, \( \Pi(V) \) consists of supersingular points. Since the Hasse invariant \( A \) has a simple root at every supersingular point on \( X_1(N)(F) \), there is \( r \geq 0 \) large enough so that \( A^r \cdot V \) contains no modular ratios with poles. This proves Theorem 2.1.b.

**Proof (of Theorem 2.3)** With notation as in the statement of the theorem (and \( F \) algebraically closed), we have \( \Pi(V'_{\ell, \ell}(F)) \subseteq Z(A) \). The sufficiency of conditions (i.) and (ii.) follow directly from Theorem 2.1.a. The sufficiency of condition (iii.) follows from Lemma 3.15.b.

**4 Hecke stability and computation**

We will now demonstrate how to use the Hecke stability theorems to compute spaces of weight 1 modular forms.

Using the \( q \)-expansion map at our chosen cusp we will identify modular ratios over a field \( \kappa \) (not necessarily algebraically closed) with their images in \( \kappa(q) \) under \( q \)-expansion. For a given \( P \in Z \) we let \( (q^P) \) denote the subspace of \( \kappa(q) \) spanned by \( \{q^n\}_{n \geq P} \). To compute a
finite-dimensional \( W \subseteq \kappa(\langle q \rangle) \) is to give an algorithm that on input \( P \in \mathbb{Z}_{\geq 0} \) outputs a basis for \( W \mod (q^P) \)—that is, a basis for \( W \) computed to precision \( P \).

Fix a choice of level \( N \geq 1 \), a character \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \bar{\mathbb{Q}}^\times \), and a prime \( \ell \nmid N \). Let \( K = \mathbb{Q}(\chi) \), and for every nonzero prime ideal \( \mathfrak{p} \subseteq \mathcal{O}_K \) (including zero) let \( \kappa_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p} \) (here \( \mathcal{O}_\mathfrak{p} \) denotes the \( \mathfrak{p} \)-integral subring of \( K \); \( \mathcal{O}_0 = \kappa_0 = K \)). The goal of the Hecke stability method is to compute for (almost) all prime ideals \( \mathfrak{p} \mid N \), a finite-dimensional \( T\ell \)-stable space \( V'(\kappa_\mathfrak{p}) \) of modular ratios such that

\[
S_1(N, \chi; \kappa_\mathfrak{p}) \subseteq V'(\kappa_\mathfrak{p}) \subseteq \mathcal{M}_1^*(N, \chi; \kappa_\mathfrak{p})
\]

where \( \chi \) is also used to denote the character obtained by composing with reduction mod \( \mathfrak{p} \). Theorem 2.3 guarantees that \( V'(\kappa_0) \) consists of modular forms, but checking the analogous statements for \( V'(\kappa_\mathfrak{p}) \) with nonzero \( \mathfrak{p} \) require more work.

### 4.1 Integral subspace operations

To simplify the exposition of the next few sections, we introduce the notion of an integral subspace operation on Laurent series. Let \( W \) be a finite-dimensional subspace of \( K(\langle q \rangle) \) (as a \( K \)-vector space) and let \( \mathfrak{p} \) be a prime of \( K \) (possibly zero). Define \( \text{Red}_\mathfrak{p}(W) \) to be the subspace of \( \kappa_\mathfrak{p}(\langle q \rangle) \) obtained by reducing \( W \cap \mathcal{O}_\mathfrak{p}(\langle q \rangle) \) modulo \( \mathfrak{p} \). We say that \( W \) has **good reduction at** \( \mathfrak{p} \) if \( \dim K(W) = \dim_{\kappa_\mathfrak{p}} \text{Red}_\mathfrak{p}(W) \).

**Definition 4.1** Let \( S \) be a set of prime ideals of \( K \) such that \( 0 \in S \) (in applications, \( S \) will consist of “good” primes). An **\( S \)-integral subspace operation** in \( K(\langle q \rangle) \) is a family \( \mathcal{F} = \{ \mathcal{F}_\mathfrak{p} \}_{\mathfrak{p} \in S} \) of maps for each \( \mathfrak{p} \),

\[
\mathcal{F}_\mathfrak{p} : \{ \text{finite-dimensional subspaces of } \kappa_\mathfrak{p}(\langle q \rangle) \} \to \{ \text{finite-dimensional subspaces of } \kappa_\mathfrak{p}(\langle q \rangle) \}
\]

satisfying the following: For all \( \mathfrak{p} \),

- The map \( \mathcal{F}_\mathfrak{p} \) is monotonic with respect to containment, and
- If \( V \subseteq K(\langle q \rangle) \) is finite-dimensional and \( V \) has good reduction at \( \mathfrak{p} \), then

\[
\text{Red}_\mathfrak{p} \mathcal{F}_0(V) \subseteq \mathcal{F}_\mathfrak{p} \text{Red}_\mathfrak{p}(V).
\]

We are primarily concerned with two kinds of subspace operations:

- **Intersection operations** Let \( U \) be a subspace of \( K(\langle q \rangle) \) that has good reduction at every prime ideal in \( S \). Define the **intersection operation** (with \( U \)) \( \mathcal{T}^U = \{ \mathcal{T}^U_\mathfrak{p} \}_{\mathfrak{p} \in S} \) by \( \mathcal{T}^U_\mathfrak{p}(W) = W \cap \text{Red}_\mathfrak{p}(U) \) for all \( \mathfrak{p} \in S \) and any finite-dimensional \( W \subseteq \kappa_\mathfrak{p}(\langle q \rangle) \).

- **Stabilization operations** Let \( T \) be a linear operator on \( K(\langle q \rangle) \) that restricts to an \( \mathcal{O}_\mathfrak{p} \)-module endomorphism on \( \mathcal{O}_\mathfrak{p}(\langle q \rangle) \) for all nonzero \( \mathfrak{p} \in S \). Then, for all \( \mathfrak{p} \in S \), there exists a unique linear transformation \( T : \kappa_\mathfrak{p}(\langle q \rangle) \to \kappa_\mathfrak{p}(\langle q \rangle) \) such that \( \text{Red}_\mathfrak{p} \circ T = T \circ \text{Red}_\mathfrak{p} \).

Define the **stabilization operation** (with respect to \( T \)) \( \mathcal{S}^T = \{ \mathcal{S}^T_\mathfrak{p} \}_{\mathfrak{p} \in S} \) by \( \mathcal{S}^T_\mathfrak{p}(W) = \{ g \in W : Tg \in W \} \) for all \( \mathfrak{p} \in S \) and any finite-dimensional \( W \subseteq \kappa_\mathfrak{p}(\langle q \rangle) \).

It is a straightforward exercise to verify that intersection operations and stabilization operations are subspace operations. The existence of \( T : \kappa_\mathfrak{p}(\langle q \rangle) \to \kappa_\mathfrak{p}(\langle q \rangle) \) above is not entirely trivial: One must check that if \( T \) restricts to an \( \mathcal{O}_\mathfrak{p} \)-module endomorphism on \( \mathcal{O}_\mathfrak{p}(\langle q \rangle) \) then \( \mathfrak{p}\mathcal{O}_\mathfrak{p}(\langle q \rangle) \) is a \( T \)-stable submodule—this is easy when \( \mathfrak{p} \) is principal, and the general case follows from the finiteness of \( \text{Cl}(K) \).
4.2 The Hecke stability method via integral subspace operations

In this section we present the theoretical details of the computation described in Sect. 2.2. This computation can be expressed as a composition of intersection operations and stabilization operations on Laurent series, introduced in the previous section. The practical details (precision requirements and linear algebra) of the computations are left to Sections 4.4 and 4.5 (respectively).

We begin by fixing a finite nonempty \( \Lambda \subseteq M_1^p(N, \chi^{-1}; K) - \{0\} \subseteq K(\langle q \rangle) \). It is ideal (but not necessary) that \( Z(\Lambda) \subseteq X_1(N)(K) \) be as small as possible and contain no cusps (despite Lemma 3.1, poles at the cusps typically increase the number of subspace operations required to compute the Hecke-stable subspace). Index \( \Lambda = \{\lambda_0, \ldots, \lambda_s\} \) and let \( U_i = \text{im}[\lambda_i^{-1}] \) where for each \( \lambda \in \Lambda \),

\[
[\lambda^{-1}] : S_2(N, 1; K) \rightarrow M_1^p(N, \chi; K) : g \mapsto g/\lambda.
\]

For all primes \( p \nmid 6N \), the reduction map \( S_2(N, 1; \mathcal{O}_K[\frac{1}{N}]) \rightarrow S_2(N, 1; \mathcal{O}_p) \) is surjective and \( S_2(N, 1; K) \) has good reduction away from \( N \) (one must account for some extra forms when \( \kappa_p \) has characteristic 2 or 3, see Proposition 1.10 of [16] or Proposition 4.2 of [28]; these cases do not present further difficulties, but we will suppress them for convenience). Let

\[
b = \prod_{\exists \lambda \in \Lambda \, \lambda \equiv 0 \, \text{ mod } p} p.
\]

Note that if \( p \nmid 6Nb \), every member of \( \{U_i\}_{0 \leq i \leq s} \) has good reduction at \( p \).

Choose \( \ell \nmid N \) and let \( S = \{p \subseteq \mathcal{O}_K : p \nmid 6\ell Nb\} \). Denote by \( T_\ell^Z \) the operator on \( K(\langle q \rangle) \) given by

\[
\sum_{n \in \mathbb{Z}} a_n q^n \mapsto \sum_{n \in \mathbb{Z}} a_{\ell n} q^n + \chi(\ell) \sum_{n \in \mathbb{Z}} a_n q^{\ell n}.
\]

\( T_\ell^Z \) coincides with \( T_\ell \) on \( M_1^p(N, \chi; F) \) (see Sect. 3.1) and it restricts to a module homomorphism \( \mathcal{O}_p(\langle q \rangle) \rightarrow \mathcal{O}_p(\langle q \rangle) \) for any \( p \in S \). We set the following notation:

- For all \( i \geq 1 \), let

\[
\mathcal{X}^{(i)} = \begin{cases} X_{U_i} & \text{if } i \leq s \\ S T_\ell^Z & \text{otherwise,} \end{cases}
\]

- Let \( V_{A,\ell}^{(0)}(\kappa_p) = \text{Red}_p(U_0) \), and for all \( i \geq 1 \), let \( V_{A,\ell}^{(i)}(\kappa_p) = T_\ell^Z V_{A,\ell}^{(i-1)}(\kappa_p) \).

Because \( \dim_{\kappa_p} V_{A,\ell}^{(0)}(\kappa_p) = \dim_{\kappa_p} S_2(N, 1; \kappa_p) \) is finite and independent of the choice of \( p \in S \), there exists \( t \) such that \( V_{A,\ell}^{(s+t)}(\kappa_p) \) is a \( T_\ell \)-stable subspace of \( M_1^p(N, \chi; \kappa_p) \) for all \( p \). In the notation of Sect. 2.2 (which we will continue to use), \( V_A' = V_{A,\ell}^{(s)}(\kappa_p) \) and \( V'_A(\kappa_p) = V_{A,\ell}^{(s+t)}(\kappa_p) \). For each \( p \) the space \( V'_A(\kappa_p) \) is \( T_\ell \)-stable and contains \( S_1(N, \chi; \kappa_p) \). Schematically,
for each \( p \in S \).

### 4.3 Nonsurjectivity of reduction

Next, we will show how the Hecke stability method can be used to produce a family \( \{ V'(\kappa_p) \}_{p \in S} \) where each \( V'(\kappa_p) \) is a \( T_\ell \)-stable subspace of \( \mathcal{M}_1^*(N, \chi; \kappa_p) \) containing \( S_1(N, \chi; \kappa_p) \).

First, recall that for almost all nonzero \( p \in S \) the reduction map \( S_1(N, \chi; \mathcal{O}_p) \rightarrow S_1(N, \chi; \kappa_p) \) is surjective. For such \( p \), taking \( V'(\kappa_p) = \text{Red}_p V'_{A, \ell}(K) \) works, provided that \( V'_{A, \ell}(K) \) also has good reduction at \( p \). We therefore only need to compute \( V'_{A, \ell}(\kappa_p) \) directly for \( p = 0 \), for the (finitely many) \( p \) at which reduction is nonsurjective, and for the (finitely many) \( p \) at which \( V'_{A, \ell}(K) \) has bad reduction.

Determining the list of primes at which reduction is nonsurjective provides the most difficulty. The idea is that when surjectivity of \( S_1(N, \chi; \mathcal{O}_p) \rightarrow S_1(N, \chi; \kappa_p) \) fails for a given \( p \), the surjectivity of

\[
V'_{A, \ell}(K) \cap \mathcal{O}_p \langle q \rangle \rightarrow V^{(i)}_{A, \ell}(\kappa_p)
\]

must fail for some minimal index \( i \). With some mild hypotheses, this is the case precisely when \( p \) is a divisor of the subspace operation \( \mathcal{F}^{(i)} \) (as defined below). In Sect. 4.5 we describe how a finite list containing the prime divisors of a given subspace operation can be computed in practice.

**Definition 4.2** Let \( \mathcal{F} \) be an \( S \)-integral subspace operation, let \( V \) be a finite-dimensional subspace of \( K \langle q \rangle \), let \( p \in S \), and suppose that both \( V \) and \( \mathcal{F}_0(V) \) have good reduction at \( p \).

We say that \( p \) divides \( \mathcal{F} \) at \( V \) if \( \text{Red}_p \mathcal{F}_0(V) \varsubsetneq \mathcal{F}_p \text{Red}_p(V) \), i.e., when the inclusion from Definition 4.1 is proper.

Recall that \( p \) is called an Eisenstein congruence prime for \( (k, N, \chi) \) if there exists an Eisenstein series and a cusp form of that type that are congruent to each other modulo \( p \).

Such \( p \) divide the numerator ideal of \( \frac{1}{k} B_{k, \chi} = -L(1 - k, \chi) \).

**Proposition 4.3** Fix \((N, \chi, \Lambda, \ell)\) and \( S \) as above.

Let \( L = L' \cup L'' \cup L''' \) where

\[
L' = \{ p \in S : \text{there is } j \text{ such that } p \text{ divides } \mathcal{F}^{(j+1)} \text{ at } V_{A, \ell}^{(j)}(K) \},
\]

\[
L'' = \{ p \in S : \text{there is } j \text{ such that } V_{A, \ell}^{(j)}(K) \text{ has bad reduction at } p \}, \text{ and}
\]

\[
L''' = \{ p \in S : p \text{ is an Eisenstein congruence prime for } (1, N, \chi) \}.
\]

Then \( L \) is finite and it contains all \( p \in S \) such that \( S_1(N, \chi; \mathcal{O}_p) \rightarrow S_1(N, \chi; \kappa_p) \) is not surjective.
Proof Suppose that $S_1(N, \chi; O_p) \rightarrow S_1(N, \chi; \kappa_p)$ is not surjective and, without loss, that $p \notin L'' \cup L''$. Because $p \notin L''$, there exists $f \in S_1(N, \chi; \kappa_p)$ that does not lift to any element of $M_1(N, \chi; O_p)$. Since $V_{A, \ell}^{(s+1)}(K)$ has good reduction at $p$, Hecke stability guarantees

$$V_{A, \ell}^{(s+1)}(K) \cap O_p((q)) \subseteq M_1(N, \chi; O_p)$$

by Theorem 1.3.i, and $S_1(N, \chi; \kappa_p) \subseteq V_{A, \ell}^{(s+1)}(\kappa_p)$, and it follows that $\text{Red}_p V_{A, \ell}^{(s+1)}(K) \subseteq V_{A, \ell}^{(s+1)}(\kappa_p)$.

On the other hand, $\text{Red}_p V_{A, \ell}^{(0)}(K) = V_{A, \ell}^{(0)}(\kappa_p)$ and—since $p \notin L''$ and each $\mathcal{F}^{(i)}$ is an $S$-integral subspace operation—$\text{Red}_p V_{A, \ell}^{(i)}(K) \subseteq V_{A, \ell}^{(i)}(\kappa_p)$ for all $i$. Hence, there exists a least $j$ satisfying

$$\text{Red}_p V_{A, \ell}^{(j)}(K) = V_{A, \ell}^{(j)}(\kappa_p) \text{ and } \text{Red}_p V_{A, \ell}^{(j+1)}(K) \subseteq V_{A, \ell}^{(j+1)}(\kappa_p).$$

By definition, $V_{A, \ell}^{(j+1)}(K) = \mathcal{F}_0^{(j+1)} V_{A, \ell}^{(j)}(K)$ and $V_{A, \ell}^{(j+1)}(\kappa_p) = \mathcal{F}_p^{(j+1)} \text{Red}_p V_{A, \ell}^{(j)}(K)$. In summary, $V_{A, \ell}^{(j)}(K)$ and $\mathcal{F}_0^{(j+1)} V_{A, \ell}^{(j)}(K)$ both have good reduction at $p$, but the containment

$$\text{Red}_p \mathcal{F}_0^{(j+1)} V_{A, \ell}^{(j)}(K) \subseteq \mathcal{F}_p^{(j+1)} \text{Red}_p V_{A, \ell}^{(j)}(K)$$

is proper. Schematically,

$$\cdots \rightarrow V_{A, \ell}^{(j)}(K) \xrightarrow{\mathcal{F}_0^{(j+1)}} V_{A, \ell}^{(j+1)}(K) \rightarrow \cdots$$

\hfill $\text{Red}_p$ \hfill $\text{Red}_p$

$$\xrightarrow{} V_{A, \ell}^{(j)}(\kappa_p) \xrightarrow{\mathcal{F}_p^{(j+1)}} V_{A, \ell}^{(j+1)}(\kappa_p) \rightarrow \cdots$$

where the broken hooked arrow indicates proper inclusion.

Hence, $p$ divides $\mathcal{F}^{(j+1)}$ at $V_{A, \ell}^{(j)}(K)$, so $p \in L'$.

4.4 Precision requirements

The subspace operations $\{\mathcal{F}^{(i)}\}_i$ in the previous section can be described easily in terms of linear algebra on Laurent series. Since $S_2(N, 1; \mathbb{Z}[\frac{1}{N}])$ and $\Lambda$ can be computed to arbitrarily high precision, for each $p \in S$, $V_{A, \ell}^{(i)}(\kappa_p)$ can be computed to precision $P$ provided that $P$ is large enough. The goal of this section is to determine exactly how large $P$ must be. These results are independent of the base field; for simplicity, we confine ourselves to working over $K$.

Recall the Sturm bound (Theorem 9.18 and Corollaries 9.19 and 9.20 in [42]):

$$\text{Sturm}_3(N) = \frac{b_1}{b_2} |S_2(\mathbb{Z}) : \Gamma_0(N)| + 1.$$

If $P \geq \text{Sturm}_3(N)$, then truncated $q$-expansion of modular forms $M_k(N, \theta; \kappa)$ is injective for any number field or finite field $\kappa$, any character $\theta : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \kappa^\times$, and any weight $k \geq 1$.

Lemma 4.4 Let $i, j \in \{0, \ldots, s\}$. If $P \geq \text{Sturm}_3(N)$ and $U_i$ and $U_j$ (as defined in Sect. 4.2) have been computed to precision $P$, then $U_i \cap U_j$ can be computed to precision $P$.\[ Springer]
Proof It is clear that we can compute the intersection of $U_i \mod (q^P)$ with $U_j \mod (q^P)$ (see Sect. 4.5), but we must verify that this is equal to $(U_i \cap U_j) \mod (q^P)$. It suffices to show that $U_i + U_j \to K(\langle q \rangle)/(q^P)$ is injective.

Suppose that $f, g \in U_i + U_j$ and that $f \equiv g \mod (q^P)$. Then $\lambda_i\lambda_j f$ and $\lambda_i\lambda_j g$ are elements of $M_3(N, \chi^{-1}; K)$ and $\lambda_i\lambda_j f \equiv \lambda_i\lambda_j g \mod (q^P)$. Since $P \geq \text{Sturm}_3(N)$, this congruence implies $\lambda_i\lambda_j f = \lambda_i\lambda_j g$, so $f = g$. \hfill \square

Lemma 4.5 If $P \geq \text{Sturm}_{\ell+3}(N)$ and a given subspace $W \subseteq V_{\Lambda}^\prime(K)$ has been computed to precision $\ell P$, then $S_{\ell}^T(W)$ can be computed to precision $\ell P$.

Proof Given a basis for $W \mod (q^P)$ we can compute the image of this basis under $T_{\ell} = T_{\ell,2}^T$ to precision $P$. Therefore, we can compute

$$\{ f \in W \mod (q^P) : T_{\ell} f \in W \mod (q^P) \}$$

to precision $q^P$ using linear algebra on formal Laurent series (see Sect. 4.5). To show that the space above is equal to $S_{0,\ell}^T(W) \mod (q^P)$ it suffices to prove that the truncated $q$-expansion map $W + T_{\ell}W \to K(\langle q \rangle)/(q^P)$ is injective.

Here we will use the $\ell$th multiplicative Hecke operator $Q_{\ell}$: $Q_{\ell}$ can be interpreted on test objects as the operator obtained by replacing the sum in (*) of Sect. 3.2 with a product and then multiplying by $\ell$. If $m$ is a classical modular form on the upper half-plane we have $(Q_{\ell}m)(\tau) = m(\ell \tau) \prod_{i=0}^{\ell-1} m(\frac{\tau+i}{\ell})$ (see also Section 3.2 of [22]). Under either interpretation, one can check that $Q_{\ell} : M_1(N, \chi^{-1}; K) \to M_{\ell+1}(N, \chi^{-(\ell+1)}; K(\zeta_\ell))$ and furthermore, if $h \in \lambda^{-1}S_2(N, 1; K)$, then $T_{\ell}h \in (Q_{\ell}\lambda)^{-1}M_{\ell+2}(N, \chi^{-\ell}; K(\zeta_\ell))$.

Now, if $f \in W + T_{\ell}W$, then $(Q_{\ell}\lambda)\lambda f \in M_{\ell+3}(N, \chi^{-(\ell+1)}; K(\zeta_\ell))$. Therefore, if $f, g \in W + T_{\ell}W$ and $f \equiv g \mod (q^P)$, the congruence $(Q_{\ell}\lambda)\lambda f \equiv (Q_{\ell}\lambda)\lambda g \mod (q^P)$ implies $(Q_{\ell}\lambda)\lambda f = (Q_{\ell}\lambda)\lambda g$ since $P \geq \text{Sturm}_{\ell+3}(N)$, whence $f = g$. \hfill \square

By induction, we obtain the following:

Lemma 4.6 If $U_0, \ldots, U_\ell$ have all been computed to precision $\ell P$ where $P \geq \text{Sturm}_{\ell+3}(N)$, then $V_{\Lambda,\ell}(K)$ can be computed to precision $\ell P$.

4.5 Constituent computations of the Hecke stability method

Let us briefly explain how the constituent computations of the HSM above are performed using computer linear algebra.

We typically express $q$-expansions as row vectors. If $A$ is a matrix with entries in a subring $O \subseteq K$ we say that a prime $p \subseteq O$ is a (left) prime divisor of $A$ if the (left) nullity of $A$ (over the field $K$) is strictly less than the nullity of the reduction of $A$ modulo $p$. If $p$ is a prime divisor of $A$, then $p$ divides the determinant of any nonsingular minor of $A$. Therefore, in practice, to compute (a list of candidates for) the prime divisors of $A$, we find two nonsingular minors $A_1$ and $A_2$, and then we factor the ideal $\gcd(\det A_1, \det A_2)$ of $O$.

Suppose that $W$ is a finite-dimensional subspace of $K(\langle q \rangle)$ where $K$ is a global field. Because there is $d$ large enough so that $q^d W \subseteq K[\langle q \rangle]$, we will assume for simplicity that $W \subseteq K[\langle q \rangle]$. Fix a basis $\{g_1, \ldots, g_r\}$ for $W$.

Table 2 summarizes the linear-algebraic computations performed by the Hecke stability method with input $W$ (represented by the chosen basis to an appropriate level of precision). In the table, $U$ is another finite-dimensional subspace of $K[\langle q \rangle]$ with basis $\{h_1, \ldots, h_u\}$, and $T$ is a $K$-linear operator on $K[\langle q \rangle]$. The subspace operations $\mathcal{T}^U$ and $\mathcal{S}^T$ were defined in Sect. 4.1.
is an isomorphism when \( p \) belongs to some work must be done to certify such a claim. \( p \in \mathbb{P} \).

Target Matrix dim’s \( j \)th Entry of matrix Computed from matrix 

| Primes of bad reduction for \( W \) | \( r \times P \) | \( j \)th coefficient of \( g_i \) | \( \subseteq \) Prime divisors of \( A \) |
| \( T^U_p(W) \) | \( (r + u) \times P \) | \( j \)th coeff. of \( i \)th entry of \( (g_1, \ldots, g_r, h_1, \ldots, h_u) \) | \( \text{isomorphism } l.\ker(A) \rightarrow \) target \( (v_1, \ldots, v_{r+u}) \) \( \mapsto \sum_{i=1}^r v_i g_i \) |
| Divisors of \( T^U \) at \( W \) | \( (r + u) \times P \) | \( j \)th coeff. of \( i \)th entry of \( (g_1, \ldots, g_r, h_1, \ldots, h_u) \) | \( \subseteq \) Prime divisors of \( A \) |
| \( S_2^U(W) \) | \( 2r \times P \) | \( j \)th coeff. of \( i \)th entry of \( (g_1, \ldots, g_r, Tg_1, \ldots, Tg_r) \) | \( \text{Isomorphism } l.\ker(A) \rightarrow \) target \( (v_1, \ldots, v_{2r}) \) \( \mapsto \sum_{i=1}^r v_{i+r} g_i \) |
| Divisors of \( S^T \) at \( W \) | \( 2r \times P \) | \( j \)th coeff. of \( i \)th entry of \( (g_1, \ldots, g_r, Tg_1, \ldots, Tg_r) \) | \( \subseteq \) Prime divisors of \( A \) |

In the first row of Table 2, \( P \) is taken large enough so that the matrix has row rank \( r \). Elsewhere, \( P \) is taken to be large enough so that the given map from the kernel to the target is an isomorphism when \( p = 0 \).

### 4.6 Certification of Hecke stability hypotheses, examples and remarks

Given input \((N, \chi, \Lambda, \ell)\) to the Hecke stability method as outlined above, we have for each \( p \in S \text{ a Hecke stability hypothesis: the proposition } "V'(\kappa_p) \subseteq M_1(N, \chi; \kappa_p)." \) The truth of the Hecke stability hypothesis at \( p = 0 \) is guaranteed by (i.) of Theorem 2.3, but for nonzero \( p \) some work must be done to certify such a claim.

Here are four methods for certifying a Hecke stability hypothesis:

a. If the space \( V'(\kappa_p) \) is equal to \( \text{Red}_p V'_{A,\ell}(K) \), then reduction \( S_1(N, \chi; \mathcal{O}_p) \rightarrow S_1(N, \chi; \kappa_p) \) is surjective and the inclusion \( V'(\kappa_p) \subseteq M_1(N, \chi; \kappa_p) \) holds automatically.

b. If one can prove that condition (ii.) or condition (iii.) of Theorem 2.3 holds with \( F = \kappa_p \), then \( V'(\kappa_p) = V'_{A,\ell}(\kappa_p) \subseteq M_1(N, \chi; \kappa_p) \).

c. If one has detailed knowledge of \( Z(\Lambda) \) in advance, more specific arguments using polar conditions on isogeny graphs can be used to prove Hecke stability hypotheses (see Example 4.8 and Remark 4.10 below).

d. We have \( V'(\kappa_p) \subseteq M_1(N, \chi; \kappa_p) \) if for some \( k \geq 2 \) and every \( f \in V'(\kappa_p) \) we have \( f^k \in M_k(N, \chi^k; \kappa_p) \). Because this containment condition is “non-linear” it can be used to certify Hecke stability hypotheses (by checking the condition on a basis for \( V'(\kappa_p) \)) but it cannot be used directly to compute \( M_1(N, \chi; \kappa_p) \). This is an especially convenient certification method when \( \chi^2 = 1 \), since the HSM requires that we compute a basis for \( S_2(N, \mathbf{1}; \kappa_p) \).

Remark 4.7 For the second and third methods above, it is useful to have some method of computing the zeros of a modular form \( \lambda \in M_1(N, \chi^{-1}; \kappa) \) with an aim towards counting its supersingular zeros. There are several ways to do this, and we outline just one below.
The principal challenge is computing the polynomial

\[ J_\lambda(X) = \prod_{\lambda(\tau) = 0} (X - j(\tau))^{\text{ord}_r(\lambda)}. \]

Suppose that we know the \( q \)-expansion of the normalized image \( \lambda^w \) of \( \lambda \) under the full-level Atkin–Lehner involution (if \( \lambda \) is an Eisenstein series this is easy); because the nebentypus of \( \lambda^w \) is inverse to that of \( \lambda, \lambda^w \) is a weight 2 modular form for \( \Gamma_0(N) \). Consider the modular ratio

\[ H_\lambda(X) = \frac{(12G_4)^3 - (G_3^3 - G_6^2)X}{\lambda^w} \]

of weight 10 for \( \Gamma_0(N) \) over the polynomial ring \( \kappa[X] \) (here \( G_k \) is the normalized weight \( k \) Eisenstein series for \( \text{SL}_2(\mathbb{Z}) \)). Note that for almost all values of \( \alpha \in \kappa \), the negative part of \( \text{div} \, H_\lambda(\alpha) = -\text{div}(\lambda^w) \). However, if \( (\lambda^w(\tau)) = 0 \), then the numerator of \( H_\lambda(X) \) vanishes at \( X = j(\tau) \) so the negative part of \( \text{div} \, H_\lambda(j(\tau)) \) is at least \( -\text{div}(\lambda^w) + [\tau] \).

Now, for even \( k \) let \( M_k = M_k(N, 1; \kappa) \). If \( k \geq 4 \), then for any \( \tau' \) we have

\[ \dim\{ g \in M_k : \text{div} \, g \geq \text{div}(\lambda^w) - [\tau'] \} > \dim\{ g \in M_k : \text{div} \, g \geq \text{div}(\lambda^w) \}. \]

The right hand side is the generic dimension of \( H_\lambda(\alpha)M_k \cap M_{k+1} \) as \( \alpha \) ranges over \( \kappa \), while the left hand side is a lower bound on the dimension of \( H_\lambda(j(\tau))M_k \cap M_{k+1} \) when \( \tau \in \mathbb{Z}(\lambda^w) \). In the language of Sect. 4.3, determining \( J_{\lambda,\kappa}(N) = J_\lambda(N)J_{\lambda,\kappa}(X) \) reduces to finding the prime ideals of \( \kappa[X] \) that divide the intersection operator \( I_{H_\lambda(N)}M_k \) at \( M_{k+1} \).

If \( \kappa \) is a finite field, we can find these divisors by taking determinants of a matrix with entries in \( \kappa[X] \) using polynomial interpolation. When \( \kappa \) is a number field, one can perform polynomial interpolation over several residue fields and then reconstruct \( J_{\lambda,\kappa}(X) \) using the Chinese remainder theorem.

This concludes the proof of Theorem 2.5. \( \square \)

Example 4.8 Let \( N \geq 1 \) and let \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times \) be a character of conductor \( M \) where \( gX_0(M) = 0 \). In this case, by taking oldforms of type \( (M, \chi^{-1}) \), we may choose \( \Lambda \subseteq M_1(N, \chi^{-1}; K) \) such that \( Z(\Lambda) \) contains only elliptic points. To prove that \( V'_{\Lambda, \ell}(\kappa_p) \subseteq M_1(N, \chi; \kappa_p) \) for a fixed nonzero prime \( p \), it suffices to prove that there is no polar condition \( P \) on \( G_\ell(\text{SL}_2(\mathbb{Z}; \kappa_p) \) satisfying \( P \subseteq W_1 \).

For concreteness, suppose that either \( M = 3 \) or \( M = 7 \) so that \( j\mathbb{Z}(\Lambda) = \{0\} \). Let \( N \) be odd and divisible by \( M \). We have \( \Phi_2(0, Y) = (Y - 54000)^3 \) and

\[ \Phi_2(54000, Y) = Y(Y^2 - 2835810000Y + 6549518250000) \]

where \( \Phi_2(X, Y) \) is the second modular polynomial. When \( p \mid 6549518250000 = 2^4 \cdot 3^9 \cdot 5^6 \cdot 11^3 \), there is a unique 2-isogeny from the elliptic curve \( E' \) with \( j \)-invariant 54000 (mod \( p \)) to the elliptic curve \( E \) with \( j \)-invariant 0 (mod \( p \)). For such \( p \), any polar condition on \( G_\ell(\Gamma(1); \overline{\kappa}_p) \) that contains the vertex \( [E] \) must also contain the vertex \( [E'] \) (which is distinct from \( [E] \) in this situation because \( p \nmid 2, 3, 5 \)). Since \( \delta_{\ell,1}(\mathbb{Z}(\Lambda)) = \{[E]\} \), it follows that \( V'_{\Lambda, \ell}(\kappa_p) \subseteq M_1(N, \chi; \kappa_p) \) as long as \( p \nmid \mathbb{Z} \notin \{2, 3, 5, 11\} \).

In fact, we have proven that \( \{ f \in V'_{\Lambda}(\kappa_p) : T_2f \in V'_{\Lambda}(\kappa_p) \} \subseteq M_1(N, \chi; \kappa_p) \).

Example 4.9 Let \( (N, \chi) = (651, e) \) where \( e \) is the quadratic character of level 651 and conductor 31. Applying the Hecke stability method in characteristic zero with \( \Lambda = \{\lambda\} \) where
\[ \lambda(q) = 3 + 2 \sum_{n=1}^{\infty} \sum_{d|n} \left( \frac{d}{31} \right) q^n \]

proves that \( S_1(651, \varepsilon; \mathbb{Q}) \) is trivial. However, the methods of Sect. 4.3 indicate that mod 337 reduction \( S_1(651, \varepsilon; \mathbb{Z}[\frac{1}{651}]) \rightarrow S_1(651, \varepsilon; \mathbb{F}_{337}) \) may not be surjective. Indeed, \( V'_{A,2}(\mathbb{F}_{337}) \) is 2-dimensional. We can verify the Hecke stability hypothesis \( V'_{A,2}(\mathbb{F}_{337}) \subseteq M_1(N, \varepsilon; \mathbb{F}_{337}) \) in three ways:

- Using the method of Remark 4.7, we find that \( \lambda(\tau) = 0 \) only if \( j(\tau) \) is a root of
  \[ 332X^3 + 394086965048982896640X^2 + 23574729187315780314726400X, \]
  which factors as \( 2X(X - 96)(X - 241) \) when reduced modulo 337. The \( j \)-invariants 0, 96, and 241 are all ordinary over \( \mathbb{F}_{337} \), so the Hecke stability hypothesis holds by condition (ii.) of Theorem 2.3.

- Applying (iii.) of Theorem 2.3 with \( M = 31, \ell = 2, \) and \( r = 2 \). Here, the inequality \( 337 > \max(\frac{1024}{31}, 64) = 64 \) guarantees that any polar condition on \( G_2(I_0(31); \mathbb{F}_{337}) \) contains at least 3 non-elliptic vertices, but \( gX_0(31) = 2 \), so \( \lambda \) has at most 2 non-elliptic zeros on \( X_0(31) \). Therefore, \( Z(\Lambda) \) cannot contain a polar condition, so elements of \( V'_{A,2}(\mathbb{F}_{337}) \) must be modular forms.

- Let \( \{f_1, f_2\} \) be a basis for \( V'_{A,2}(\mathbb{F}_{337}) \). To check the Hecke stability hypothesis, it is enough to verify that \( f_1^2, f_2^2 \in M_2(651, 1; \mathbb{F}_{337}) \), and this is the case.

Using any of these methods, we find that \( \dim S_1(651, \varepsilon; \mathbb{F}_{337}) = 2 \). The discrepancy in dimensions between this space over \( \mathbb{Q} \) and \( \mathbb{F}_{337} \) indicates the existence of nontrivial 337-torsion in the cohomology \( H^1(X_1(651), \omega(-\text{cusps})) \).

Remark 4.10 Though we will not go into the details, some improvements to the bounds in (iii.) of Theorem 2.3 can be formulated using the Goren–Lauter lemma when \( \delta_{N,M}Z(\Lambda) \) is known to consist of CM points on \( X_0(M)(\mathbb{Q}) \).

It is also worth mentioning that if \( \lambda \) vanishes at some \( \tau \in X_1(N)(\mathbb{Q}) \) with non-CM \( j(\tau) \) (for example when \( j(\tau) \) is non-integral), \( j(\tau) \) has a sparse set of primes of supersingular reduction [39].

Remark 4.11 The author has so far encountered only one family of false Hecke stability hypotheses: If \( \varepsilon \) is the quadratic character of conductor 11 and \( \lambda \) is the unique normalized weight 1 Eisenstein series of type \((11, \varepsilon)\), then \( S_1(11, \varepsilon; \mathbb{F}_7) \) is trivial, but

\[ \dim_{\mathbb{F}_7} V'_{[\lambda],\ell}(\mathbb{F}_7) = 1 \]

for \( \ell \in \{5, 59, \ldots\} \). Note that in this case, the zeros of \( \lambda \)—which lie over \( j = -32^3 \), the \( j \)-invariant of the elliptic curve \( \mathbb{C}/\mathbb{Z}[\frac{1+\sqrt{-11}}{2}] \)—are supersingular, and the inequalities of (iii.) in Theorem 2.3 do not hold.

4.7 An informal discussion of complexity

We refrain from a detailed account of the complexity of the Hecke stability method, since its complexity depends on the efficiency of other algorithms already in place.

- The HSM requires that we compute a basis for \( S_2(N, 1; \mathbb{Z}[\frac{1}{N}]) \) to high precision: For fixed \( \ell \) (which can be assumed to be the smallest prime not dividing \( N \)) Lemma 4.6 requires that we compute a basis for the weight 2 cusp forms to precision \( \ell \text{ Sturm}_{\ell+2}(N) \), which is on the order of \( \ell^2 N \).
The complexity of computing this space using modular symbols is polynomial in $\ell^2 N$, with order perhaps $O(N^{4+\epsilon})$ when $\ell$ is fixed; a precise reference for this complexity is difficult to find.

When $N$ is squarefree, there is an algorithm for computing the action of $T_2$ on $S_2(N, 1; \mathbb{Z}[\frac{1}{N}])$ that (conditionally on GRH) has a running time that is polynomial in $N$ and $\log n$ (see [5] and [18]). Implementing this algorithm could attenuate the effect that precision has on the overall complexity of the HSM.

- Implementing the algorithm of Theorem 2.5 requires that we evaluate the determinants of large matrices over a number field $K$ where $[K : \mathbb{Q}] = \varphi(\text{ord} \chi)$. Fast algorithms for computing the determinant of an $r \times r$ matrix require about $O(r^3)$ field operations (e.g., Gaussian elimination), but over a number field, these operations are essentially operations on polynomials of degree $[K : \mathbb{Q}] - 1$. The time and memory requirements for the naive adaptation of these methods to $K$ scale poorly as the degree increases.

Some computational tricks using the Chinese remainder theorem and the theory of cyclotomic fields yield noticeable improvements to computing such determinants in practice.

- Once the determinants of the matrices above are computed, we compute their GCD $a$ and then factor $a$ to determine candidates for nonsurjectivity (see Sect. 4.5). Without an estimate for the size of $a$, it is not clear how difficult this factorization problem is, but it is a necessary step if one wants to completely characterize weight 1 forms of a given type. Our data suggest that $N(a)$ grows quickly in the index of $\Gamma_0(N)$ (see Sect. 5.1).

### 5 Products of the Hecke stability method

The Hecke stability method provides us with a systematic way of computing tables of weight 1 modular forms. Because of the correspondence between mod $p$ modular forms and Galois representations with controlled ramification, these data are relevant to the refined inverse Galois problem for $\text{PXL}_2(\mathbb{F}_q)$. In what follows we comment on some of our more remarkable findings.

All tables produced by the Hecke stability method are currently being integrated into “The L-functions and modular forms database” (LMFDB). The known data are also available by request, and some tables are also provided in [36].

#### 5.1 Growth of torsion in $H^1(X_1(N), \omega(−\text{cusps}))$

Extensive computations with the Hecke stability method have produced evidence that the torsion subgroup of $H^1(X_1(N), \omega(−\text{cusps}))$ grows at least exponentially in the index of $\Gamma_1(N)$.

**Conjecture 5.1** The limit

$$\liminf_{N \to \infty} \left( \frac{\log |H^1(X_1(N), \omega(−\text{cusps}))_{\text{tors}}|}{[\text{SL}_2(\mathbb{Z}) : \Gamma_1(N)]} \right)$$

is positive.

Similar conjectures on the growth of torsion (co)homology in other situations have been made in the literature (e.g., [1] and [7]), and further evidence and results in these directions have accumulated recently (e.g., [30], [32], [33], and [37]).

The most coherent set of data relevant to our particular conjecture above is given by the contributions to torsion from $S_1(N, \varepsilon; \mathbb{F}_p)$ where $N = 3 \nu$ for a prime $\nu$ and $\varepsilon$ is the quadratic
character of conductor 3. These data are relatively easy to obtain because the forms are defined over \( \mathbb{Z} \), one can take \( s = 1 \) and \( t = 1 \) (as defined in Sect. 4.2), and the relevant Hecke stability hypotheses over \( F \) require no extra certification step when \( \text{char}(F) \not\in \{2, 3, 5, 11\} \) (see Example 4.8).

For \( N \) divisible by 3, set
\[
\tau'(N, \varepsilon) = \prod_{p | N\varphi(N)} p^{\dim \mathbf{S}_1(N, \varepsilon; \mathbb{F}_p) - \dim \mathbf{S}_1(N, \varepsilon; \mathbb{Q})}.
\]

The exclusion of primes dividing \( \varphi(N) \) guarantees that when
\[
\dim_{\mathbb{F}_p} \mathbf{S}_1(N, \varepsilon; \mathbb{F}_p) > \dim_{\mathbb{Q}} \mathbf{S}_1(N, \varepsilon; \mathbb{Q})
\]
there exists a Hecke eigenform \( f \in \mathbf{S}_1(N, \varepsilon; \mathbb{F}_p) \) such that \( a_1(f) = 1 \) and \( f \) does not lift to an element of \( \mathbf{S}_1(N, \varepsilon; \mathbb{Q}) \) (note that Hecke modules over fields of characteristics dividing \( \varphi(N) \) do not always admit bases consisting of Hecke eigenforms). Because the primes dividing \( \tau'(N, \varepsilon) \) grow precipitously, excluding these small primes does not affect the magnitude of \( \tau'(N, \varepsilon) \) very much.

Table 3 gives the values of \( \tau'(N, \varepsilon) \) where \( N = 3\nu \) and \( \nu \) ranges over all primes in \([47, 600]\). There are three such levels where \( \tau'(N, \varepsilon) = 1 \), namely 177, 183, and 201—the table skips these levels. For every level in Table 3, \( \mathbf{S}_1(N, \varepsilon; \mathbb{Q}) \) is trivial. In Fig. 2 we plot \( \log \tau'(N, \varepsilon)/[\text{SL}_2(\mathbb{Z}) : F_0(N)] \) for the same levels; this is the analog of the quantity in Conjecture 5.1 for the contribution from forms of a fixed nebentypus.

Finally, it should be mentioned that the Hecke stability hypotheses over \( \mathbb{F}_5 \) and \( \mathbb{F}_{11} \) were certified using method (d.) of Sect. 4.6 (all other Hecke stability hypotheses follow from the argument in Example 4.8).

The reader may observe that the values of \( \tau'(N, \varepsilon) \) in Table 3 are always square. This is because the fixed points of the Atkin–Lehner involution on \( \mathbf{S}_1(N, \varepsilon; \mathbb{F}_p) \) are precisely the dihedral eigenforms of type \( (N, \varepsilon) \) and such forms always lift to characteristic zero (in the same level and character) \([45]\), so \( \dim \mathbf{S}_1(N, \varepsilon; \mathbb{F}_p) - \dim \mathbf{S}_1(N, \varepsilon; \mathbb{Q}) \) is always even. This argument generalizes:

**Theorem 5.2** If \( \chi \) is a quadratic character of level \( N \) and \( p \nmid \varphi(N) \), then
\[
\dim_{\mathbb{F}_p} \mathbf{S}_1(N, \chi; \mathbb{F}_p) \equiv \dim_{\mathbb{Q}} \mathbf{S}_1(N, \chi; \mathbb{Q}) \mod 2.
\]

**Remark 5.3** A qualitative phenomenon observed over larger sets of data seem to indicate that classical newforms (over \( \mathbb{Q} \)) and mod \( p \) eigenforms that do not lift to characteristic zero tend to repel each other (in the same level and character). That is, when the dimension of \( \mathbf{S}_1(N, \chi; \mathbb{Q}) \) is positive, the contribution to \( H^1(X_1(N), \omega(-\text{cusps}))_{\text{tors}} \) from forms with character \( \chi \) tends to be trivial provided that \( N \) is small.

As pointed out to the author by Frank Calegari, \([6]\) predicts that this tendency will fail as \( N \) grows. Indeed, if \( N = 1999 \) and \( \chi \) is the mod \( N \) quadratic character, we computed \( \dim \mathbf{S}_1(N, \chi, \mathbb{Q}) = 13 \) and \( \dim \mathbf{S}_1(N, \chi, \mathbb{Q}) = 15 \).

### 5.2 Galois number fields with small root discriminant

Recall that when \( K \) is a number field, the quantity \( \text{rd}(K) = |\text{disc}(K)|^{1/[K: \mathbb{Q}]} \) is the root discriminant of \( K \). Under the generalized Riemann hypothesis,
\[
\lim_{[K : \mathbb{Q}] \to \infty} \inf \{ \text{rd}(K) : K/\mathbb{Q} \} = 8\pi e^{\gamma} \approx 44.76323.
\]

\( \mathfrak{S} \) Springer
Table 3  Torsion associated to mod 3 quadratic nebentypus

| $N$ | $t'(N, \varepsilon)$ | $N$ | $t'(N, \varepsilon)$ |
|-----|-----------------|-----|-----------------|
| 141 | $5^2$           | 933 | $23^2 \cdot 11177^2 \cdot 2036539^2$ |
| 159 | $5^2$           | 939 | $11643684611137^2$ |
| 213 | $17^2$          | 951 | $13^2 \cdot 593^2 \cdot 1427^2 \cdot 136363^2$ |
| 219 | $41^2$          | 993 | $1399^2 \cdot 5767763143^2$ |
| 237 | $5^2$           | 1011| $47^2 \cdot 587^2 \cdot 6004682531^2$ |
| 249 | $89^2$          | 1041| $5^2 \cdot 297255711552329^2$ |
| 267 | $41^2$          | 1047| $5684921432074812^2$ |
| 291 | $73^2$          | 1059| $293^2 \cdot 411688918531337^2$ |
| 303 | $199^2$         | 1077| $61^2 \cdot 1097549^2 \cdot 17174569^2$ |
| 309 | $11^2$          | 1101| $33377^2 \cdot 167296128361^2$ |
| 321 | $73^2$          | 1119| $7^2 \cdot 13^2 \cdot 101^2 \cdot 1567^2 \cdot 30449^2 \cdot 75629^2$ |
| 327 | $281^2$         | 1137| $5^2 \cdot 11^2 \cdot 1811^2 \cdot 7757^2 \cdot 1883500559^2$ |
| 339 | $11801^2$       | 1149| $17^2 \cdot 587^2 \cdot 7459050493709^2$ |
| 381 | $13^2$          | 1167| $19^2 \cdot 4353193^2 \cdot 27646401661^2$ |
| 393 | $7^2 \cdot 1669^2$| 1191| $23^2 \cdot 8219^2 \cdot 264610601669^2$ |
| 411 | $223^2 \cdot 613^2$| 1203| $17^2 \cdot 56675^2 \cdot 83439102139^2$ |
| 417 | $37^2 \cdot 227^2$| 1227| $5^2 \cdot 17^6 \cdot 23^2 \cdot 4501099^2 \cdot 106521127^2$ |
| 447 | $353^2 \cdot 937^2$| 1257| $90379^2 \cdot 6166483^2 \cdot 27175307^2$ |
| 453 | $2417^2$        | 1263| $11^4 \cdot 167^4 \cdot 3359^2 \cdot 589072513^2$ |
| 471 | $4523^2$        | 1293| $67^2 \cdot 1921529195814127^2$ |
| 489 | $11^2 \cdot 463^2$| 1299| $17^2 \cdot 116866832706907338779^2$ |
| 501 | $191^2 \cdot 859^2$| 1317| $5^2 \cdot 66025499784624707^2$ |
| 519 | $257^2 \cdot 523^2$| 1329| $2316157573^2 \cdot 743496822373^2$ |
| 537 | $5^2 \cdot 97^2 \cdot 8713^2$| 1347| $2311^2 \cdot 6717077^2 \cdot 1707229020033067^2$ |
| 543 | $67^2 \cdot 193^2$| 1371| $227^2 \cdot 751^2 \cdot 45599^2 \cdot 1224778807207^2$ |
| 573 | $59^2 \cdot 397^2 \cdot 439^2$| 1383| $47^2 \cdot 3108109^2 \cdot 8284637^2 \cdot 12903830^2$ |
| 579 | $67^2 \cdot 1573^2$| 1389| $23^3 \cdot 7116615393905984791^2$ |
| 591 | $29^2 \cdot 444151^2$| 1401| $5^2 \cdot 857030122343348247418273^2$ |
| 597 | $19^2 \cdot 62617^2$| 1437| $7^2 \cdot 20753^2 \cdot 3413228933067061^2$ |
| 633 | $451933^2$      | 1461| $1561303^2 \cdot 68396038855089373^2$ |
| 669 | $11489^2 \cdot 48883^2$| 1473| $113^2 \cdot 525503753^2 \cdot 91045960949^2$ |
| 681 | $163316303^2$   | 1497| $347095820483556600660647^2$ |
| 687 | $1140121^2$     | 1509| $1259^2 \cdot 7689582211^2 \cdot 18300110183^2$ |
| 699 | $41^2 \cdot 89^2 \cdot 223^2 \cdot 1109^2$| 1527| $11^2 \cdot 732709^2 \cdot 296442544991039301013^2$ |
| 717 | $619^2 \cdot 26921^2$| 1563| $139^2 \cdot 132467773^2 \cdot 189430903^2 \cdot 2365816319^2$ |
| 723 | $770297621^2$   | 1569| $53^2 \cdot 6219652614813901269147^2$ |
| 753 | $23741^2 \cdot 13669147^2$| 1623| $19^2 \cdot 142802913789809452984252^2$ |
| 771 | $97^2 \cdot 3833^2 \cdot 11383^2$| 1641| $53^2 \cdot 73^2 \cdot 1489^2 \cdot 8052073^2 \cdot 36978604703^2$ |
| 789 | $23^2 \cdot 101879593^2$| 1671| $7^4 \cdot 71^2 \cdot 2198029^2 \cdot 5826349757405731^2$ |
Table 3 continued

|  |  |
|---|---|
| \(N\) | \(t'(N, \varepsilon)\) |
| 807 | \(20983^2 \cdot 887059^2\) |
| 813 | \(53^2 \cdot 71^2 \cdot 51803^2\) |
| 831 | \(13^2 \cdot 59^2 \cdot 79^2 \cdot 311603^2\) |
| 843 | \(709^2 \cdot 1471^2 \cdot 165606751^2\) |
| 849 | \(421^2 \cdot 4325322613^2\) |
| 879 | \(19^2 \cdot 139^2 \cdot 13339^2\) |
| 921 | \(166017730847^2\) |
| 1689 | \(11^2 \cdot 68581518742288026772115454991^2\) |
| 1707 | \(5^2 \cdot 277^2 \cdot 154664726857^2 \cdot 1697802067421853871^2\) |
| 1713 | \(5^2 \cdot 107^2 \cdot 70663^2 \cdot 101011208101^2 \cdot 127452545273^2\) |
| 1731 | \(31^2 \cdot 433^2 \cdot 19159873^2 \cdot 36001051344486600557^2\) |
| 1761 | \(5^2 \cdot 11^2 \cdot 521393^2 \cdot 121756570064236471668019^2\) |
| 1779 | \(1104047325433567^2 \cdot 615184180444752239^2\) |
| 1797 | \(5^2 \cdot 11^2 \cdot 755809^2 \cdot 14302275115816198137271^2\) |

Fig. 2 Growth of torsion

The constant \(8\pi e^\gamma\) is sometimes referred to as the Odlyzko–Serre bound [40].

Let \(\mathcal{E}(G)\) be the set of all Galois number fields \(K \subset \mathbb{C}\) such that \(\text{rd}(K) \leq 8\pi e^\gamma\) and \(\text{Gal}(K/\mathbb{Q}) \simeq G\). It is a natural problem to determine each of the finite sets \(\mathcal{E}(G)\).

- Jones and Roberts have shown that \(|\bigcup_{A \in \mathcal{A}} \mathcal{E}(A)| = 7063\). This led them to conjecture that the set \(\bigcup_{G} \mathcal{E}(G)\) is in fact finite [23].
- In her thesis [44], Wallington developed algorithms for analyzing \(\mathcal{E}(G)\) with \(G \leq S_6\). Subsequently, Jones and Wallington characterized \(\mathcal{E}(G)\) for all solvable transitive \(G \leq S_n\) with \(n \leq 10\), all groups \(G\) of order \(\leq 24\), and all dihedral groups of prime degree [25].
- Many nonsolvable \(K\) with \(\text{rd}(K) \leq 8\pi e^\gamma\) were found in [23]; since then, new nonsolvable fields with low root discriminant have been discovered at a rate of about two per year [34] (see [24], Table 9.1).

Suppose that \(f\) is a Hecke eigenform in \(S_1(N, \chi; \bar{\mathbb{F}}_p)\) where \(N\) is squarefree and \(\chi\) is quadratic of conductor \(f\), and let \(K_f\) be the number field constructed from the Galois representation associated to \(f\). In this case,
This formula can be obtained following the computation in Section 2 of [23] remembering that $K_f$ is unramified at $p$, ramification is tame at all $v \mid N$ (because $N$ is squarefree), and the contribution to the root discriminant at $v \mid f$ is $v^{1/2}$ (because $\chi$ is quadratic). Bearing this formula in mind, the tables of weight 1 modular forms mod $p$ produced by the Hecke stability method (see Appendix A of [36]) reveal six new examples of $PXL_2(\mathbb{F}_7)$- and $PXL_2(\mathbb{F}_{11})$-extensions of $\mathbb{Q}$ with root discriminant $\leq 8\pi e^\nu$ listed in Table 4.

In Table 4, $d$ is the discriminant of the quadratic subfield and the polynomials are given as coefficient lists (with leading coefficient first)—the polynomials were computed by Roberts [35]. The corresponding number fields have also been recorded in the Number Fields database [24].

### 5.3 Nonsolvable Galois number fields ramified at a single prime

For a finite group $G$ and a set $S$ of rational primes, let $\mathcal{K}(G, S)$ be the set of $G$-extensions of $\mathbb{Q}$ unramified at primes outside of $S$.

In the 1970s, Serre proved a “large image theorem” for the mod $p$ Galois representations attached to level 1 eigenforms. As a corollary, he showed that for every prime $v \geq 11$ there is a nonsolvable group $G$ such that $\mathcal{K}(G, \{v\})$ is nonempty. That is, for every prime $v \geq 11$ there is a nonsolvable number field ramified only at $v$.

Gross observed in the 1990s that there were no known number fields with this property for $v \leq 7$. Examples were subsequently found by Dembélé for $v = 2$ [9] (using Hilbert modular forms), Dembélé–Greenberg–Voight for $v = 3, 5$ [10] (using Hilbert modular forms), and Dieulefait for $v = 7$ [15] (using Siegel modular forms).

We can give a novel solution to Gross’ problem using weight 1 modular forms over $\overline{\mathbb{F}}_p$.

Table 5 summarizes our solution: Using the HSM we found for each level $N$ in the table an eigenform $f \in S_1(N, \chi; \overline{\mathbb{F}}_p)$ such that the number field $K_f/\mathbb{Q}$ is ramified only at the single prime $v \mid N$ and such that $\text{Gal}(K_f/\mathbb{Q}) \cong G$.

| $v$ | $N$ | $p$ | $\text{ord}(\chi)$ | $\chi(g)$ | $G$ |
|-----|-----|-----|---------------------|-----------|-----|
| 2   | 256 | 374377637683781311 | 64        | *244174677499476933 | $\text{PGL}_2(\mathbb{F}_p)$ |
| 3   | 243 | 44056205122990214764331 | 162       | *2893275249056947848386 | $\text{PSL}_2(\mathbb{F}_p)$ |
| 5   | 125 | 199         | 100       | *79                    | $\text{PSL}_2(\mathbb{F}_p)$ |
| 7   | 343 | 74873         | 98        | 16423                 | $\text{PGL}_2(\mathbb{F}_p)$ |
The $\chi(g)$ column in Table 5 is meant to provide enough information to retrieve the (odd) nebentypus $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ for each of these forms: In the first row, $g = 5$ (determining the character up to parity), and in all other rows, $g$ is the least primitive root for $\mathbb{Z}/N\mathbb{Z}$. An entry of the form $a$ means that $\chi(g) = a$, and an entry of the form $\ast a$ means that $\chi(g)$ is an element of $\overline{\mathbb{F}}_p^2$ whose trace is equal to $a$ and whose norm is 1.

The corresponding Hecke stability hypotheses can all be certified using condition (ii.) or (iii.) of Theorem 2.3. In each case, we took $\Lambda = \{\lambda\chi - 1\}$ where $\lambda\chi - 1$ is the unique normalized weight 1 Eisenstein series of character $\chi^{-1}$ and we took $\ell$ to be the least prime not dividing $N$.

- When $N = 256, 243$ the elementary bound $|\delta_{N,N}Z(\lambda\chi^{-1})| \leq gX_0(N)$ suffices to apply condition (iii.) of Theorem 2.3 since $p$ is rather large compared to $N$ in these cases.
- For $N = 125, 343$, the set $\delta_{N,1}Z(\lambda\chi^{-1})$ was computed directly using the method of Remark 4.7 over $\overline{\mathbb{F}}_p$; in both cases, $\lambda\chi^{-1}$ was found to have no supersingular non-elliptic zeros.

Once eigenforms of these types were computed to sufficient precision, the Galois groups $G$ were identified in a manner similar to that found in [4].

Acknowledgments The author would like to thank Akshay Venkatesh, John Voight, Kevin Buzzard, Frank Calegari, Dave Roberts, Chandrashekhar Khare, and Haruzo Hida for their input and support. The author would also like to thank the anonymous referee for their helpful comments and suggestions.

References

1. Bergeron, N., Venkatesh, A.: The asymptotic growth of torsion homology for arithmetic groups. J. Inst. Math. Jussieu 12, 391–447 (2012)
2. Bröker, R., Lauter, K., Sutherland, A.V.: Modular polynomials via isogeny volcanoes. Math. Comp. 81, 1201–1231 (2012)
3. Buhler, J.P.: Icosahedral Galois Representations. Springer, Berlin (1978)
4. Buzzard, K.: Computing weight one modular forms over $\mathbb{C}$ and $\overline{\mathbb{F}}_p$. In: Böckle, G., Wiese, G. (eds.) Proceedings of the Summer School and Conference, “Computations with Modular Forms,” pp. 129–146. Springer, Heidelberg (2012)
5. Bruin, P.J.: Modular Curves, Arakelov Theory, Algorithmic Applications. Ph.D. Thesis, University of Leiden (2010)
6. Calegari, F., Geraghty, D.: Modularity Lifting Beyond the Taylor-Wiles Method. arXiv:1207.4224 and arXiv:1209.6293. Preprint (2012)
7. Calegari, F., Venkatesh, A.: Towards a Torsion Jacquet-Langlands Correspondence. arXiv:1212.3847. Preprint (2012)
8. Coleman, R., Voloch, J.-F.: Companion forms and Kodaira-Spencer theory. Invent. Math. 110, 263–328 (1992)
9. Dembélé, L.: A non-solvable Galois extension of ramified at 2 only. Comptes Rendus Math. 347, 111–116 (2008)
10. Dembélé, L., Greenberg, M., Voight, J.: Nonsolvable number fields ramified only at 3 and 5. Comp. Math. 147, 716–734 (2011)
11. Deligne, P.: Formes modulaires et représentations $\ell$-adiques. Sem. Bourbaki 355, 136–172 (1968)
12. Deligne, P., Serre, J.-P.: Formes modulaires de poids 1. Annales Scientifiques de l’É.N.S., 4e série 7, 507–530 (1974)
13. Diamond, F., Shurman, J.M.: A First Course in Modular Forms. Springer, Heidelberg (2005)
14. Dicksan, L.E.: Linear Groups, with an Exposition of the Galois Field Theory. Teubner, Leipzig (1901)
15. Dieulefait, L.V.: A non-solvable extension of $\mathbb{Q}$ unramified outside 7. Compos. Math. 148, 669–674 (2012)
16. Edixhoven, B.: “Serre’s Conjectures” in Modular Forms and Fermat’s Last Theorem. Springer, Heidelberg (1997)
17. Edixhoven, B.: Comparison on integral structures of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. With appendices by Jean-François Mestre and Gabor Wiese. J. Inst. Math. Jussieu 5, 1–34 (2006)
18. Edixhoven, B., Couveignes, J.-M. (eds.): Computational Aspects of Modular Forms and Galois Representations. Princeton University Press, Princeton (2011)
19. Goren, E.Z.: Lectures on Hilbert Modular Varieties and Modular Forms. Centre de Recherches Mathématiques, Montreal (2002)
20. Frey, G. (ed.): On Artin’s Conjecture for Odd 2-dimensional Representations. Springer, Berlin (1994)
21. Goren, E.Z., Lauter, K.E.: Class invariants for quartic CM fields. Annales de l’Institut Fourier 57, 457–480 (2007)
22. Heim, B., Murase, A.: Borcherds lifts on $\text{Sp}_2(\mathbb{Z})$. In: Yoshinori, H., Ichikawa, T., Murase, A., Sugano, T. (eds.) Geometry and Analysis of Automorphic forms, pp. 56–76. World Scientific Publishing Co., Singapore (2009)
23. Jones, J.W., Roberts, D.P.: Galois number fields with small root discriminant. J. Number Theory 122, 379–409 (2007)
24. Jones, J.W., Roberts, D.P.: A database of number fields. LMS J. Comput. Math. 17, 595–618 (2014)
25. Jones, J.W., Wallington, R.Q.: Number fields with solvable Galois groups and small Galois root discriminants. Math. Comput. 81, 555–567 (2012)
26. Katz, N.M.: $p$-Adic Properties of Modular Schemes and Modular Forms. International Summer School on Modular Forms, Antwerp (1972)
27. Khare, C.: Serre’s modularity conjecture: the level one case. Duke Math. J. 134, 557–589 (2006)
28. Khare, C.: Modularity of Galois representations and motives with good reduction properties. J. Ramanujan Math. Soc. 22, 1–26 (2007)
29. Khare, C., Wintenberger, J.-P.: Serre’s modularity conjecture. Inv. Math. 178, 485–586 (2009)
30. Marshall, S., Müller, W.: On the torsion in the cohomology of arithmetic hyperbolic 3-manifolds. Duke Math. J. 162, 863–888 (2013)
31. Mestre, J.-F.: La méthode des graphes, exemples et applications. Notes (2004)
32. Page, A.: Méthodes explicites pour les groupes arithmétiques. Ph.D. Thesis, Université de Bordeaux (2012)
33. Raimbault, J.: Asymptotics of analytic torsion for hyperbolic 3-manifolds. arXiv:1212.3161 (2013)
34. Roberts, D.P.: Chebyshev covers and exceptional number fields. (2008)
35. Roberts, D.P.: Personal communication (November, 2013)
36. Schaeffer, G.J.: The Hecke stability method and ethereal forms. Ph.D. Thesis, University of California, Berkeley (2012)
37. Şengün, M.H.: On the integral cohomology of Bianchi groups. Exp. Math. 20, 487–505 (2011)
38. Serre, J.-P.: Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. Invent. Math. 15, 259–331 (1972)
39. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Publ. Math. I.H.E.S 54, 123–201 (1981)
40. Serre, J.-P.: Minoration de discriminants. Note of October 1975. Œuvres. Volume III, pp. 1972–1984. Springer, Heidelberg (2003)
41. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Publication of Mathematical Society of Japan, vol. 11. Princeton University Press, Princeton (1971)
42. Stein, W.: Modular forms: a computational approach. Graduate studies in mathematics, vol 79. American Mathematical Society (2007)
43. Stein, W.: Computing with Modular Forms, Course Notes. Harvard University, Harvard (2004)
44. Wallington, R.Q.: Number fields with solvable Galois groups and small Galois root discriminants. Ph.D. Thesis, Arizona State University (2009)
45. Wiese, G.: Dihedral Galois representations and Katz modular forms. Doc. Math. 9, 123–133 (2004)
46. Wiese, G.: On Galois representations of weight one. Doc. Math. 19, 689–707 (2014)