Chow, S., & Ghitza, A. (2015). Distinguishing newforms. International Journal of Number Theory, 11, 893-908. DOI: 10.1142/S1793042115500499

Distinguishing newforms*

Sam Chow[†]
University of Bristol
sam.chow42@gmail.com

Alexandru Ghitza[‡]
University of Melbourne
aghitza@alum.mit.edu

July 21, 2014

Abstract

Let $n_0(N, k)$ be the number of initial Fourier coefficients necessary to distinguish newforms of level N and even weight k. We produce extensive data to support our conjecture that if N is a fixed squarefree positive integer and k is large then $n_0(N, k)$ is the least prime that does not divide N.

1 Introduction

The predominant way of specifying a modular form is via its Fourier expansion

$$f(q) = \sum_{n=0}^{\infty} a_n(f) q^n. \tag{1.1}$$

Since this power series representation involves infinitely many coefficients, a natural question is whether one can recognise a given form f by looking at only finitely many (initial) coefficients. This is the object of a classical result of Sturm:[1]

Theorem 1.1 ([23], see also [18])**.** *Let $N, k \in \mathbb{Z}_{>0}$, and let $f, g \in M_k(\Gamma_0(N))$ with $f \neq g$. Then there exists*

$$n \leq \frac{k}{12} [\mathrm{SL}_2(\mathbb{Z})\colon \Gamma_0(N)] \tag{1.2}$$

such that $a_n(f) \neq a_n(g)$.

We refer to (1.2) as the *Sturm bound.* It is sharp at this level of generality. However, many modular forms that occur naturally in applications (especially in number-theoretic contexts) have additional properties, such as being eigenvectors for the Hecke operators. We ask the question: *Is it possible to sharpen the Sturm bound in the presence of this extra information?* More precisely, let $n_0 = n_0(N, k)$ be the smallest nonnegative integer such that the following statement is true:

*Thanks to James Withers for running some of the code. We also thank David Loeffler, M. Ram Murty, Abhishek Saha and Fredrik Strömberg for useful comments.

[†]The first author was supported by the Elizabeth and Vernon Puzey scholarship, and is grateful towards the University of Melbourne for their hospitality while preparing this memoir.

[‡]The second author was supported by Discovery Grant DP120101942 from the Australian Research Council.

[1]Theorem 1.1 is a special case of Sturm's main result, which is concerned with congruences between modular forms. The particular case we state here was very likely already known to Hecke, long before Sturm's work.

Let $f, g \in S_k(\Gamma_0(N))$ be newforms such that $a_n(f) = a_n(g)$ for all $n \leq n_0$. Then $f = g$.

The main problem studied in this paper is the dependence of n_0 on the parameters N and k, for $N, k \in \mathbb{Z}_{>0}$. Note that if k is odd then $n_0 = 0$, since $S_k(\Gamma_0(N)) = \{0\}$ (see [12, p. 15]). We therefore restrict attention to even weights k. The empirical data that we computed strongly support the following stability conjecture for squarefree levels:

Conjecture 4.1. *Let $N \in \mathbb{Z}_{>0}$ be squarefree. Then there exists $K \in \mathbb{Z}_{>0}$ such that if $k \geq K$ is an even integer then $n_0(N, k)$ is equal to the least prime that does not divide N.*

We note that the least prime that does not divide N is bounded above by $2(\log N + 1)$; see the proof of [6, Theorem 1]. The data also indicate a stability phenomenon in the non-squarefree level case, but we have not found a simple conjectural characterisation of the eventual value of n_0 in this situation—there are cases where it appears to exceed the least prime that does not divide N. We can prove the "easy half" of Conjecture 4.1:

Theorem 4.4. *Let $N \in \mathbb{Z}_{>0}$, and let $k \geq 38$ be an even integer. Then $n_0(N, k)$ is greater than or equal to the least prime that does not divide N.*

One might reasonably ask how large K needs to be in Conjecture 4.1. The data suggest $K = 38$ as a candidate for $1 \leq N \leq 30$ and $K = 8$ for $30 < N \leq 100$ (squarefree N). Does $K = 38$ suffice uniformly, or might K need to depend on N? The answer is not clear from the results of our computations, however it does seem that we can always take K to be quite small.

Many authors have studied the recognition problem for modular forms, e.g. [2], [3], [6], [8], [10], [13], [14], [17], [18], [23]. Maeda's conjecture (Conjecture 5.1) would imply that $n_0(1, k) \leq 2$ for all $k \in \mathbb{Z}_{>0}$, and from this and [15, Theorem 1] it would follow that $n_0(1, k) = 2$ for all even numbers $k \geq 28$. The second author and J. Withers [9] have proposed a generalisation of Maeda's conjecture that would imply Conjecture 4.1; this is discussed in §5.

Our algorithm for evaluating $n_0(N, k)$ is based on the fact that if f is a normalised Hecke eigenform and $n \in \mathbb{Z}_{>0}$ then $a_n(f)$ equals the eigenvalue of f with respect to the Hecke operator T_n. Moreover, it suffices to consider T_p for primes p (see Lemma 3.1). We consider intersections of T_p-eigenspaces over all primes p up to a point (call such intersections "homes"). Any home H has a basis given by its newforms, so the number of newforms in H is equal to $\dim H$. We continue until there are no homes of dimension greater than one.

Two main refinements improve the efficiency of our algorithm. We use modular symbols instead of modular forms (see (2.5)). Our second improvement is harder to describe. The idea is to factorise over $\mathbb{Q}$ the characteristic polynomial of T_p, considering the kernel of each irreducible factor. We intersect these kernels for small primes p, and run our algorithm on each such intersection. This enables us to work in smaller spaces, reducing the need to manipulate large matrices.

This paper is organised as follows. In §2, we clarify definitions and recall key results. In §3, we describe in detail our algorithm for computing $n_0(N, k)$. In §4, we discuss Conjecture 4.1 in more detail. In particular, we prove Theorem 4.4, and further address the case where N is not squarefree. Finally, in §5, we relate Conjecture 4.1 to a conjecture of the second author and J. Withers.

For $k \in \mathbb{Z}_{>0}$ and Γ a congruence subgroup, we denote by $M_k(\Gamma)$ the complex vector space of weight k modular forms for Γ, and write $S_k(\Gamma)$ for its cuspidal subspace. The symbol p is reserved for primes. For $r \in \mathbb{Z}_{>0}$, we write p_r for the rth smallest prime number. We shall write $\omega(N)$ for the number of distinct prime divisors of N. The algebraic closure of $\mathbb{Q}$ will be denoted $\overline{\mathbb{Q}}$.

2 Some background

In this section we recall some standard definitions and results. Let $N, k \in \mathbb{Z}_{>0}$. We shall work in

$$S := S_k^{\mathrm{new}}(\Gamma_0(N)), \tag{2.1}$$

the new subspace of $S_k(\Gamma_0(N))$. Here we refer the reader to [4, §I.6]. (The space S was first defined in [1].)

For each $n \in \mathbb{Z}_{>0}$ we have a Hecke operator T_n acting on S, and these commute (see [5, §5.3] and [20, Ch. 9]). The *Hecke algebra* is the commutative ring generated by the T_n:

$$\mathbb{T} = \mathbb{Z}[T_1, T_2, \ldots].$$

A *Hecke eigenform* is a modular form that is an eigenvector of T_n for every n. A Hecke eigenform is *normalised* if $a_1(f) = 1$, where $a_1(f)$ is as in (1.1). By [20, Proposition 9.10], if f is a normalised Hecke eigenform then

$$T_n f = a_n(f) f \qquad (n \in \mathbb{Z}_{>0}), \tag{2.2}$$

where $a_n(f)$ is as in (1.1). This means that we can compare Fourier coefficients by studying eigenvalues and eigenspaces of the operators T_n. A *newform* (in $S_k(\Gamma_0(N))$) is a normalised Hecke eigenform that lies in S. The proof of [5, Theorem 5.8.2] shows that the set of newforms in S is a basis for S. In particular, the space S contains precisely $\dim S$ newforms.

Let $n \in \mathbb{Z}_{>0}$. From [16, Theorem 4.5.19] (see also [19, Theorem 3.48]), we see that the characteristic polynomial χ_n of T_n acting on $S_k(\Gamma_0(N))$ has rational integer coefficients. If $f \in S_k(\Gamma_0(N))$ is a normalised Hecke eigenform then it follows from (2.2) that $a_n(f)$ is a root of χ_n, and is therefore an algebraic integer.

To hasten our calculations, we use modular symbols. There is a $\mathbb{T}$-module isomorphism

$$\Phi : S \to \mathbb{S}_k^{\mathrm{new}}(\Gamma_0(N); \mathbb{C})^+ \tag{2.3}$$

between S and the plus subspace of the new subspace of the vector space of cuspidal weight k modular symbols for $\Gamma_0(N)$ over $\mathbb{C}$ (see [20, Theorem 8.23] and the discussion on [20, p. 165]). We perform many of our calculations in $S^* := \mathbb{S}_k^{\mathrm{new}}(\Gamma_0(N); \mathbb{Q})^+$. The Hecke algebra acts on S^*, and there are isomorphisms

$$S^* \otimes F \simeq \mathbb{S}_k^{\mathrm{new}}(\Gamma_0(N); F)^+ \qquad (F = \overline{\mathbb{Q}}, \mathbb{C}) \tag{2.4}$$

of $\mathbb{T}$-modules. These isomorphisms follow from the definitions in [20, Ch. 8].

Let $B = B(N, k)$ be the Sturm bound, and let $f_1, \ldots, f_d$ be the newforms in S. There exist $r_1, \ldots, r_B \in \overline{\mathbb{Q}}$ such that

$$\sum_{n \le B} r_n a_n(f_i) \ne \sum_{n \le B} r_n a_n(f_j) \qquad (1 \le i < j \le d).$$

Indeed, if M is a matrix over $\overline{\mathbb{Q}}$ with distinct rows then the column span of M contains a vector whose entries are distinct. (With P a large positive integer, take the first column plus P times the second column plus P^2 times the third column, and so on.) The linear operator $T = \sum_{n \le B} r_n T_n$ acts irreducibly on S, since its eigenvalues are distinct. Hence, by (2.3) and (2.4), the linear operator T acts irreducibly on $S^* \otimes \mathbb{C}$, and therefore uniquely defines a basis of eigenvectors, up to rescaling. The space $S^* \otimes \overline{\mathbb{Q}}$ is stable under this action, and $\overline{\mathbb{Q}}$ is algebraically closed, so $S^* \otimes \overline{\mathbb{Q}}$ must have a basis $\mathcal{B}$ of eigenvectors for T. By (2.3) and (2.4), the modular symbols $\Phi(f_1), \ldots, \Phi(f_d)$ form a basis of eigenvectors for the action of T on $S^* \otimes \mathbb{C}$. For $i = 1, 2, \ldots, d$, choose $s_i \in \mathcal{B}$ equal to a constant times $\Phi(f_i)$. Now $f_i \mapsto s_i$ $(1 \le i \le d)$ is a $\mathbb{T}$-module isomorphism

$$S_k^{\mathrm{new}}(\Gamma_0(N); \overline{\mathbb{Q}}) \simeq S^* \otimes \overline{\mathbb{Q}}. \tag{2.5}$$

3 The algorithm for computing $n_0(N, k)$

Let $N, k \in \mathbb{Z}_{>0}$, and recall (2.1). We begin with the following observation:

Lemma 3.1. *Let $f, g \in M_k(\Gamma_0(N))$ be normalised Hecke eigenforms. Suppose $a_n(f) \neq a_n(g)$ for some $n \in \mathbb{Z}_{>0}$. Then there exists a prime divisor p of n such that $a_p(f) \neq a_p(g)$.*

Proof. This follows from (2.2) and [5, (5.10)], upon noting that $T_{mn} = T_m T_n$ whenever $(m, n) = 1$ (see [5, §5.3]). □

In view of (2.2), we now see that if $\dim S \ge 2$ then $n_0(N, k)$ is the least prime ℓ such that there do not exist distinct newforms $f, g \in S$ such that f and g have the same T_p eigenvalues for each prime $p \le \ell$. Our basic algorithm is as follows:

Algorithm 3.2. *Build S.*

1. *If* $\dim S < 2$*, return 0.*
2. *Consider the eigenspaces of the action of T_2 on S. Let $A_1, \ldots, A_a$ be the eigenspaces of dimension greater than one, and call these the* homes for T_2*. If $a = 0$, return 2.*
3. *Consider the eigenspaces of the action of T_3 on S, and intersect these with $A_1, \ldots, A_a$, separately. Let $B_1, \ldots, B_b$ be the intersections of dimension greater than one, and call these the* homes for T_3*. If $b = 0$, return 3.*
4. *Repeat for $T_5, T_7, T_{11}, \ldots$.*

As the newforms in S are linearly independent, the dimension of any subspace of S is greater than or equal to the number of newforms it contains. Thus, by the above discussion, the Sturm bound implies that Algorithm 3.2 terminates and returns an upper bound for n_0. In fact the output of Algorithm 3.2 is exactly n_0, since we can show that the dimension of any "home" is equal to the number of newforms it contains:

Lemma 3.3. *Every home, as defined in steps 2 and 3 of Algorithm 3.2, has a basis given by its newforms.*

Proof. We induct on primes. As discussed in §2, the space S has a basis given by its newforms. Let p be prime. If $p = 2$, let $H = S$. Otherwise, let H be a home for the Hecke operator corresponding to the prime before p. Our inductive hypothesis is that the set $\{f_1, \ldots, f_d\}$ of newforms in H is a basis for H. Let B be a home for T_p that comes from intersecting with H in step 3 of Algorithm 3.2 (if $p = 2$, let B be any home for T_2). It remains to show that the newforms in B constitute a basis for B.

Note that T_p acts on H, since the Hecke operators commute. Further, the home B is an eigenspace of this action. Recalling (1.1), and letting $a_p(f_i) = \lambda_i$ $(1 \leq i \leq d)$, we see that the characteristic polynomial of this action is $\prod_{i \leq d}(X - \lambda_i)$. Let λ be the eigenvalue associated to B, and let I be the set of $i \in \{1, 2, \ldots, d\}$ such that $\lambda_i = \lambda$. The set of newforms in B is $\{f_i : i \in I\}$. This is a basis for B, being a linearly independent subset of size $|I| = \dim B$. □

Using the software Sage [21], we may implement Algorithm 3.2. It suffices to work over $\overline{\mathbb{Q}}$, since the Fourier coefficients of normalised Hecke eigenforms are algebraic. Moreover, by (2.5), we may use modular symbols instead of modular forms. These changes improve the speed of our algorithm. They are implemented in Sage as follows:

Algorithm 3.4. *Build $S^* = \mathbb{S}_k^{\mathrm{new}}(\Gamma_0(N); \mathbb{Q})^+$. Suppose we wish to build the eigenspaces for the action of a Hecke operator on $S_k^{\mathrm{new}}(\Gamma_0(N); \overline{\mathbb{Q}})$. Compute the matrix of its action on S^*, then use the command*

```
base_extend
```

to consider it as a matrix with entries in $\overline{\mathbb{Q}}$. Build the eigenspaces for this matrix.

We thus produce the eigenspaces in $S^* \otimes \overline{\mathbb{Q}}$, which correspond via (2.5) to the eigenspaces in $S_k^{\mathrm{new}}(\Gamma_0(N); \overline{\mathbb{Q}})$. The drawback of the algorithm as described thus far (that is, modifying Algorithm 3.2 using Algorithm 3.4) is that it requires the manipulation of large matrices. To overcome this, we introduce the following refinement:

- Let q be a prime number.
- Consider, as a polynomial in T_2, the characteristic polynomial of the action of T_2 on S^*. Factorising this over $\mathbb{Q}$, consider the irreducible factors of dimension greater than 1, and take their kernels. Call these the *streets for* T_2.
- Compute the corresponding kernels with T_3 in place of T_2, intersect them with the streets for T_2, and take the intersections of dimension greater than one. Call these the *streets for* T_3.
- Repeat for $T_5, \ldots, T_q$.
- Return the streets for T_q, and call these the *final streets.*

Let q be prime, let $\mathcal{F}$ be a final street, and let $\mathcal{F}' = \mathcal{F} \otimes \overline{\mathbb{Q}}$. We seek to show that running the algorithm with $\mathcal{F}$ in place of S^* returns the smallest integer m such that if $f, g \in \mathcal{F}'$ are newforms such that $a_n(f) = a_n(g)$ for all $n \leq m$ then $f = g$ (*newforms* are understood with reference to (2.5)). For this purpose, it suffices to obtain the appropriate analogue to Lemma 3.3. By the proof of Lemma 3.3, it remains to show that $\mathcal{F}'$ has a basis given by its newforms.

Lemma 3.5. *Let q be prime, and let $\mathcal{F}$ be a corresponding final street. Then $\mathcal{F} \otimes \overline{\mathbb{Q}}$ has a basis given by its newforms.*

Proof. By the discussion after Algorithm 3.4, we may assume that $\mathfrak{S} := S_k^{\mathrm{new}}(\Gamma_0(N); \overline{\mathbb{Q}})$ is used, rather than S^*. We regard streets as intersections of kernels in $\mathfrak{S}$, and proceed by induction on primes. The base case is $\mathfrak{S}$, which has a basis given by its newforms. Let p be prime. If $p = 2$, let $F = \mathfrak{S}$. Otherwise, let F be a street for the Hecke operator corresponding to the prime before p. Our inductive hypothesis is that the set $\{f_1, \ldots, f_d\}$

of newforms in F is a basis for F. Consider the characteristic polynomial χ_p of the action of T_p on $\mathfrak{S}$. Factorising χ_p over $\mathbb{Q}$, let $P_1, \ldots, P_t$ be the distinct monic irreducible factors, and let $X_j = F \cap \ker P_j(T_p)$ $(1 \le j \le t)$. It remains to show that each X_j has a basis given by its newforms.

Recall (1.1), and let $a_p(f_i) = \lambda_i$ $(1 \le i \le d)$. Fix $j \in \{1, 2, \ldots, t\}$, and let I be the set of $i \in \{1, 2, \ldots, d\}$ such that $P_j(\lambda_i) = 0$. The set of newforms in X_j is $\{f_i : i \in I\}$. This set is linearly independent, so it remains to show that it spans X_j. Let $f \in X_j$, and write $f = c_1 f_1 + \ldots + c_d f_d$ with $c_1, \ldots, c_d \in \overline{\mathbb{Q}}$. Now

$$0 = P_j(T_p)(c_1 f_1 + \ldots + c_d f_d) = \sum_{i \le d} c_i P_j(\lambda_i) f_i,$$

so $c_i = 0$ whenever $i \notin I$. Now f lies in the span of $\{f_i : i \in I\}$, which completes the proof. $\square$

Let q be a prime number, and build the final streets as above. We run our algorithm on each of the final streets, and consider the maximum output, m. Suppose $m \ge q$. There exist distinct newforms $f, g \in S$ whose Fourier coefficients satisfy $a_p(f) = a_p(g)$ for all primes $p < m$; so $n_0 \ge m$. Further, there cannot exist distinct newforms $f, g \in S$ such that $a_p(f) = a_p(g)$ for all primes $p \le m$ (otherwise they would be in $\mathcal{F} \otimes \overline{\mathbb{Q}}$ for the same final street $\mathcal{F}$, contradicting the fact that m was the maximum output obtained by running the algorithm on the final streets). Hence $n_0 \le m$, so we must have $n_0 = m$.

To summarise the above discussion, if the maximum output is greater than or equal to our chosen prime number q, then it equals n_0. Thus, the following procedure returns $n_0(N, k)$:

- If $\dim S < 2$, return 0.
- Choose $q = 7$, and run the algorithm on each of the final streets, taking the maximum output m. If $m \ge q$, return m.
- Repeat for $q = 5, 3, 2$.
- Return 2.

For efficiency, we adopt one final finesse. By similar reasoning to above, we note that if $m < q$ then $n_0 \le q$. We can sometimes use this to deduce the value of n_0 without completing every step of the algorithm. For instance, if we know that $n_0 \le 7$, and that one of the final streets for $q = 5$ returns 7, then we must have $n_0 = 7$. Our full Sage [21] code may be found at the second author's webpage.[2] A sample of the resulting data is given in the appendix.

4 The stability conjecture

Our data suggest that if N is fixed then $n_0(N, k)$ stabilises as k increases (k even); see the appendix. The evidence is particularly compelling when N is squarefree, and we propound a more precise statement in this case:

Conjecture 4.1. *Let $N \in \mathbb{Z}_{>0}$ be squarefree. Then there exists $K \in \mathbb{Z}_{>0}$ such that if $k \ge K$ is an even integer then $n_0(N, k)$ is equal to the least prime that does not divide N.*

[2] `http://aghitza.org/research/`

Part of this conjecture can be obtained from the following result:

Theorem 4.2 (Atkin-Lehner [1, Theorem 3]). *Let $N, k \in \mathbb{Z}_{>0}$, let $f \in S_k(\Gamma_0(N))$ be a newform, and let p be a prime dividing N.*

(a) If $p^2 \mid N$ then $a_p(f) = 0$.

(b) If $p^2 \nmid N$ then $a_p(f) = \pm p^{\frac{k}{2}-1}$.

So for primes $p \mid N$, the eigenvalue $a_p(f)$ is heavily prescribed, which makes the operator T_p particularly bad at telling apart eigenforms. Thus, we would expect $n_0(N,k)$ to be greater than or equal to the least prime that does not divide N. This is indeed the case if the space $S = S_k^{\text{new}}(\Gamma_0(N))$ is sufficiently large:

Corollary 4.3. *Let $N, k \in \mathbb{Z}_{>0}$. Let $t \in \mathbb{Z}_{\geq 0}$ be the number of consecutive primes, starting from 2, that divide N (so p_{t+1} is the least prime that does not divide N). Suppose*

$$\dim S > 2^t.$$

Then n_0 is greater than or equal to the least prime that does not divide N.

Proof. Let $i \in \{1, 2, \ldots, t\}$, and note that $p_i \mid N$. By Theorem 4.2, there are at most 2 possible values for the p_i-th coefficient of a newform in S. (There is one possibility if $p_i^2 \mid N$, and two possibilities if $p_i^2 \nmid N$.)

Since S has a basis given by its newforms, there exist $\dim S \geq 2^t + 1$ distinct newforms in S. By the pigeonhole principle, there exist at least $2^{t-1} + 1$ distinct newforms in S with the same Fourier coefficient a_2. Among these, there exist at least $2^{t-2} + 1$ distinct newforms with the same a_3. Continuing in this way, there exist at least $2^{t-t} + 1 = 2$ distinct newforms with the same $a_2, a_3, a_5, \ldots, a_{p_t}$. We conclude that $n_0 \geq p_{t+1}$. □

Martin [15, Theorem 1] provides a formula for $\dim S$. Combining it with Corollary 4.3 gives rise to the "easy half" of Conjecture 4.1:

Theorem 4.4. *Let $N \in \mathbb{Z}_{>0}$, and let $k \geq 38$ be an even integer. Then $n_0(N, k)$ is greater than or equal to the least prime that does not divide N.*

Proof. As $k > 2$ is even, Martin [15, Theorem 1] gives

$$\dim S = (k-1)Ns_0^+(N)/12 - v_\infty^+(N)/2 + c_2(k)v_2^+(N) + c_3(k)v_3^+(N), \tag{4.1}$$

where s_0^+, v_∞^+, c_2, v_2^+, c_3 and v_3^+ are certain quickly computable arithmetic functions.

First suppose $N \geq 1000$. We deduce from (4.1) and the definitions of the arithmetic functions therein that

$$\dim S \geq (k-1)N/12 \times \Big(\prod_{p \mid N}(1 - p^{-1} - p^{-2})\Big) - \sqrt{N}/2 - 17/12 \times 2^{\omega(N)}.$$

Since $t \leq \omega(N)$ in Corollary 4.3, it now remains to show that

$$k > 1 + 12/N \times (\sqrt{N}/2 + 29/12 \times 2^{\omega(N)}) \times \prod_{p \mid N}(1 - p^{-1} - p^{-2})^{-1}. \tag{4.2}$$

We may easily verify the bounds

$$\prod_{p \mid N}(1 - p^{-1} - p^{-2})^{-1} \leq 20/9 \times (9/5)^{\omega(N)},$$

$(9/5)^{\omega(N)} < 2.8N^{1/4}$ and $2^{\omega(N)} < 5N^{1/4}$. Since

$$k \geq 38 > 1 + 6.23(6N^{-1/4} + 145N^{-1/2})$$

for all $N \geq 1000$, we now have (4.2).

For $N = 2, 4, 6, 12$, we shall use (4.1) to check that the hypothesis of Corollary 4.3 is met. We note that $-3/4 < c_2(k) \leq 1/4$ and $-2/3 < c_3(k) \leq 1/3$. If $N = 2$ then (4.1) yields

$$\dim S = (k-1)/12 - c_2(k) - 2c_3(k) \geq 37/12 - 1/4 - 2/3 > 2 = 2^t.$$

If $N = 4$ then (4.1) yields

$$\dim S = (k-1)/12 - c_2(k) + c_3(k) > 37/12 - 1/4 - 2/3 > 2 = 2^t.$$

If $N = 12$ then (4.1) yields

$$\dim S = (k-1)/6 + 2c_2(k) - c_3(k) > 37/6 - 3/2 - 1/3 > 4 = 2^t.$$

Consider $N = 6$. By (4.1), it suffices to prove that

$$(k-1)/6 + 2c_2(k) + 2c_3(k) > 4.$$

We can verify this directly for $k = 38, 40$, while if $k \geq 42$ then

$$(k-1)/6 + 2c_2(k) + 2c_3(k) > 41/6 - 3/2 - 4/3 = 4.$$

Finally, suppose that $N < 1000$ with $N \notin \{2, 4, 6, 12\}$. By direct computation, we have

$$k \geq 38 > 1 + \frac{12(v_\infty^+(N)/2 + 3|v_2^+(N)|/4 + 2|v_3^+(N)|/3 + 2^t)}{Ns_0^+(N)}.$$

The proof is completed via (4.1) and Corollary 4.3, recalling that $|c_2(k)| < 3/4$ and $|c_3(k)| < 2/3$. $\square$

The following example suggests that the non-squarefree level case is more complicated. We take the following definition from [24, p. 2]. Let $N, k \in \mathbb{Z}_{>0}$, let $f \in S_k(\Gamma_0(N))$, and let χ be a Dirichlet character. The *twist of f by χ* is given by

$$f \otimes \chi(q) = \sum_{n=1}^{\infty} \chi(n) a_n(f) q^n.$$

Example 4.5. *Let $S = S_k^{\mathrm{new}}(\Gamma_0(49))$, and let χ be the Legendre symbol modulo 7, i.e.*

$$\chi(n) = \left(\frac{n}{7}\right) \qquad (n \in \mathbb{Z}).$$

For each $k \in \{4, 6, 8, 10, 12\}$, we observe newforms $f, g \in S$ such that $f = g \otimes \chi$ and $g = f \otimes \chi$. As $\chi(2) = 1$, we have $a_2(f) = a_2(g)$, so T_2 fails to distinguish f and g.

This phenomenon is closely related to the existence of CM forms (see [24, p. 2]). Indeed, in the example above $f + g$ has complex multiplication by χ. It is likely that the forms f and g, although "new" in the usual sense (not arising from $\Gamma_0(7)$ or $\Gamma_0(1)$), are coming from a different congruence subgroup Γ of level 7. For an explanation of this type of behaviour for $\Gamma_0(9)$, see [22].

There may be a more general stability phenomenon which also encompasses non-squarefree values of N. In the cases $N = 49, 108, 147, 225$, one might predict from the data that n_0 stabilises towards a prime that exceeds the least prime that does not divide N (see Tables 5 and 8). For all other values of N that we examined, it would appear that n_0 stabilises towards the least prime that does not divide N. Does there always exist $K \in \mathbb{Z}_{>0}$ such that if $k \geq K$ is an even integer then $n_0(N, k) = n_0(N, K)$?

5 Irreducibility of Hecke polynomials

A *Hecke polynomial* is the characteristic polynomial of a Hecke operator T_n acting on a space of modular forms. In the 1970s, Maeda observed that the Hecke polynomials of T_2 on $S_k(\mathrm{SL}_2(\mathbb{Z}))$ are irreducible over $\mathbb{Q}$ for all k such that $\dim S_k(\mathrm{SL}_2(\mathbb{Z})) \leq 12$. Over the next 20 years, this observation matured into the following statement:

Conjecture 5.1 (Maeda [11])**.** *Let $k \in \mathbb{Z}_{>0}$, $n \in \mathbb{Z}_{>1}$, and let $F \in \mathbb{Z}[X]$ be the characteristic polynomial of the Hecke operator T_n acting on $\mathcal{S} := S_k(\mathrm{SL}_2(\mathbb{Z}))$. Then F is irreducible over $\mathbb{Q}$ and its Galois group G is isomorphic to the symmetric group $\Sigma_{\dim \mathcal{S}}$.*

We refer the reader to [7] for a survey of results on Maeda's conjecture and a report on its verification for the operator T_2 and weights $k \leq 14\,000$.

In [24], Tsaknias considers higher-level generalisations of the following weak version of Conjecture 5.1: *there is a unique Galois orbit of Hecke eigenforms in* $S_k(\mathrm{SL}_2(\mathbb{Z}))$. We describe his findings in the squarefree level case. If $N = p_1 p_2 \ldots p_t$ is squarefree, the Atkin-Lehner involutions w_{p_i} decompose the space of newforms into eigenspaces

$$S_k^{\mathrm{new}}(\Gamma_0(N)) = \bigoplus_{\epsilon \in \{\pm 1\}^t} S_\epsilon.$$

Tsaknias's computations indicate that, for k large enough, the space $S_k^{\mathrm{new}}(\Gamma_0(N))$ has 2^t Galois orbits of newforms. The second author and J. Withers [9] have investigated higher-level analogues of the full Maeda conjecture. Their experiments suggest the following statement in the squarefree level case:

Conjecture 5.2. *Let $N \in \mathbb{Z}_{>0}$ be squarefree. Then there exists $K' \in \mathbb{Z}_{>0}$ such that the following hold whenever $k \geq K'$ is even and $n \geq 2$ is coprime to N:*

(a) The characteristic polynomial F of the Hecke operator T_n acting on $S_k^{\mathrm{new}}(\Gamma_0(N))$ is separable (that is, F has no repeated roots over $\overline{\mathbb{Q}}$).

(b) The Atkin-Lehner decomposition

$$S_k^{\mathrm{new}}(\Gamma_0(N)) = \bigoplus_{\epsilon} S_\epsilon$$

is the only obstacle to the irreducibility of the polynomial F.

These statements have been verified computationally for squarefree $N \leq 200$, even weights $k \leq 30$ and operators T_p for $p < 100$ prime and not dividing N. Our immediate interest in Conjecture 5.2 is the following result:

Theorem 5.3. *Part (a) of the generalised Maeda Conjecture 5.2 implies the stability Conjecture 4.1.*

Proof. Let $N \in \mathbb{Z}_{>0}$ be squarefree. Let $K = \max\{38, K'\}$, with K' provided by Conjecture 5.2. Let p be the least prime that does not divide N, and let $k \geq K$ be even. By Theorem 4.4, we have $n_0(N, k) \geq p$. So it suffices to show that if $f, g \in S_k(\Gamma_0(N))$ are distinct newforms then $a_p(f) \neq a_p(g)$.

Let $\mathcal{B} = \{f_1, f_2, \ldots, f_d\}$ be the newforms in $S_k(\Gamma_0(N))$, where $d = \dim S_k^{\mathrm{new}}(\Gamma_0(N))$. We know that $\mathcal{B}$ is a basis for $S_k^{\mathrm{new}}(\Gamma_0(N))$, so $\{a_p(f_1), a_p(f_2), \ldots, a_p(f_d)\}$ is precisely the set of roots of the characteristic polynomial of T_p. But by part (a) of Conjecture 5.2, this polynomial has d distinct roots, hence $a_p(f_i) \neq a_p(f_j)$ for $i \neq j$. □

Appendix: Data

We tabulate $n_0 = n_0(N, k)$ for k even (if k is odd then $n_0 = 0$). We put N on the vertical axis and k on the horizontal axis, so that along any row N is fixed and k varies. A larger set of data may be found at the second author's webpage.[3]

Table 1: Some values of $n_0(N, k)$.

N \ k	38	40	42	44	46	48	50	52	54	56
1	2	2	2	2	2	2	2	2	2	2
2	3	3	3	3	3	3	3	3	3	3
3	2	2	2	2	2	2	2	2	2	2
4	3	3	3	3	3	3	3	3	3	3
5	2	2	2	2	2	2	2	2	2	2
6	5	5	5	5	5	5	5	5	5	5

Table 2: More values of $n_0(N, k)$.

N \ k	24	26	28	30	32	34	36	38	40	42
7	2	2	2	2	2	2	2	2	2	2
8	3	3	3	3	3	3	3	3	3	3
9	2	2	2	2	2	2	2	2	2	2
10	3	3	3	3	3	3	3	3	3	3
11	2	2	2	2	2	2	2	2	2	2
12	5	5	5	5	5	5	5	5	5	5

[3] `http://aghitza.org/research/`

Table 3: More values of $n_0(N, k)$.

N \ k	12	14	16	18	20	22	24	26	28	30
13	2	2	2	2	2	2	2	2	2	2
14	3	3	3	3	3	3	3	3	3	3
15	2	2	2	2	2	2	2	2	2	2
16	3	3	3	3	3	3	3	3	3	3
17	2	2	2	2	2	2	2	2	2	2
18	5	5	5	5	5	5	5	5	5	5
19	2	2	2	2	2	2	2	2	2	2
20	3	3	3	3	3	3	3	3	3	3
21	2	2	2	2	2	2	2	2	2	2
22	3	3	3	3	3	3	3	3	3	3
23	2	2	2	2	2	2	2	2	2	2
24	5	5	5	5	5	5	5	5	5	5
25	2	2	2	2	2	2	2	2	2	2
26	3	3	3	3	3	3	3	3	3	3

Table 4: More values of $n_0(N, k)$.

N \ k	10	12	14	16	18	20	22	24	26	28
27	2	2	2	2	2	2	2	2	2	2
28	3	3	3	3	3	3	3	3	3	3
29	2	2	2	2	2	2	2	2	2	2
30	5	5	7	7	7	7	7	7	7	7
31	2	2	2	2	2	2	2	2	2	2
32	2	3	3	3	3	3	3	3	3	3
33	2	2	2	2	2	2	2	2	2	2
34	3	3	3	3	3	3	3	3	3	3
35	2	2	2	2	2	2	2	2	2	2
36	5	5	5	5	5	5	5	5	5	5
37	2	2	2	2	2	2	2	2	2	2

Table 5: More values of $n_0(N, k)$.

N \ k	2	4	6	8	10	12	14	16	18	20	22	24
38	2	3	3	3	3	3	3	3	3	3	3	3
39	2	2	2	2	2	2	2	2	2	2	2	2
40	0	3	3	3	3	7	3	3	3	3	3	3
41	2	2	2	2	2	2	2	2	2	2	2	2
42	0	3	5	5	5	5	5	5	5	5	5	5
43	2	2	2	2	2	2	2	2	2	2	2	2
44	0	3	3	3	3	3	3	3	3	3	3	3
45	0	2	2	2	2	2	2	2	2	2	2	2
46	0	3	3	3	3	3	3	3	3	3	3	3
47	2	2	2	2	2	2	2	2	2	2	2	2
48	0	5	5	5	5	5	5	5	5	5	5	5
49	0	3	3	3	3	3	3	3	3	3	3	3
50	2	3	3	3	3	3	3	3	3	3	3	3
51	2	3	2	2	2	2	2	2	2	2	2	2
52	0	3	3	3	3	3	3	3	3	3	3	3
53	2	2	2	2	2	2	2	2	2	2	2	2
54	2	5	5	5	5	5	5	5	5	5	5	5
55	2	2	2	2	2	2	2	2	2	2	2	2
56	3	3	3	3	3	3	3	3	3	3	3	3
57	3	2	2	2	2	2	2	2	2	2	2	2

Table 6: More values of $n_0(N, k)$.

N \ k	2	4	6	8	10	12	14	16	18	20	22	24
58	2	3	3	3	3	3	3	3	3	3	3	3
59	2	2	2	2	2	2	2	2	2	2	2	2
60	0	5	5	5	7	7	7	7	7	7	7	7
61	2	2	2	2	2	2	2	2	2	2	2	2
62	3	3	3	3	3	3	3	3	3	3	3	3
63	2	2	2	2	2	2	2	2	2	2	2	2
64	0	3	3	3	3	3	3	3	3	3	3	3
65	2	2	2	2	2	2	2	2	2	2	2	2
66	3	5	7	5	5	5	5	5	5	5	5	5
67	2	2	2	2	2	2	2	2	2	2	2	2
68	3	3	3	3	3	3	3	3	3	3	3	3

Table 7: More values of $n_0(N, k)$.

N \ k	2	4	6	8	10	12	14	16	18	20
69	2	2	2	2	2	2	2	2	2	2
70	0	3	3	3	3	3	3	3	3	3
71	2	2	2	2	2	2	2	2	2	2
72	0	5	5	5	5	5	5	5	5	5
73	2	2	2	2	2	2	2	2	2	2
74	3	3	3	3	3	3	3	3	3	3
75	2	2	2	2	2	2	2	2	2	2
76	0	3	3	3	3	3	3	3	3	3
77	3	2	2	2	2	2	2	2	2	2
78	0	5	5	5	5	5	5	5	5	5
79	2	2	2	2	2	2	2	2	2	2
80	3	7	3	3	3	7	3	3	3	3
81	2	2	2	2	2	2	2	2	2	2
82	3	3	3	3	3	3	3	3	3	3
83	2	2	2	2	2	2	2	2	2	2
84	3	3	5	5	5	5	5	5	5	5
85	2	3	2	2	2	2	2	2	2	2
86	3	3	3	3	3	3	3	3	3	3
87	2	2	2	2	2	2	2	2	2	2

Table 8: More values of $n_0(N, k)$.

N \ k	2	4	6	8	10	12	14	16
88	3	3	3	3	3	3	3	3
89	2	2	2	2	2	2	2	2
90	5	7	7	7	7	7	7	7
91	2	2	2	2	2	2	2	2
92	3	3	3	3	3	3	3	3
93	2	2	2	2	2	2	2	2
94	3	3	3	3	3	3	3	3
95	2	3	2	2	2	2	2	2
96	3	5	5	5	5	5	5	5
97	2	2	2	2	2	2	2	2
98	3	3	3	3	3	3	3	3
99	5	2	2	2	2	2	2	2
100	0	3	3	3	3	3	3	3
108	0	7	7	5	7	5	5	7
147	3	5	3	3	3	3		
225	7	7	7	7	7	7		

References

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

[2] S. Baba, K. Chakraborty and Y. N. Petridis, *On the number of Fourier coefficients that determine a Hilbert modular form*, Proc. Amer. Math. Soc. **130** (2002), no. 9, 2497–2502.

[3] S. Chow and A. Ghitza, *Distinguishing modular forms modulo a prime ideal*, Funct. Approx. Comment. Math., to appear, `arXiv:1304.1832`.

[4] F. Diamond and J. Im, *Modular forms and modular curves*, in *Seminar on Fermat's Last Theorem*, CMS Conference Proceedings **17** (Amer. Math. Soc. 1995), 39–133.

[5] F. Diamond and J. Shurman, *A first course in modular forms*, Springer, 2005.

[6] A. Ghitza, *Distinguishing Hecke eigenforms*, Int. J. Number Theory **7** (2011), 1247–1253.

[7] A. Ghitza and A. McAndrew, *Experimental evidence for Maeda's conjecture on modular forms*, Tbil. Math. J. **5**, no. 2 (2012), 55–69, special issue on symbolic computation using Sage.

[8] A. Ghitza and R. Sayer, *Hecke eigenvalues of Siegel modular forms of "different weights"*, arXiv:1305.7011.

[9] A. Ghitza and J. Withers, *A higher level version of Maeda's conjecture*, in preparation.

[10] D. Goldfeld and J. Hoffstein, *On the number of terms that determine a modular form*, in *A tribute to Emil Grosswald: number theory and related analysis*, Contemp. Math. **143** (Amer. Math. Soc. 1993), 385–393.

[11] H. Hida and Y. Maeda, *Non-abelian base change for totally real fields*, Olga Taussky-Todd: in memoriam, Pacific J. Math. **Special Issue** (1997), 189–217.

[12] L. Kilford, *Modular Forms: A classical and computational introduction*, Imperial College Press, 2008.

[13] W. Kohnen, *On Fourier coefficients of modular forms of different weights*, Acta Arith. **113** (2004), no. 1, 57–67.

[14] E. Kowalski, *Variants of recognition problems for modular forms*, Arch. Math. (Basel) **84** (2005), no. 1, 57–70.

[15] G. Martin, *Dimensions of the spaces of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$, J. Number Theory **112** (2005), 298–331.

[16] T. Miyake, *Modular forms*, Springer-Verlag, 1997.

[17] C. J. Moreno, *Analytic proof of the strong multiplicity one theorem*, Amer. J. Math. **107** (1985), no. 1, 163–206.

[18] M. Ram Murty, *Congruences between modular forms*, London Mathematical Society Lecture Note Series **247** (1997), Cambridge University Press, 309–320.

[19] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[20] W. Stein, *Modular Forms, a Computational Approach*, Graduate Studies in Mathematics **79**, American Mathematical Society, 2007. With an appendix by Paul E. Gunnells.

[21] W. Stein et al., Sage Mathematics Software (Version 5.1), The Sage Development Team, 2012, `http://www.sagemath.org`.

[22] F. Strömberg, *Newforms and spectral multiplicity for* $\Gamma_0(9)$, Proc. Lond. Math. Soc. (3) **105**, no. 2 (2012), 281–310.

[23] J. Sturm, *On the congruence of modular forms*, in *Number Theory*, Lecture Notes in Mathematics **1240** (1987), Springer-Verlag, 275–280.

[24] P. Tsaknias, *A possible generalization of Maeda's conjecture*, in *Computations with Modular Forms*, Contributions in Mathematical and Computational Sciences **6** (2014), Springer, 317–329.