On the failure of the Gorenstein property for Hecke algebras of prime weight

L. J. P. Kilford and Gabor Wiese

9th October 2007

Abstract

In this article we report on extensive calculations concerning the Gorenstein defect for Hecke algebras of spaces of modular forms of prime weight p at maximal ideals of residue characteristic p such that the attached mod p Galois representation is unramified at p and the Frobenius at p acts by scalars. The results lead us to the ask the question whether the Gorenstein defect and the multiplicity of the attached Galois representation are always equal to 2. We review the literature on the failure of the Gorenstein property and multiplicity one, discuss in some detail a very important practical improvement of the modular symbols algorithm over finite fields and include precise statements on the relationship between the Gorenstein defect and the multiplicity of Galois representations.

1 Introduction

In Wiles' proof of Fermat's Last Theorem (see [Wiles 1995]) an essential step was to show that certain Hecke algebras are Gorenstein rings. Moreover, the Gorenstein property of Hecke algebras is equivalent to the fact that Galois representations appear on certain Jacobians of modular curves precisely with multiplicity one. This article is concerned with the Gorenstein property and with the multiplicity one question. We report previous work and exhibit many new examples where multiplicity one and the Gorenstein property fail. We compute the multiplicity in these cases. Moreover, we ask the question suggested by our computations whether it is always equal to two if it fails.

We first have to introduce some notation. For integers $N \geq 1$ and $k \geq 2$ and a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ we let $S_k(\Gamma_1(N))$ be the $\mathbb{C}$-vector space of holomorphic cusp forms on $\Gamma_1(N)$ of weight k and $S_k(N, \chi)$ the subspace on which the diamond operators act through the character χ. We now introduce some extra notation for Hecke algebras over specified rings.

Notation 1.1 (Notation for Hecke algebras) *Whenever $S \subseteq R$ are rings and M is an R-module on which the Hecke and diamond operators act, we let $\mathbb{T}_S(M)$ be the S-subalgebra inside the R-endomorphism ring of M generated by the Hecke and the diamond operators. If $\phi : S \to S'$ is a ring homomorphism, we let $\mathbb{T}_\phi(M) := \mathbb{T}_S(M) \otimes_S S'$ or with ϕ understood $\mathbb{T}_{S \to S'}(M)$.*

We will mostly be dealing with the Hecke algebras $\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N)))$ and $\mathbb{T}_{\mathbb{Z}[\chi]}(S_k(N,\chi))$, their completions $\mathbb{T}_{\mathbb{Z}\to\mathbb{Z}_p}(S_k(\Gamma_1(N)))$ and $\mathbb{T}_{\mathcal{O}\to\widehat{\mathcal{O}}}(S_k(N,\chi))$, as well as their reductions $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N)))$ and $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(S_k(N,\chi))$. Here, p is a prime and $\mathcal{O}=\mathbb{Z}[\chi]$ is the smallest subring of $\mathbb{C}$ containing all values of χ, $\widehat{\mathcal{O}}$ is the completion at a prime above p and $\mathcal{O}\twoheadrightarrow\mathbb{F}$ is the reduction modulo that prime. In Section 3 the reductions of the Hecke algebras are identified with Hecke algebras of mod p modular forms, which are closely related to Hecke algebras of Katz modular forms over finite fields (see Section 2).

We choose a holomorphic cuspidal Hecke eigenform as the starting point of our discussion and treatment. So let $f\in S_k(N,\chi)\subseteq S_k(\Gamma_1(N))$ be an eigenform for all Hecke and diamond operators. It (more precisely, its Galois conjugacy class) corresponds to minimal ideals, both denoted by $\mathfrak{p}_f$, in each of the two Hecke algebras $\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N)))$ and $\mathbb{T}_{\mathbb{Z}[\chi]}(S_k(N,\chi))$. We also choose maximal ideals $\mathfrak{m}=\mathfrak{m}_f$ containing $\mathfrak{p}_f$ of residue characteristic p again in each of the two. Note that the residue fields are the same in both cases.

By work of Shimura and Deligne, one can associate to f (more precisely, to $\mathfrak{m}$) a continuous odd semi-simple Galois representation

$$\rho_f=\rho_{\mathfrak{m}_f}=\rho_{\mathfrak{m}}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{GL}_2(\mathbb{T}_{\mathbb{Z}}(S_k(N,\chi))/\mathfrak{m})$$

unramified outside Np satisfying $\mathrm{Tr}(\rho_{\mathfrak{m}}(\mathrm{Frob}_l))\equiv T_l \mod \mathfrak{m}$ and $\mathrm{Det}(\rho_{\mathfrak{m}}(\mathrm{Frob}_l))\equiv l^{k-1}\chi(l) \mod \mathfrak{m}$ for all primes $l\nmid Np$. In the case of weight $k=2$ and level N, the representation $\rho_{\mathfrak{m}}$ can be naturally realised on the p-torsion points of the Jacobian of the modular curve $X_1(N)_{\mathbb{Q}}$. The algebra $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(N)))$ acts naturally on $J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[p]$ and we can form the Galois module $J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[\mathfrak{m}]=J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[p][\widetilde{\mathfrak{m}}]$ with $\widetilde{\mathfrak{m}}$ the maximal ideal of $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(N)))$ which is the image of $\mathfrak{m}$ under the natural projection. Supposing that $\rho_{\mathfrak{m}}$ is absolutely irreducible, the main result of [Boston et al. 1991] shows that the Galois representation $J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[\mathfrak{m}]$ is isomorphic to a direct sum of r copies of $\rho_{\mathfrak{m}}$ for some integer $r\geq 1$, which one calls the *multiplicity of* $\rho_{\mathfrak{m}}$ *on* $J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[\mathfrak{m}]$ (cf. [Ribet and Stein 2001]). We shall for short only speak about the multiplicity of $\rho_{\mathfrak{m}}$. One says that $\rho_{\mathfrak{m}}$ is a *multiplicity one representation* or *satisfies multiplicity one*, if $r=1$. See [Mazur 1977] for a similar definition for $J_0(N)$ and Prop. 2.6 for a comparison.

The notion of multiplicity can be naturally extended to Galois representations attached to eigenforms f of weights $3\leq k\leq p+1$ for $p\nmid N$. This is accomplished by a result of Serre's which implies the existence of a maximal ideal $\mathfrak{m}_2\subset\mathbb{T}_{\mathbb{Z}}(S_2(\Gamma_1(Np)))$ such that $\rho_{\mathfrak{m}_f}\cong\rho_{\mathfrak{m}_2}$ (see Prop. 2.3). One hence obtains the notion of multiplicity (on $J_1(Np)$) for the representation $\rho_{\mathfrak{m}_f}$ by defining it as the multiplicity of $\rho_{\mathfrak{m}_2}$. Moreover, when allowing twists by the cyclotomic character, it is even possible to treat arbitrary weights. The following theorem summarises results on when the multiplicity in the above sense is known to be one.

Theorem 1.2 (Mazur, Edixhoven, Tilouine, Gross, Buzzard) *Let $\rho_{\mathfrak{m}}$ be a representation associated with a modular cuspidal eigenform $f\in S_k(N,\chi)$ and let p be the residue characteristic of $\mathfrak{m}$. Suppose that $\rho_{\mathfrak{m}}$ is absolutely irreducible and that p does not divide N. If either*

1. $2 \leq k \leq p-1$, *or*
2. $k = p$ *and* $\rho_{\mathfrak{m}}$ *is ramified at* p, *or*
3. $k = p$ *and* $\rho_{\mathfrak{m}}$ *is unramified at* p *and* $\rho_{\mathfrak{m}}(\mathrm{Frob}_p)$ *is not scalar,*

then the multiplicity of $\rho_{\mathfrak{m}}$ *is one.*

This theorem is composed of [Mazur 1977], Lemma 15.1, [Tilouine 1987], Proposition 5.6, [Edixhoven 1992], Theorem 9.2, as well as [Gross 1990], Proposition 12.10, and [Buzzard 1999], Theorem 6.1. The following theorem by the second author ([Wiese 2007a], Corollary 4.5) tells us when the multiplicity is not one.

Theorem 1.3 *Let* $\rho_{\mathfrak{m}}$ *as in the previous theorem. Suppose* $k = p$ *and that* $\rho_{\mathfrak{m}}$ *is unramified at* p. *If* $p = 2$, *assume also that a Katz cusp form over* $\mathbb{F}_2$ *of weight* 1 *on* $\Gamma_1(N)$ *exists which gives rise to* $\rho_{\mathfrak{m}}$.

If $\rho_{\mathfrak{m}}(\mathrm{Frob}_p)$ *is a scalar matrix, then the multiplicity of* $\rho_{\mathfrak{m}}$ *is bigger than* 1.

In Section 2 we explain how the Galois representation $J_1(Np)_{\mathbb{Q}}(\overline{\mathbb{Q}})[\mathfrak{m}]$ is related to the different Hecke algebras evoked above and see in many cases of interest a precise relationship between the geometrically defined term of *multiplicity* and the *Gorenstein defect* of these algebras. The latter can be computed explicitly, which is the subject of the present article. We now give the relevant definitions.

Definition 1.4 (The Gorenstein property) *Let* A *be a local Noetherian ring with maximal ideal* $\mathfrak{m}$. *Suppose first that the Krull dimension of* A *is zero, i.e. that* A *is Artinian. We then define the* Gorenstein defect *of* A *to be the minimum number of* A*-module generators of the annihilator of* $\mathfrak{m}$ *(i.e.* $A[\mathfrak{m}]$*) minus 1; equivalently, this is the* $A/\mathfrak{m}$*-dimension of the annihilator of* $\mathfrak{m}$ *minus 1. We say that* A *is* Gorenstein *if its Gorenstein defect is 0, and* non-Gorenstein *otherwise. If the Krull dimension of* A *is positive, we inductively call* A Gorenstein, *if there exists a non-zero-divisor* $x \in \mathfrak{m}$ *such that* $A/(x)$ *is a Gorenstein ring of smaller Krull dimension (see [Eisenbud 1995], p. 532; note that our definition implies that* A *is Cohen-Macaulay). A (not necessarily local) Noetherian ring is said to be* Gorenstein *if and only if all of its localisations at its maximal ideals are Gorenstein.*

We will for example be interested in the Gorenstein property of $\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N)))_{\mathfrak{m}}$. Choosing $x = p$ in the definition with p the residue characteristic of $\mathfrak{m}$, we see that this is equivalent to the Gorenstein defect of the finite dimensional $\mathbb{F}_p$-algebra $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N)))_{\mathfrak{m}}$ being zero. Whenever we refer to the Gorenstein defect of the former algebra (over $\mathbb{Z}$), we mean the one of the latter. Our computations will concern the Gorenstein defect of $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(S_k(\Gamma_1(N),\chi))_{\mathfrak{m}}$. See Section 2 for a comparison with the one not involving a character. It is important to remark that the Gorenstein defect of a local Artin algebra over a field does not change after passing to a field extension and taking any of the conjugate local factors.

We illustrate the definition by an example. The algebra $k[x,y,z]/(x^2,y^2,z^2,xy,xz,yz)$ for a field k is Artinian and local with maximal ideal $\mathfrak{m} := (x,y,z)$ and the annihilator of $\mathfrak{m}$ is $\mathfrak{m}$ itself,

so the Gorenstein defect is $3 - 1 = 2$. We note that this particular case does occur in nature; a localisation $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_2}(S_2(\Gamma_0(431)))_{\mathfrak{m}}$ at one maximal ideal is isomorphic to this, with $k = \mathbb{F}_2$ (see [Emerton 2002], the discussion just before Lemma 6.6). This example can also be verified with the algorithm presented in this paper.

We now state a translation of Theorem 1.2 in terms of Gorenstein defects, which is immediate from the propositions in Section 2.

Theorem 1.5 *Assume the set-up of Theorem 1.2 and that one of 1., 2., or 3. is satisfied. We use notations as in the discussion of multiplicities above.*

If $k = 2$, then $\mathbb{T}_{\mathbb{Z}}(S_2(\Gamma_1(N)))_{\mathfrak{m}}$ is a Gorenstein ring.

If $k \geq 3$, then $\mathbb{T}_{\mathbb{Z}}(S_2(\Gamma_1(Np)))_{\mathfrak{m}_2}$ is, too. Supposing in addition that $\mathfrak{m}$ is ordinary (i.e. $T_p \notin \mathfrak{m}$), then also $\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N)))_{\mathfrak{m}}$ is Gorenstein. If, moreover, $p \geq 5$ or $\rho_{\mathfrak{m}}$ is not induced from $\mathbb{Q}(\sqrt{-1})$ (if $p = 2$) or $\mathbb{Q}(\sqrt{-3})$ (if $p = 3$), then $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(S_k(N,\chi))_{\mathfrak{m}}$ is Gorenstein as well. □

We now turn our attention to computing the Gorenstein defect and the multiplicity in the case when it is known not to be one.

Corollary 1.6 *Let $\rho_{\mathfrak{m}}$ be a representation associated with a cuspidal eigenform $f \in S_p(N,\chi)$ with p the residue characteristic of $\mathfrak{m}$. Assume that $\rho_{\mathfrak{m}}$ is absolutely irreducible, unramified at p such that $\rho_{\mathfrak{m}}(\mathrm{Frob}_p)$ is a scalar matrix. Let r be the multiplicity of $\rho_{\mathfrak{m}}$ and d the Gorenstein defect of any of $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(S_k(N,\chi))_{\mathfrak{m}}$, $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N)))_{\mathfrak{m}}$ or $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(Np)))_{\mathfrak{m}_2}$.*

Then the relation $d = 2r - 2$ holds.

Proof. The equality of the Gorenstein defects and the relation with the multiplicity are proved in Section 2, noting that $\mathfrak{m}$ is ordinary, as $a_p(f)^2 = \chi(p) \neq 0$ (e.g. by [Gross 1990], p. 487). □

1.1 Previous results on the failure of multiplicity one or the Gorenstein property

Prior to the present work and the article [Wiese 2007a], there have been some investigations into when Hecke algebras fail to be Gorenstein. In [Kilford 2002], the first author showed, using MAGMA [Bosma et al. 1997], that none of the three Hecke algebras $\mathbb{T}_{\mathbb{Z}}(S_2(431,\chi_{\mathrm{triv}}))$, $\mathbb{T}_{\mathbb{Z}}(S_2(503,\chi_{\mathrm{triv}}))$ and $\mathbb{T}_{\mathbb{Z}}(S_2(2089,\chi_{\mathrm{triv}}))$ is Gorenstein by explicit computation of the localisation of the Hecke algebra at a suitable maximal ideal above 2, and in [Ribet and Stein 2001], it is shown that $\mathbb{T}_{\mathbb{Z}}(S_2(2071,\chi_{\mathrm{triv}}))$ is not Gorenstein in a similar fashion. These examples were discovered by considering elliptic curves $E/\mathbb{Q}$ such that in the ring of integers of $\mathbb{Q}(E[2])$ the prime ideal (2) splits completely, and then doing computations with MAGMA.

There are also some results in the literature on the failure of multiplicity one within the torsion of certain Jacobians. In [Agashe et al. 2006], Proposition 5.1, the following theorem is proved:

Theorem 1.7 (Agashe, Ribet, Stein) *Suppose that E is an optimal elliptic curve over $\mathbb{Q}$ of conductor N, with congruence number r_E and modular degree m_E and that p is a prime such that $p|r_E$ but $p \nmid m_E$. Let $\mathfrak{m}$ be the annihilator in $\mathbb{T}_{\mathbb{Z}}(S_2(N,\chi_{\mathrm{triv}}))$ of $E[p]$. Then multiplicity one fails for $\mathfrak{m}$.*

They give a table of examples; for instance, $\mathbb{T}_{\mathbb{Z}}(S_2(54, \chi_{\mathrm{triv}}))$ does not satisfy multiplicity one at some maximal ideal above 3. It is not clear whether this phenomenon occurs infinitely often.

The first examples of the failure of multiplicity one were given in [Mazur and Ribet 1991], where it is proved in Theorem 2 that the mod p multiplicity of a suitable representation $\rho_{\mathfrak{m}}$ of level prime to N in the torsion of the Jacobian $J_0(p^3N)$ is greater than 1. The explicit example given there is of a representation of level 11 having mod 11 multiplicity greater than one in $J_0(11^3)[11]$.

In [Ribet 1990], it is shown that the mod p multiplicity of a certain representation in the Jacobian of the Shimura curve derived from the rational quaternion algebra of discriminant $11 \cdot 193$ is 2; this result inspired the calculations in [Kilford 2002].

Let us finally mention that for $p = 2$ the Galois representations ρ with image equal to the dihedral group D_3 come from an elliptic curve over $\mathbb{Q}$. We observe that $D_3 = \mathrm{GL}_2(\mathbb{F}_2)$. Any S_3-extension K of the rationals can be obtained as the splitting field of an irreducible integral polynomial $f = X^3 + aX + b$. The 2-torsion of the elliptic curve $E : Y^2 = f$ consists precisely of the three roots of f and the point at infinity. So, the field generated over $\mathbb{Q}$ by the 2-torsion of E is K.

1.2 New results

Using the modular symbols algorithm over finite fields with an improved stop criterion (see Section 3), we performed computations in MAGMA concerning the Gorenstein defect of Hecke algebras of cuspidal modular forms of prime weights p at maximal ideals of residue characteristic p in the case of Theorem 1.3. All of our 384 examples have Gorenstein defect equal to 2 and hence their multiplicity is 2.

We formulate part of our computational findings as a theorem.

Theorem 1.8 *For every prime $p < 100$ there exists a prime $N \neq p$ and a Dirichlet character χ such that the Hecke algebra $\mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_p(N, \chi))$ has Gorenstein defect 2 at some maximal ideal $\mathfrak{m}$ of residue characteristic p. The corresponding Galois representation $\rho_{\mathfrak{m}}$ appears with multiplicity two on the $\mathfrak{m}$-torsion of the Jacobian $J_1(Np)_{\mathbb{Q}}(\overline{\mathbb{Q}})$ if p is odd, respectively $J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})$ if $p = 2$.*

Our computational results are discussed in more detail in Section 4.

1.3 A question

Question 1.9 *Let p be a prime. Let f be a normalised cuspidal modular eigenform of weight p, prime level $N \neq p$ for some Dirichlet character χ. Let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be the modular Galois representation attached to f. We assume that ρ_f is irreducible and unramified at p and that $\rho_f(\mathrm{Frob}_p)$ is a scalar matrix.*

Write $\mathbb{T}_{\mathbb{F}}$ for $\mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_p(N, \chi))$. Recall that this notation stands for the tensor product over $\mathbb{Z}[\chi]$ of a residue field $\mathbb{F}/\mathbb{F}_p$ of $\mathbb{Z}[\chi]$ by the $\mathbb{Z}[\chi]$-algebra generated inside the endomorphism algebra of $S_p(N, \chi)$ by the Hecke operators and by the diamond operators. Let $\mathfrak{m}$ be the maximal ideal of $\mathbb{T}_{\mathbb{F}}$ corresponding to f.

Is the Gorenstein defect of the Hecke algebra $\mathbb{T}_{\mathbb{F}}$ localised at $\mathfrak{m}$, denoted by $\mathbb{T}_{\mathfrak{m}}$, always equal to 2?

Equivalently, is the multiplicity of the Galois representation attached to f always equal to 2?

This question was also raised both by Kevin Buzzard and James Parson in communications to the authors.

2 Relation between multiplicity and Gorenstein defect

In this section we collect results, some of which are well-known, on the multiplicity of Galois representations, the Gorenstein defect and relations between the two. Whereas the mod p modular symbols algorithm naturally computes mod p modular forms (see Section 3), this rather geometrical section uses (mostly in the references) the theory of Katz modular forms over finite fields (see e.g. [Edixhoven 1997]). If $N \geq 5$ and $k \geq 2$, the Hecke algebra $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N)))$ is both the Hecke algebra of mod p cusp forms of weight k on $\Gamma_1(N)$ and the Hecke algebra of the corresponding Katz cusp forms over $\mathbb{F}_p$. However, in the presence of a Dirichlet character $\mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_k(N,\chi))$ only has an interpretation as the Hecke algebra of the corresponding mod p cusp forms and there may be differences with the respective Hecke algebra for Katz forms (see Carayol's Lemma, Prop. 1.10 of [Edixhoven 1997]).

We start with the well-known result in weight 2 (see e.g. [Mazur 1977], Lemma 15.1, or [Tilouine 1997]) that multiplicity one implies that the corresponding local Hecke factor is a Gorenstein ring.

Proposition 2.1 *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T} := \mathbb{T}_{\mathbb{Z}}(S_2(\Gamma_1(N)))$ of residue characteristic p which may divide N. Denote by $\widetilde{\mathfrak{m}}$ the image of $\mathfrak{m}$ in $\mathbb{T}_{\mathbb{F}_p} := \mathbb{T}\otimes_{\mathbb{Z}}\mathbb{F}_p = \mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(N)))$. Suppose that the Galois representation $\rho_{\mathfrak{m}}$ is irreducible and satisfies multiplicity one (see Section 1).*

Then as $\mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}$-modules one has

$$J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[p]_{\widetilde{\mathfrak{m}}} \cong \mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}} \oplus \mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}$$

and the localisations $\mathbb{T}_{\mathfrak{m}}$ and $\mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}$ are Gorenstein rings. Similar results hold if one replaces $\Gamma_1(N)$ and $J_1(N)$ by $\Gamma_0(N)$ and $J_0(N)$.

Proof. For the proof we have to pass to $\mathbb{T}_{\mathbb{Z}_p} = \mathbb{T}_{\mathbb{Z}}\otimes_{\mathbb{Z}}\mathbb{Z}_p$. We also denote by $\mathfrak{m}$ the maximal ideal in $\mathbb{T}_{\mathbb{Z}_p}$ that corresponds to $\mathfrak{m}$. Let V be the $\mathfrak{m}$-part of the p-Tate module of $J_1(N)_{\mathbb{Q}}$. Multiplicity one implies that $V/\mathfrak{m}V$ is a 2-dimensional $\mathbb{T}/\mathfrak{m} = \mathbb{T}_{\mathbb{Z}_p}/\mathfrak{m} = \mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}/\widetilde{\mathfrak{m}}$-vector space, since

$$V/\mathfrak{m}V \cong (V/pV)/\widetilde{\mathfrak{m}} \cong (J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[p])/\widetilde{\mathfrak{m}} \cong (J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[p])^{\vee}/\widetilde{\mathfrak{m}} \cong (J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[\mathfrak{m}])^{\vee},$$

where the self-duality comes from the modified Weil pairing which respects the Hecke action (see e.g. [Tilouine 1987], Lemme 4.1, or [Gross 1990], p. 485). Nakayama's Lemma hence implies that V is a $\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}}$-module of rank 2. As one knows that $V\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ is a $\mathbb{T}_{\mathfrak{m}}\otimes\mathbb{Q}_p$-module of rank 2, it follows that V is a free $\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}}$-module of rank 2, whence $J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[p]_{\widetilde{\mathfrak{m}}}$ is a free $\mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}$-module of rank 2.

Taking the $\widetilde{\mathfrak{m}}$-kernel gives $J_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})[\mathfrak{m}] = (\mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}[\widetilde{\mathfrak{m}}])^2$, whence the Gorenstein defect is zero. In the Γ_0-situation, the same proof holds. □

In the so-called ordinary case, we have the following precise relationship between the multiplicity and the Gorenstein defect, which was suggested to us by Kevin Buzzard. A proof can be found in [Wiese 2007a], Corollaries 2.3 and 4.2.

Proposition 2.2 *Suppose $p \nmid N$ and let $M = N$ or $M = Np$. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_{\mathbb{Z}}(S_2(\Gamma_1(M)))$ of residue characteristic p and assume that $\mathfrak{m}$ is ordinary, i.e. that the p-th Hecke operator T_p is not in $\mathfrak{m}$. Assume also that $\rho_{\mathfrak{m}}$ is irreducible. Denote by $\widetilde{\mathfrak{m}}$ the image of $\mathfrak{m}$ in $\mathbb{T}_{\mathbb{F}_p} := \mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(M)))$. Then the following statements hold:*

(a) There is the exact sequence

$$0 \to \mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}} \to J_1(M)(\overline{\mathbb{Q}})[p]_{\widetilde{\mathfrak{m}}} \to \mathbb{T}^{\vee}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}} \to 0$$

of $\mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}$-modules, where the dual is the $\mathbb{F}_p$-linear dual.

(b) If d is the Gorenstein defect of $\mathbb{T}_{\mathbb{F}_p,\widetilde{\mathfrak{m}}}$ and r is the multiplicity of $\rho_{\mathfrak{m}}$, then the relation

$$d = 2r - 2$$

holds.

We now establish a relation between mod p Hecke algebras of weights $3 \le k \le p+1$ for levels N not divisible by p with Hecke algebras of weight 2 and level Np. It is needed in order to compare the Hecke algebras in higher weight to those acting on the p-torsion of Jacobians and thus to make a link to the multiplicity of the attached Galois representations.

Proposition 2.3 *Let $N \ge 5$, $p \nmid N$ and $3 \le k \le p+1$. Let $\mathfrak{m}$ be a maximal ideal of the mod p Hecke algebra $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N))$. Then there exists a maximal ideal $\mathfrak{m}_2$ of $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(Np))$ and a natural surjection*

$$\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(Np))_{\mathfrak{m}_2} \twoheadrightarrow \mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N))_{\mathfrak{m}}.$$

If $\mathfrak{m}$ is ordinary ($T_p \notin \mathfrak{m}$), this surjection is an isomorphism.

Proof. From Sections 5 and 6 of [Wiese 2007b], whose notation we adopt for this proof, one obtains without difficulty the commutative diagram of Hecke algebras:

$$\begin{array}{ccccc}
\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(Np))_{\mathfrak{m}_2} & \twoheadrightarrow & \mathbb{T}_{\mathbb{F}_p}(J_1(Np)_{\mathbb{Q}}(\overline{\mathbb{Q}})[p])_{\mathfrak{m}_2} & \twoheadrightarrow & \mathbb{T}_{\mathbb{F}_p}(H^1(\Gamma_1(N),V_{k-2}(\mathbb{F}_p)))_{\mathfrak{m}} \\
\| & & \downarrow & & \uparrow \\
\mathbb{T}_{\mathbb{Z}_p\to\mathbb{F}_p}(L)_{\mathfrak{m}_2} & \twoheadrightarrow & \mathbb{T}_{\mathbb{F}_p}(\overline{L})_{\mathfrak{m}_2} & \twoheadrightarrow & \mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N))_{\mathfrak{m}}.
\end{array}$$

The claimed surjection can be read off. The ideal $\mathfrak{m}_2$ can be explicitly defined as the preimage of $\mathfrak{m}$ (before localisation). Then it necessarily holds that $\langle a\rangle_p - a^{k-2}$ is in $\mathfrak{m}_2$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$. In the

ordinary situation, Proposition 2.2 shows that the upper left horizontal arrow is in fact an isomorphism. That also the upper right horizontal arrow is an isomorphism is explained in [Wiese 2007b]. The result follows. □

As pointed out by one of the referees, the result in the ordinary case was first obtained in [Hida 1981]. In the next proposition we compare Hecke algebras for spaces of modular forms on $\Gamma_1(N)$ to those of the same level and weight, but with a Dirichlet character.

Proposition 2.4 *Let $N \geq 5$, $k \geq 2$ and let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. Let $f \in S_k(N,\chi) \subset S_k(\Gamma_1(N))$ be a normalised Hecke eigenform. Let further $\mathfrak{m}_{\overline{\chi}}$ be the maximal ideal in $\mathbb{T}_{\mathbb{F}}^{\overline{\chi}} := \mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_k(N,\chi))$ and $\mathfrak{m}$ the one in $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N)))$ of residue characteristic p for $p \nmid N$ belonging to f. If $k = 2$, suppose additionally that $\rho_{\mathfrak{m}}$ is irreducible. If $p = 2$, suppose that $\rho_{\mathfrak{m}}$ is not induced from $\mathbb{Q}(\sqrt{-1})$, and if $p = 3$, suppose that $\rho_{\mathfrak{m}}$ is not induced from $\mathbb{Q}(\sqrt{-3})$.*

Then the Gorenstein defects of $\mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_k(N,\chi))_{\mathfrak{m}_{\overline{\chi}}}$ and $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_k(\Gamma_1(N)))_{\mathfrak{m}}$ are equal.

Proof. Write $\Delta := (\mathbb{Z}/N\mathbb{Z})^\times$ and let Δ_p be its p-Sylow subgroup. Let $\overline{\chi} : \Delta \to \mathbb{F}^\times$ be the reduction of χ obtained by composing χ with $\mathbb{Z}[\chi] \to \mathbb{F}$. As the Gorenstein defect is invariant under base extension, it is no loss to work with $\mathbb{T}_{\mathbb{F}} := \mathbb{T}_{\mathbb{Z}\to\mathbb{F}}(S_k(\Gamma_1(N)))$. We still write $\mathfrak{m}$ for the maximal ideal in $\mathbb{T}_{\mathbb{F}}$ belonging to f. Note that $\langle\delta\rangle - \overline{\chi}(\delta) \in \mathfrak{m}$ for all $\delta \in \Delta$.

We let Δ act on $\mathbb{T}_{\mathbb{F}}$ via the diamond operators and we let $\mathbb{F}^{\overline{\chi}}$ be a copy of $\mathbb{F}$ with Δ-action through the inverse of $\overline{\chi}$. We have

$$(\mathbb{T}_{\mathbb{F},\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})_\Delta = (\mathbb{T}_{\mathbb{F},\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})/(1-\delta|\delta \in \Delta) \cong \mathbb{T}_{\mathbb{F},\mathfrak{m}_{\overline{\chi}}}^{\overline{\chi}},$$

which one obtains by considering the duals, identifying Katz cusp forms with mod p ones on $\Gamma_1(N)$ and applying Carayol's Lemma ([Edixhoven 1997], Prop. 1.10). For the case $k = 2$, we should point the reader to the correction at the end of the introduction to [Edixhoven 2006]. However, the statement still holds after localisation at maximal ideals corresponding to irreducible representations. Moreover, the equality $(\mathbb{T}_{\mathbb{F},\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})^\Delta = \mathbb{T}_{\mathbb{F},\mathfrak{m}}[\langle\delta\rangle - \overline{\chi}(\delta)|\delta \in \Delta]$ holds by definition.

Now Lemma 7.3 of [Wiese 2007b] tells us that the localisation at $\mathfrak{m}$ of the $\mathbb{F}$-vector space of Katz cusp forms of weight k on $\Gamma_1(N)$ over $\mathbb{F}$ is a free $\mathbb{F}[\Delta_p]$-module. Note that the standing hypothesis $k \leq p+1$ of Section 7 of [Wiese 2007b] is not used in the proof of that lemma and see also [Wiese 2007b], Remark 7.5. From an elementary calculation one now obtains that $N_\Delta = \sum_{\delta\in\Delta} \delta$ induces an isomorphism

$$(\mathbb{T}_{\mathbb{F}_\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})_\Delta \xrightarrow{N_\Delta} (\mathbb{T}_{\mathbb{F}_\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})^\Delta.$$

We now take the $\mathfrak{m}_{\overline{\chi}}$-kernel on both sides and obtain

$$\mathbb{T}_{\mathbb{F},\mathfrak{m}_{\overline{\chi}}}^{\overline{\chi}}[\mathfrak{m}_{\overline{\chi}}] \cong (\mathbb{T}_{\mathbb{F},\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})_\Delta[\mathfrak{m}_{\overline{\chi}}] \cong (\mathbb{T}_{\mathbb{F},\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})_\Delta[\mathfrak{m}] \cong (\mathbb{T}_{\mathbb{F},\mathfrak{m}} \otimes_{\mathbb{F}} \mathbb{F}^{\overline{\chi}})^\Delta[\mathfrak{m}] = \mathbb{T}_{\mathbb{F},\mathfrak{m}}[\mathfrak{m}].$$

This proves that the two Gorenstein defects are indeed equal. □

The Gorenstein defect that we calculate on the computer is the number d of the following corollary, which relates it to the multiplicity of a Galois representation.

Corollary 2.5 *Let p be a prime, $N \geq 5$ an integer such that $p \nmid N$, k an integer satisfying $2 \leq k \leq p$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character. Let $f \in S_k(N, \chi)$ be a normalised Hecke eigenform. Let further $\mathfrak{m}$ denote the maximal ideal in $\mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_k(N,\chi))$ belonging to f. Suppose that $\mathfrak{m}$ is ordinary and that $\rho_\mathfrak{m}$ is irreducible and not induced from $\mathbb{Q}(\sqrt{-1})$ (if $p = 2$) and not induced from $\mathbb{Q}(\sqrt{-3})$ (if $p = 3$). We define d to be the Gorenstein defect of $\mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_k(N,\chi))_\mathfrak{m}$ and r to be the multiplicity of $\rho_\mathfrak{m}$.*

Then the equality $d = 2r - 2$ holds. □

We include the following proposition because it establishes equality of the two different notions of multiplicities of Galois representations in the case of the trivial character.

Proposition 2.6 *Let $N \geq 1$ and $p \nmid N$ and $f \in S_2(\Gamma_0(N)) \subseteq S_2(\Gamma_1(N))$ be a normalised Hecke eigenform belonging to maximal ideals $\mathfrak{m}_0 \subseteq \mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_0(N)))$ and $\mathfrak{m}_1 \subseteq \mathbb{T}_{\mathbb{Z}\to\mathbb{F}_p}(S_2(\Gamma_1(N)))$ of residue characteristic p. Suppose that $\rho_{\mathfrak{m}_0} \cong \rho_{\mathfrak{m}_1}$ is irreducible.*

Then the multiplicity of $\rho_{\mathfrak{m}_1}$ on $J_1(N)_\mathbb{Q}(\overline{\mathbb{Q}})[p]$ is equal to the multiplicity of $\rho_{\mathfrak{m}_0}$ on $J_0(N)_\mathbb{Q}(\overline{\mathbb{Q}})[p]$. Thus, if $p > 2$, this multiplicity is equal to one by Theorem 1.2.

Proof. Let $\Delta := (\mathbb{Z}/N\mathbb{Z})^\times$. We first remark that one has the isomorphism

$$J_0(N)_\mathbb{Q}(\overline{\mathbb{Q}})[p]_{\mathfrak{m}_0} \cong \left((J_1(N)_\mathbb{Q}(\overline{\mathbb{Q}})[p])^\Delta\right)_{\mathfrak{m}_0},$$

which one can for example obtain by comparing with the parabolic cohomology with $\mathbb{F}_p$-coefficients of the modular curves $Y_0(N)$ and $Y_1(N)$. Taking the $\mathfrak{m}_0$-kernel yields

$$J_0(N)_\mathbb{Q}(\overline{\mathbb{Q}})[\mathfrak{m}_0] \cong J_1(N)_\mathbb{Q}(\overline{\mathbb{Q}})[\mathfrak{m}_1],$$

since $\mathfrak{m}_1$ contains $\langle\delta\rangle - 1$ for all $\delta \in \Delta$. □

3 Modular Symbols and Hecke Algebras

The aim of this section is to present the algorithm that we use for the computations of local factors of Hecke algebras of mod p modular forms. It is based on mod p modular symbols which have been implemented in MAGMA [Bosma et al. 1997] by William Stein.

The bulk of this section deals with proving the main advance, namely a stop criterion (Corollary 3.8), which in practice greatly speeds up the computations in comparison with "standard" implementations, as it allows us to work with many fewer Hecke operators than indicated by the theoretical Sturm bound (Proposition 3.10). We shall list results proving that the stop criterion is attained in many cases. However, the stop criterion does not depend on them, in the sense that it being attained is equivalent to a proof that the algebra it outputs is equal to a direct factor of a Hecke algebra of mod p modular forms.

Whereas for Section 2 the notion of Katz modular forms seems the right one, the present section works entirely with mod p modular forms, the definition of which is also recalled. This is very natural, since all results in this section are based on a comparison with the characteristic zero theory.

3.1 Mod p modular forms and modular symbols

Mod p modular forms

Let us for the time being fix integers $N \geq 1$ and $k \geq 2$, as well as a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi(-1) = (-1)^k$. Let $M_k(N, \chi)$ be the space of holomorphic modular forms for $\Gamma_1(N)$, Dirichlet character χ, and weight k. It decomposes as a direct sum (orthogonal direct sum with respect to the Petersson inner product) of its cuspidal subspace $S_k(N, \chi)$ and its Eisenstein subspace $\mathrm{Eis}_k(N, \chi)$. As before, we let $\mathcal{O} = \mathbb{Z}[\chi]$. Moreover, we let $\mathfrak{P}$ be a maximal ideal of $\mathcal{O}$ above p with residue field $\mathbb{F}$ and $\widehat{\mathcal{O}}$ be the completion of $\mathcal{O}$ at $\mathfrak{P}$. Furthermore, let $K = \mathbb{Q}_p(\chi)$ be the field of fractions of $\widehat{\mathcal{O}}$ and $\bar{\chi}$ be χ followed by the natural projection $\mathcal{O} \twoheadrightarrow \mathbb{F}$.

Denote by $M_k(N, \chi\,;\, \mathcal{O})$ the sub-$\mathcal{O}$-module generated by those modular forms whose (standard) q-expansion has coefficients in $\mathcal{O}$. It follows from the q-expansion principle that

$$M_k(N, \chi\,;\, \mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}\big(\mathbb{T}_{\mathcal{O}}(M_k(N, \chi)), \mathcal{O}\big)$$

and that hence $M_k(N, \chi\,;\, \mathcal{O}) \otimes_{\mathcal{O}} \mathbb{C} \cong M_k(N, \chi)$. We put

$$M_k(N, \bar{\chi}\,;\, \mathbb{F}) := M_k(N, \chi\,;\, \mathcal{O}) \otimes_{\mathcal{O}} \mathbb{F} \cong \mathrm{Hom}_{\mathbb{F}}\big(\mathbb{T}_{\mathcal{O}}(M_k(N, \chi)), \mathbb{F}\big)$$

and call the elements of this space *mod p modular forms*. The Hecke algebra $\mathbb{T}_{\mathcal{O}}(M_k(N, \chi))$ acts naturally and it follows that $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(M_k(N, \chi)) \cong \mathbb{T}_{\mathbb{F}}(M_k(N, \chi\,;\, \mathbb{F}))$. Similar statements hold for the cuspidal and the Eisenstein subspaces and we use similar notations.

We call a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(M_k(N, \chi\,;\, \mathcal{O})$ (respectively, the corresponding maximal ideal of $\mathbb{T}_{\mathcal{O}\to\widehat{\mathcal{O}}}(M_k(N, \chi\,;\, \mathcal{O}))$) *non-Eisenstein* if and only if

$$S_k(N, \bar{\chi}\,;\, \mathbb{F})_{\mathfrak{m}} \cong M_k(N, \bar{\chi}\,;\, \mathbb{F})_{\mathfrak{m}}.$$

Otherwise, we call $\mathfrak{m}$ *Eisenstein*.

We now include a short discussion of minimal and maximal primes, in view of Proposition 3.5. Write $\mathbb{T}_{\widehat{\mathcal{O}}}$ for $\mathbb{T}_{\mathcal{O}\to\widehat{\mathcal{O}}}(S_k(N, \chi))$. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_{\widehat{\mathcal{O}}}$. It corresponds to a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F})$-conjugacy class of normalised eigenforms in $S_k(N, \bar{\chi}\,;\, \mathbb{F})$. That means for each $n \in \mathbb{N}$ that the minimal polynomial of T_n acting on $S_k(N, \bar{\chi}\,;\, \mathbb{F})_{\mathfrak{m}}$ is equal to a power of the minimal polynomial of the coefficient a_n of each member of the conjugacy class. Similarly, a minimal prime $\mathfrak{p}$ of $\mathbb{T}_{\mathcal{O}\to\widehat{\mathcal{O}}}(S_k(N, \chi))$ corresponds to a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$-conjugacy class of normalised eigenforms in $S_k(N, \chi\,;\, \mathcal{O}) \otimes_{\mathcal{O}} K$.

Suppose that $\mathfrak{m}$ contains minimal primes $\mathfrak{p}_i$ for $i = 1, \ldots, r$. Then the normalised eigenforms corresponding to the $\mathfrak{p}_i$ are congruent to one another modulo a prime above p. Conversely, any congruence arises in this way. Thus, a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$ is Eisenstein if and only if it contains a minimal prime corresponding to a conjugacy class of Eisenstein series. As it is the reduction of a reducible representation, the mod p Galois representation corresponding to an Eisenstein prime is reducible. It should be possible to show the converse, too.

Modular symbols

We now recall the modular symbols formalism and prove two useful results on base change and torsion. The main references for the definitions are [Stein 2007] and [Wiese 2005].

Let R be a ring, $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ a subgroup and V a left $R[\Gamma]$-module. Recall that $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ is the set of cusps of $\mathrm{SL}_2(\mathbb{Z})$, which carries a natural $\mathrm{SL}_2(\mathbb{Z})$-action via fractional linear transformations. We define the R-modules

$$\mathcal{M}_R := R[\{\alpha, \beta\} | \alpha, \beta \in \mathbb{P}^1(\mathbb{Q})] / \langle \{\alpha, \alpha\}, \{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} | \alpha, \beta, \gamma \in \mathbb{P}^1(\mathbb{Q}) \rangle$$

and $\mathcal{B}_R := R[\mathbb{P}^1(\mathbb{Q})]$. They are connected via the *boundary map* $\delta : \mathcal{M}_R \to \mathcal{B}_R$ which is given by $\{\alpha, \beta\} \mapsto \beta - \alpha$. Both are equipped with the natural left Γ-actions. Also let $\mathcal{M}_R(V) := \mathcal{M}_R \otimes_R V$ and $\mathcal{B}_R(V) := \mathcal{B}_R \otimes_R V$ with the left diagonal Γ-action. We call the Γ-coinvariants

$$\mathcal{M}_R(\Gamma, V) := \mathcal{M}_R(V)_\Gamma = \mathcal{M}_R(V) / \langle (x - gx) | g \in \Gamma, x \in \mathcal{M}_R(V) \rangle$$

the space of (Γ, V)*-modular symbols.* Furthermore, *the space of* (Γ, V)*-boundary symbols* is defined as the Γ-coinvariants

$$\mathcal{B}_R(\Gamma, V) := \mathcal{B}_R(V)_\Gamma = \mathcal{B}_R(V) / \langle (x - gx) | g \in \Gamma, x \in \mathcal{B}_R(V) \rangle.$$

The boundary map δ induces the *boundary map* $\mathcal{M}_R(\Gamma, V) \to \mathcal{B}_R(\Gamma, V)$. Its kernel is denoted by $\mathcal{CM}_R(\Gamma, V)$ and is called *the space of cuspidal* (Γ, V)*-modular symbols.*

Let now $N \geq 1$ and $k \geq 2$ be integers and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ be a character, i.e. a group homomorphism, such that $\chi(-1) = (-1)^k$ in R. Write $V_{k-2}(R)$ for the homogeneous polynomials of degree $k-2$ over R in two variables, equipped with the natural $\Gamma_0(N)$-action. Denote by $V_{k-2}^\chi(R)$ the tensor product $V_{k-2}(R) \otimes_R R^\chi$ for the diagonal $\Gamma_0(N)$-action which on R^χ comes from the isomorphism $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ given by sending $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to d followed by χ^{-1}.

We use the notation $\mathcal{M}_k(N, \chi\,;\, R)$ for $\mathcal{M}(\Gamma_0(N), V_{k-2}^\chi(R))$, as well as similarly for the boundary and the cuspidal spaces. The natural action of the matrix $\eta = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ gives an involution on all of these spaces. We will denote by the superscript $^+$ the subspace invariant under this involution, and by the superscript $^-$ the anti-invariant one. On all modules discussed so far one has Hecke operators T_n for all $n \in \mathbb{N}$ and diamond operators. For a definition see [Stein 2007].

Lemma 3.1 *Let R, Γ and V as above and let $R \to S$ be a ring homomorphism. Then*

$$\mathcal{M}(\Gamma, V) \otimes_R S \cong \mathcal{M}(\Gamma, V \otimes_R S).$$

Proof. This follows immediately from the fact that tensoring and taking coinvariants are both right exact. □

Proposition 3.2 *Let R be a local integral domain of characteristic zero with principal maximal ideal $\mathfrak{m} = (\pi)$ and residue field $\mathbb{F}$ of characteristic p. Also let $N \geq 1$, $k \geq 2$ be integers and*

$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ *a character such that* $\chi(-1) = (-1)^k$*. Suppose (i) that* $p \geq 5$ *or (ii) that* $p = 2$ *and* N *is divisible by a prime which is* 3 *modulo* 4 *or by* 4 *or (iii) that* $p = 3$ *and* N *is divisible by a prime which is* 2 *modulo* 3 *or by* 9*. Then the following statements hold:*

(a) If $k \geq 3$*, then* $\mathcal{M}_k(N, \chi\,;\, R)[\pi] = \left(V_{k-2}^{\chi}(\mathbb{F})\right)^{\Gamma_0(N)}$.

(b) If $k = 2$ *or if* $3 \leq k \leq p + 2$ *and* $p \nmid N$*, then* $\mathcal{M}_k(N, \chi\,;\, R)[\pi] = 0$.

Proof. The conditions assure that the group $\Gamma_0(N)$ does not have any stabiliser of order $2p$ for its action on the upper half plane. Hence, by [Wiese 2005], Theorem 6.1, the modular symbols space $\mathcal{M}_k(N, \chi\,;\, R)$ is isomorphic to $H^1(\Gamma_0(N), V_{k-2}^{\chi}(R))$. The arguments are now precisely those of the beginning of the proof of [Wiese 2007b], Proposition 2.6. □

Hecke algebras of modular symbols and the Eichler-Shimura isomorphism

From Lemma 3.1 one deduces a natural surjection

$$\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(\mathcal{M}_k(N, \chi\,;\, \mathcal{O})) \twoheadrightarrow \mathbb{T}_{\mathbb{F}}(\mathcal{M}_k(N, \bar{\chi}\,;\, \mathbb{F})). \tag{3.1}$$

In the same way, one also obtains

$$\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N, \chi\,;\, \mathcal{O})) \twoheadrightarrow \mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N, \chi\,;\, \mathcal{O})/\text{torsion}) \cong \mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N, \chi\,;\, \mathbb{C})), \tag{3.2}$$

where one uses for the isomorphism that the Hecke operators are already defined over $\mathcal{O}$. Similar statements hold for the cuspidal subspace.

We call a maximal prime $\mathfrak{m}$ of $\mathbb{T}_{\mathcal{O}\to\widehat{\mathcal{O}}}(\mathcal{M}_k(N, \chi\,;\, \mathcal{O}))$ (respectively the corresponding prime of $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(\mathcal{M}_k(N, \chi\,;\, \mathcal{O}))$) *non-torsion* if

$$\mathcal{M}_k(N, \chi\,;\, \widehat{\mathcal{O}})_{\mathfrak{m}} \cong (\mathcal{M}_k(N, \chi\,;\, \widehat{\mathcal{O}})/\text{torsion})_{\mathfrak{m}}.$$

This is equivalent to the height of $\mathfrak{m}$ being 1. Proposition 3.2 tells us some cases in which all primes are non-torsion.

Theorem 3.3 (Eichler-Shimura) *There are isomorphisms respecting the Hecke operators*

(a) $M_k(N, \chi) \oplus S_k(N, \chi)^\vee \cong \mathcal{M}_k(N, \chi\,;\, \mathbb{C})$,

(b) $S_k(N, \chi) \oplus S_k(N, \chi)^\vee \cong \mathcal{CM}_k(N, \chi\,;\, \mathbb{C})$,

(c) $S_k(N, \chi) \cong \mathcal{CM}_k(N, \chi\,;\, \mathbb{C})^+$.

Proof. Parts (a) and (b) are [Diamond and Im 1995], Theorem 12.2.2, together with the comparison of [Wiese 2005], Theorem 6.1. We use that the space of anti-holomorphic cusp forms is dual to the space of holomorphic cusp forms. Part (c) is a direct consequence of (b). □

Corollary 3.4 *There are isomorphisms*

$$\mathbb{T}_{\mathcal{O}}(S_k(N, \chi)) \cong \mathbb{T}_{\mathcal{O}}(\mathcal{CM}_k(N, \chi\,;\, \mathbb{C})) \cong \mathbb{T}_{\mathcal{O}}(\mathcal{CM}_k(N, \chi\,;\, \mathbb{C})^+),$$

given by sending T_n *to* T_n *for all positive* n*.* □

3.2 The stop criterion

Although it is impossible to determine a priori the dimension of the local factor of the Hecke algebra associated with a given modular form mod p, Corollary 3.8 implies that the computation of Hecke operators can be stopped when the algebra generated has reached a certain dimension that is computed along the way. This criterion has turned out to be extremely useful and has made possible some of our computations which would not have been feasible using the Hecke bound naively. See Section 4 for a short discussion of this issue.

Some commutative algebra

We collect some useful statements from commutative algebra, which will be applied to Hecke algebras in the sequel.

Proposition 3.5 *Let R be an integral domain of characteristic zero which is a finitely generated $\mathbb{Z}$-module. Write $\widehat{R}$ for the completion of R at a maximal ideal of R and denote by $\mathbb{F}$ the residue field and by K the fraction field of $\widehat{R}$. Let furthermore A be a commutative R-algebra which is finitely generated as an R-module. For any ring homomorphism $R \to S$ write A_S for $A \otimes_R S$. Then the following statements hold.*

(a) The Krull dimension of $A_{\widehat{R}}$ is less than or equal to 1. The maximal ideals of $A_{\widehat{R}}$ correspond bijectively under taking pre-images to the maximal ideals of $A_{\mathbb{F}}$. Primes $\mathfrak{p}$ of height 0 which are contained in a prime of height 1 of $A_{\widehat{R}}$ are in bijection with primes of A_K under extension (i.e. $\mathfrak{p}A_K$), for which the notation $\mathfrak{p}^e$ will be used.

Under these correspondences, one has $A_{\mathbb{F},\mathfrak{m}} \cong A_{\widehat{R},\mathfrak{m}} \otimes_{\widehat{R}} \mathbb{F}$ and $A_{K,\mathfrak{p}^e} \cong A_{\widehat{R},\mathfrak{p}}$.

(b) The algebra $A_{\widehat{R}}$ decomposes as

$$A_{\widehat{R}} \cong \prod_{\mathfrak{m}} A_{\widehat{R},\mathfrak{m}},$$

where the product runs over the maximal ideals $\mathfrak{m}$ of $A_{\widehat{R}}$.

(c) The algebra $A_{\mathbb{F}}$ decomposes as

$$A_{\mathbb{F}} \cong \prod_{\mathfrak{m}} A_{\mathbb{F},\mathfrak{m}},$$

where the product runs over the maximal ideals $\mathfrak{m}$ of $A_{\mathbb{F}}$.

(d) The algebra A_K decomposes as

$$A_K \cong \prod_{\mathfrak{p}} A_{K,\mathfrak{p}^e} \cong \prod_{\mathfrak{p}} A_{\widehat{R},\mathfrak{p}},$$

where the products run over the minimal prime ideals $\mathfrak{p}$ of $A_{\widehat{R}}$ which are contained in a prime ideal of height 1.

Proof. As $A_{\widehat{R}}$ is a finitely generated $\widehat{R}$-module, $A_{\widehat{R}}/\mathfrak{p}$ with a prime $\mathfrak{p}$ is an integral domain which is a finitely generated $\widehat{R}$-module. Hence, it is either a finite field or a finite extension of $\widehat{R}$. This proves that the height of $\mathfrak{p}$ is less than or equal to 1. The correspondences and the isomorphisms of Part (a) are easily verified. The decompositions in Parts (b) and (c) hold, since $\widehat{R}$ is Henselian and hence any finite algebra is the product of its localisations. Part (d) follows by tensoring (b) over $\widehat{R}$ with K. □

Similar decompositions for A-modules are derived by applying the idempotents of the decompositions of Part (b).

Proposition 3.6 *Assume the set-up of Proposition 3.5 and let M, N be A-modules which as R-modules are free of finite rank. Suppose that*

(a) $M \otimes_R \mathbb{C} \cong N \otimes_R \mathbb{C}$ as $A \otimes_R \mathbb{C}$-modules, or

(b) $M \otimes_R \bar{K} \cong N \otimes_R \bar{K}$ as $A \otimes_R \bar{K}$-modules.

Then for all prime ideals $\mathfrak{m}$ of $A_{\mathbb{F}}$ corresponding to height 1 primes of $A_{\widehat{R}}$ the equality

$$\dim_{\mathbb{F}}(M \otimes_R \mathbb{F})_{\mathfrak{m}} = \dim_{\mathbb{F}}(N \otimes_R \mathbb{F})_{\mathfrak{m}}$$

holds.

Proof. As for A, we also write M_K for $M \otimes_R K$ and similarly for N and $\widehat{R}$, $\mathbb{F}$, etc. By choosing an isomorphism $\mathbb{C} \cong \bar{K}$, it suffices to prove Part (b). Using Proposition 3.5, Part (d), the isomorphism $M \otimes_R \bar{K} \cong N \otimes_R \bar{K}$ can be rewritten as

$$\bigoplus_{\mathfrak{p}} (M_{K,\mathfrak{p}^e} \otimes_K \bar{K}) \cong \bigoplus_{\mathfrak{p}} (N_{K,\mathfrak{p}^e} \otimes_K \bar{K}),$$

where the sums run over the minimal primes $\mathfrak{p}$ of $A_{\widehat{R}}$ which are properly contained in a maximal prime. Hence, an isomorphism $M_{K,\mathfrak{p}^e} \otimes_K \bar{K} \cong N_{K,\mathfrak{p}^e} \otimes_K \bar{K}$ exists for each $\mathfrak{p}$. Since for each maximal ideal $\mathfrak{m}$ of $A_{\widehat{R}}$ of height 1 we have by Proposition 3.5

$$M_{\widehat{R},\mathfrak{m}} \otimes_{\widehat{R}} K \cong \bigoplus_{\mathfrak{p} \subseteq \mathfrak{m} \text{ min.}} M_{K,\mathfrak{p}^e}$$

and similarly for N, we get

$$\begin{aligned} \dim_{\mathbb{F}} M_{\mathbb{F},\mathfrak{m}} =& \operatorname{rk}_{\widehat{R}} M_{\widehat{R},\mathfrak{m}} = \sum_{\mathfrak{p} \subseteq \mathfrak{m} \text{ min.}} \dim_K M_{K,\mathfrak{p}^e} \\ =& \sum_{\mathfrak{p} \subseteq \mathfrak{m} \text{ min.}} \dim_K N_{K,\mathfrak{p}^e} = \operatorname{rk}_{\widehat{R}} N_{\widehat{R},\mathfrak{m}} = \dim_{\mathbb{F}} N_{\mathbb{F},\mathfrak{m}}. \end{aligned}$$

This proves the proposition. □

The stop criterion

Proposition 3.7 *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_{\mathcal{O}\to\mathbb{F}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O}))$ which is non-torsion and non-Eisenstein. Then the following statements hold:*

(a) $\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m} \cong \mathcal{M}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m}$.

(b) $2\cdot\dim_\mathbb{F} S_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m} = \dim_\mathbb{F} \mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m}$.

(c) If $p\neq 2$, then $\dim_\mathbb{F} S_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m} = \dim_\mathbb{F} \mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})^+_\mathfrak{m}$.

Proof. Part (c) follows directly from Part (b) by decomposing $\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})$ into a direct sum of its plus- and its minus-part. Statements (a) and (b) will be concluded from Proposition 3.6. More precisely, it allows us to derive from Theorem 3.3 that

$$\begin{aligned}&\dim_\mathbb{F}\big((\mathcal{M}_k(N,\chi\,;\,\mathcal{O})/\text{torsion})\otimes_\mathcal{O}\mathbb{F}\big)_\mathfrak{m}\\ =&\dim_\mathbb{F}\big(\mathrm{Eis}_k(N,\bar\chi\,;\,\mathbb{F})\oplus S_k(N,\bar\chi\,;\,\mathbb{F})\oplus S_k(N,\bar\chi\,;\,\mathbb{F})^\vee\big)_\mathfrak{m}\end{aligned}$$

and

$$\dim_\mathbb{F}\big((\mathcal{CM}_k(N,\chi\,;\,\mathcal{O})/\text{torsion})\otimes_\mathcal{O}\mathbb{F}\big)_\mathfrak{m} = 2\cdot\dim_\mathbb{F}\big(S_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m}.$$

The latter proves Part (b), since $\mathfrak{m}$ is non-torsion. As by the definition of a non-Eisenstein prime $\mathrm{Eis}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m}=0$ and again since $\mathfrak{m}$ is non-torsion, it follows that

$$\dim_\mathbb{F}\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m} = \dim_\mathbb{F}\mathcal{M}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m},$$

which implies Part (a). □

We will henceforth often regard non-Eisenstein non-torsion primes as in the proposition as maximal primes of $\mathbb{T}_\mathbb{F}(S_k(N,\bar\chi\,;\,\mathbb{F})) = \mathbb{T}_{\mathcal{O}\to\mathbb{F}}(S_k(N,\chi))$.

Corollary 3.8 (Stop Criterion) *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_\mathbb{F}(S_k(N,\bar\chi\,;\,\mathbb{F}))$ which is non-Eisenstein and non-torsion.*

(a) One has $\dim_\mathbb{F}\mathcal{M}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m} = 2\cdot\dim_\mathbb{F}\mathbb{T}_\mathbb{F}\big(\mathcal{M}_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m}$ *if and only if*

$$\mathbb{T}_\mathbb{F}\big(S_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m} \cong \mathbb{T}_\mathbb{F}\big(\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m}.$$

(b) One has $\dim_\mathbb{F}\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})_\mathfrak{m} = 2\cdot\dim_\mathbb{F}\mathbb{T}_\mathbb{F}\big(\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m}$ *if and only if*

$$\mathbb{T}_\mathbb{F}\big(S_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m} \cong \mathbb{T}_\mathbb{F}\big(\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m}.$$

(c) Assume $p\neq 2$. One has $\dim_\mathbb{F}\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})^+_\mathfrak{m} = \dim_\mathbb{F}\mathbb{T}_\mathbb{F}\big(\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m}$ *if and only if*

$$\mathbb{T}_\mathbb{F}\big(S_k(N,\bar\chi\,;\,\mathbb{F})\big)_\mathfrak{m} \cong \mathbb{T}_\mathbb{F}\big(\mathcal{CM}_k(N,\bar\chi\,;\,\mathbb{F})^+\big)_\mathfrak{m}.$$

Proof. We only prove (a), as (b) and (c) are similar. From Part (b) of Proposition 3.7 and the fact that the $\mathbb{F}$-dimension of the algebra $\mathbb{T}_{\mathbb{F}}\big(S_k(N,\bar{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}$ is equal to the one of $S_k(N,\bar{\chi}\,;\,\mathbb{F})$, as they are dual to each other, it follows that

$$2\cdot\dim_{\mathbb{F}}\mathbb{T}_{\mathbb{F}}\big(S_k(N,\bar{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}=\dim_{\mathbb{F}}\big(\mathcal{CM}_k(N,\bar{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}.$$

The result is now a direct consequence of Equations 3.1 and 3.2 and Corollary 3.4. □

Note that the first line of each statement only uses modular symbols and not modular forms, but it allows us to make statements involving modular forms. This is the aforementioned stop criterion; the computation of Hecke operators can be stopped if this equality is reached.

We now list some results concerning the validity of the equivalent statements of Corollary 3.8.

Proposition 3.9 *Let $p\geq 5$ be a prime, $k\geq 2$ and $N\geq 5$ with $p\nmid N$ integers, $\mathbb{F}$ a finite extension of $\mathbb{F}_p$, $\bar{\chi}:(\mathbb{Z}/N\mathbb{Z})^{\times}\to\mathbb{F}^{\times}$ a character and $\mathfrak{m}$ a maximal ideal of $\mathbb{T}_{\mathbb{F}}(S_k(N,\bar{\chi}\,;\,\mathbb{F}))$ which is non-Eisenstein and non-torsion. Suppose (i) that $2\leq k\leq p-1$ or (ii) that $k\in\{p,p+1\}$ and $\mathfrak{m}$ is ordinary. Then*

$$\mathbb{T}_{\mathbb{F}}\big(S_k(N,\bar{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}\cong\mathbb{T}_{\mathbb{F}}\big(\mathcal{CM}_k(N,\bar{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}\cong\mathbb{T}_{\mathbb{F}}\big(\mathcal{CM}_k(N,\bar{\chi}\,;\,\mathbb{F})^{+}\big)_{\mathfrak{m}}.$$

Proof. Using the comparison with group cohomology of [Wiese 2005], Theorem 6.1, the result follows under Assumption (i) from [Edixhoven 2006], Theorem 5.2, and is proved under Assumption (ii) in [Wiese 2007b], Corollary 6.9, for the case of the group $\Gamma_1(N)$ and no Dirichlet character. The passage to a character is established by [Wiese 2007b], Theorem 7.4 and the remark following it. One identifies the mod p modular forms appearing with corresponding Katz forms using Carayol's Lemma ([Edixhoven 1997], Prop. 1.10). □

We end this section by stating the so-called Sturm bound (also called the Hecke bound), which gives the best a priori upper bound for how many Hecke operators are needed to generate all the Hecke algebra. We only need it in our algorithm in cases in which it is theoretically not known that the stop criterion will be reached. This will enable the algorithm to detect if the Hecke algebra on modular symbols is not isomorphic to the corresponding one on cuspidal modular forms.

Proposition 3.10 (Sturm bound) *The Hecke algebra $\mathbb{T}_{\mathbb{Z}[\chi]\to\mathbb{F}}(S_k(N,\chi))$ can be generated as an algebra by the Hecke operators T_l for all primes l smaller than or equal to $\frac{kN}{12}\prod_{q|N,q\ prime}(1+\frac{1}{q})$.*

Proof. This follows from [Stein 2007], Theorem 9.18. □

3.3 Algorithm

In this section we present a sketch of the algorithm that we used for our computations. The MAGMA code, an example and a manual are published as supplemental material to this article and can be downloaded as

http://www.expmath.org/expmath/volumes/VOL/VOL.ISS/AUTHOR/HeckeAlgebra.mg,

http://www.expmath.org/expmath/volumes/VOL/VOL.ISS/AUTHOR/Example.mg,
http://www.expmath.org/expmath/volumes/VOL/VOL.ISS/AUTHOR/Manual.pdf,
respectively.
Input: Integers $N \geq 1$, $k \geq 2$, a finite field $\mathbb{F}$, a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{F}^\times$ and for each prime l less than or equal to the Sturm bound an irreducible polynomial $f_l \in \mathbb{F}[X]$.
Output: An $\mathbb{F}$-algebra.

- $M \leftarrow \mathcal{CM}_k(N, \chi\,;\, \mathbb{F})$, $l \leftarrow 1$, $L \leftarrow$ empty list.
- repeat
  - $l \leftarrow$ next prime after l.
  - Compute T_l on M and append it to the list L.
  - $M \leftarrow$ the restriction of M to the f_l-primary subspace for T_l, i.e. to the biggest subspace of M on which the minimal polynomial of T_l is a power of f_l.
  - $A \leftarrow$ the $\mathbb{F}$-algebra generated by the restrictions to M of $T_2, T_3, \ldots, T_l$.
- until $2 \cdot \dim(A) = \dim(M)$ *[the stop criterion]* or $l >$ Sturm bound.
- return A.

The f_l should, of course, be chosen as the minimal polynomials of the coefficients $a_l(f)$ of the normalised eigenform $f \in S_k(N, \chi\,;\, \bar{\mathbb{F}})$ whose local Hecke algebra one wants to compute. Suppose the algorithm stops at the prime q. If q is bigger than the Sturm bound, the equivalent conditions of Corollary 3.8 do not hold. In that case the output should be disregarded. Otherwise, A is isomorphic to a direct product of the form $\prod_{\mathfrak{m}} \mathbb{T}(S_k(N, \chi\,;\, \mathbb{F}))_{\mathfrak{m}}$ where the $\mathfrak{m}$ are those maximal ideals such that the minimal polynomials of $T_2, T_3, \ldots, T_q$ on $\mathbb{T}(S_k(N, \chi\,;\, \mathbb{F}))_{\mathfrak{m}}$ are equal to powers of $f_2, f_3, \ldots, f_q$. It can happen that A consists of more than one factor. Hence, one should still decompose A into its local factors. Alternatively, one can also replace the last line but one in the algorithm by

- until $\big((2 \cdot \dim(A) = \dim(M))$ and A is local$\big)$ or $l >$ Sturm bound,

which ensures that the output is a local algebra. In practice, one modifies the algorithm such that not for every prime l a polynomial f_l need be given, but that the algorithm takes each irreducible factor of the minimal polynomial of T_l if no f_l is known. It is also useful to choose the order how l runs through the primes. For example, one might want to take $l = p$ at an early stage with p the characteristic of $\mathbb{F}$, if one knows that this operator is needed, which is the case in all computations concerning Question 1.9.

4 Computational results

In view of Question 1.9, we produced 384 examples of odd irreducible continuous Galois representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ that are completely split at p. The results are documented in tables that

are published as supplemental material to this article:
http://www.expmath.org/expmath/volumes/VOL/VOL.ISS/AUTHOR/Tables.pdf.
The complete data, which can be processed by the MAGMA package
http://www.expmath.org/expmath/volumes/VOL/VOL.ISS/AUTHOR/HeckeAlgebra.mg,
can be downloaded at:
http://www.expmath.org/expmath/volumes/VOL/VOL.ISS/AUTHOR/data.tar.gz.

The Galois representations were created either by class field theory or from an irreducible integer polynomial whose Galois group embeds into $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$. All examples but one are dihedral; the remaining one is icosahedral. For each of these an eigenform was computed giving rise to it. The Gorenstein defect of the corresponding local Hecke algebra factor turned out always to be 2, supporting Question 1.9.

The authors preferred to proceed like this, instead of computing all Hecke algebras mod p in weight p for all "small" primes p and all "small" levels, since non-dihedral examples in which the assumptions of Question 1.9 are satisfied are very rare.

4.1 Table entries

For every computed local Hecke algebra enough data are stored to recreate it as an abstract algebra and important characteristics are listed in the tables at
http://www.expmath.org/expmath/volumes/VOL/VOL.ISS/AUTHOR/Tables.pdf.
A sample table entry is the following.

Level	Wt	ResD	Dim	EmbDim	NilO	GorDef	#Ops	#(p<HB)	Gp
5939	5	3	12	3	5	2	5	366	D_7

Each entry corresponds to the Galois conjugacy class of an eigenform f mod p with associated local Hecke algebra A. The first and the second column indicate the level and the weight of f. The latter is in all examples equal to the characteristic of the base field k (a finite extension of $\mathbb{F}_p$) of the algebra. Let $\mathfrak{m}_A$ denote the maximal ideal of A. Then ResD stands for the degree of $K = A/\mathfrak{m}_A$ over $\mathbb{F}_p$. Let us consider $A \otimes_k K$. It decomposes into a direct product of a local K-algebra B and its $\mathrm{Gal}(K/k)$-conjugates. The K-dimension of B (which is equal to the k-dimension of A) is recorded in the fourth column.

Let $\mathfrak{m}_B$ be the maximal ideal of B. The *embedding dimension* EmbDim is the K-dimension of $\mathfrak{m}_B/\mathfrak{m}_B^2$. By Nakayama's Lemma this is the minimal number of B-generators for $\mathfrak{m}_B$. The *nilpotency order* NilO is the maximal integer n such that $\mathfrak{m}_B^n$ is not the zero ideal. The column GorDef contains the Gorenstein defect of B (which is the same as the Gorenstein defect of A).

By #Ops it is indicated how many Hecke operators were used to generate the algebra A, applying the stop criterion (Corollary 3.8). This is contrasted with the number of primes smaller than the Sturm bound (Proposition 3.10, it is also called the Hecke bound), denoted by #(p<HB). One immediately observes that the stop criterion is very efficient. Whereas the Sturm bound is roughly linear in the

level, in 365 of the 384 calculated examples, less than 10 Hecke operators sufficed, in 252 examples even 5 were enough.

The final column contains the image of the mod p Galois representation attached to f as an abstract group.

4.2 Dihedral examples

All Hecke algebras except one in our tables correspond to eigenforms whose Galois representations are dihedral, since these are by far the easiest to obtain explicitly as one can use class field theory. This is explained now.

Let p be a prime and d a square-free integer which is 1 mod 4 and not divisible by p. We denote by K the quadratic field $\mathbb{Q}(\sqrt{d})$. Further we consider an unramified character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \overline{\mathbb{F}}_p{}^{\times}$ of order $n \geq 3$. We assume that its inverse χ^{-1} is equal to χ conjugated by σ, denoted χ^{σ}, for σ (a lift of) the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. The induced representation

$$\rho_{\chi} := \mathrm{Ind}_{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(\chi) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

is irreducible and its image is the dihedral group D_n of order $2n$. If l is a prime not dividing $2d$, we have $\rho_{\chi}(\mathrm{Frob}_l) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ if $\left(\frac{d}{l}\right) = -1$, and $\rho_{\chi}(\mathrm{Frob}_l) = \left(\begin{smallmatrix} \chi(\mathrm{Frob}_{\Lambda}) & 0 \\ 0 & \chi^{\sigma}(\mathrm{Frob}_{\Lambda}) \end{smallmatrix}\right)$ if $\left(\frac{d}{l}\right) = 1$ and $l\mathcal{O}_K = \Lambda\sigma(\Lambda)$. This explicit description makes it obvious that the determinant of ρ_{χ} is the Legendre symbol $l \mapsto \left(\frac{d}{l}\right)$.

Since the kernel of χ corresponds to a subfield of the Hilbert class field of K, simple computations in the class group of K allow one to determine which primes split completely. These give examples satisfying the assumptions of Question 1.9 (the Frobenius at p is the identity) if ρ_{χ} is odd, i.e. if $p = 2$ or $d < 0$.

We remark that for characters χ of odd order n the assumption $\chi^{-1} = \chi^{\sigma}$ is not a big restriction, since any character can be written as $\chi = \chi_1\chi_2$ with $\chi_1^{\sigma} = \chi_1^{-1}$ and $\chi_2^{\sigma} = \chi_2$, hence the latter descends to a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the representation ρ_{χ} is isomorphic to $\rho_{\chi_1} \otimes \chi_2$.

All dihedral representations are known to come from eigenforms in the minimal possible weight with level equal to the (outside of p) conductor of the representation (see [Wiese 2004], Theorem 1).

In the tables we computed the Hecke algebras of odd dihedral representations as above in the following ranges. For each prime p less than 100 and each prime l less than or equal to the largest level occurring in the table for p, we chose d as plus or minus l such that d is 1 mod 4 and we let H run through all non-trivial cyclic quotients of the class group of $\mathbb{Q}(\sqrt{d})$ of order coprime to p. For each H we chose (unramified) characters χ of the absolute Galois group of $\mathbb{Q}(\sqrt{d})$ corresponding to H, up to Galois conjugacy and up to replacing χ by its inverse. Then χ is not the restriction of a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By genus theory the order of χ is odd, as the class number is, so we necessarily have $\chi^{-1} = \chi^{\sigma}$. We computed the local factor of $\mathbb{T}_{\mathbb{F}_p}(S_p(d, \left(\frac{d}{\cdot}\right); \mathbb{F}_p))$ corresponding to ρ_{χ} if ρ_{χ} is odd and p is completely split. For the prime $p = 2$ we also allowed square-free integers d which are 1 mod 4 and whose absolute value is less than 5000.

4.3 Icosahedral example

With the help of a list of polynomials provided by Gunter Malle ([Malle 2006]) a Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ which is of prime conductor, completely split at 2 and thus satisfies the assumptions of Question 1.9 and whose image is isomorphic to the icosahedral group A_5 could be described explicitly. The modular forms in weight 2 predicted by Serre's conjecture were found and the corresponding Hecke algebra turned out to have Gorenstein defect equal to 2.

Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree 5 whose Galois group, i.e. the Galois group of the normal closure L of $K = \mathbb{Q}[X]/(f)$, is isomorphic to A_5. We assume that K is unramified at 2, 3 and 5. We have the Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(L/\mathbb{Q}) \cong A_5 \cong \mathrm{SL}_2(\mathbb{F}_4).$$

We now determine its conductor and its traces. Let p be a ramified prime. As the ramification is tame, the image of the inertia group $\rho_f(I_p)$ at p is cyclic of order 2, 3 or 5. In the first case, the image of a decomposition group $\rho_f(D_p)$ at p is either equal to $\rho_f(I_p)$ or equal to $\mathbb{Z}/2\mathbb{Z} \times \rho_f(I_p)$. If the order of $\rho_f(I_p)$ is odd and $\rho_f(I_p) = \rho_f(D_p)$, then any completion of L at the unique prime above p is totally ramified and cyclic of degree $\#\rho_f(I_p)$, hence contained in $\mathbb{Q}_p(\zeta_p)$ for ζ_p a primitive p-th root of unity. It follows that p is congruent to 1 mod $\#\rho_f(I_p)$. If the order of $\rho_f(I_p)$ is odd, but $\rho_f(I_p)$ is not equal to $\rho_f(D_p)$, then $\rho_f(D_p)$ is a dihedral group and the completion of L at a prime above p has a unique unramified quadratic subfield S. Thus, we have the exact sequence

$$0 \to \rho_f(I_p) \to \rho_f(D_p) \to \mathrm{Gal}(S/\mathbb{Q}_p) \to 0.$$

On the one hand, it is well-known that the conjugation by a lift of the Frobenius element of $\mathrm{Gal}(S/\mathbb{Q}_p)$ acts on $\rho_f(I_p)$ by raising to the p-th power. On the other hand, as the action is non-trivial it also corresponds to inversion on $\rho_f(I_p)$, since the only elements of order 2 in $(\mathbb{Z}/3\mathbb{Z})^\times$ and $(\mathbb{Z}/5\mathbb{Z})^\times$ are -1. As a consequence, p is congruent to -1 mod $\#\rho_f(I_p)$ in this case.

We hence have the following cases.

(1) Suppose $p\mathcal{O}_K = \mathfrak{P}^5$. Then $p \equiv \pm 1 \mod 5$.

  (a) If $p \equiv 1 \mod 5$, then $\rho_f|_{I_p} \sim \begin{pmatrix} \chi & 0 \\ 0 & \chi^{-1} \end{pmatrix}$ with χ a totally ramified character of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ of order 5.

  (b) If $p \equiv -1 \mod 5$, then $\rho_f(D_p)$ is the dihedral group with 10 elements.

(2) Suppose $p\mathcal{O}_K = \mathfrak{P}^3\mathfrak{Q}\mathfrak{R}$ or $p\mathcal{O}_K = \mathfrak{P}^3\mathfrak{Q}$.

  (a) If $p \equiv 1 \mod 3$, then $\rho_f|_{I_p} \sim \begin{pmatrix} \chi & 0 \\ 0 & \chi^{-1} \end{pmatrix}$ with χ a totally ramified character of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ of order 3.

  (b) If $p \equiv -1 \mod 3$, then $\rho_f(D_p)$ is the dihedral group with 6 elements.

(3) Suppose that p is ramified, but that we are neither in Case (1) nor in Case (2). Then $\rho_f|_{I_p} \sim \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

By the definition of the conductor at p it is clear that it is p^2 in Cases (1) and (2) and p in Case (3). However, in Cases (1)(a) and (2)(a) one can choose a character ϵ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the same order as χ whose restriction to D_p gives the character χ. If one twists the representation ρ_f by ϵ one finds also in these cases that the conductor at p is p.

An inspection of the conjugacy classes of the group $\mathrm{SL}_2(\mathbb{F}_4)$ shows that the traces of ρ_f twisted by some character ϵ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ are as follows. Let l be an unramified prime.

- If the order of Frob_l is 5, then the trace at Frob_l is $\epsilon(\mathrm{Frob}_l)w$ where w is a root of the polynomial $X^2 + X + 1$ in $\mathbb{F}_2[X]$.
- If the order of Frob_l is 3, then the trace at Frob_l is $\epsilon(\mathrm{Frob}_l)$.
- If the order of Frob_l is 1 or 2, then the trace at Frob_l is 0.

These statements allow the easy identification of the modular form belonging to an icosahedral representation.

We end this section with some remarks on our icosahedral example. It was obtained using the polynomial $x^5 - x^4 - 79x^3 + 225x^2 + 998x - 3272$. The corresponding table entry is:

Level	Wt	ResD	Dim	EmbDim	NilO	GorDef	#Ops	#(p<HB)	Gp
89491	2	2	12	4	3	2	4	1746	A_5

Hence, in level 89491 and weight 2 there is a single eigenform g mod 2 up to Galois conjugacy whose first couple of q-coefficients agree with the traces of a twist of the given icosahedral Galois representation. From this one can deduce that the Galois representation ρ_g of g has an icosahedral image and is only ramified at 89491. As weight lowering is not known in our case, we cannot prove that ρ_g coincides with a twist of the given one. It might, however, be possible to exclude the existence of two distinct icosahedral extensions of the rationals inside $\mathbb{C}$ that ramify only at 89491 by consulting tables. According to Malle, the icosahedral extension used has smallest discriminant among all totally real A_5-extensions of the rationals in which 2 splits completely.

5 Further results and questions

In this section we present some more computational observations for Hecke algebras under the assumptions of Question 1.9, which lead us to ask some more questions.

On the dimension of the Hecke algebra

From the data, we see that many even integers appear as dimensions of the $\mathbb{T}_{\mathfrak{m}}$. We know that the dimension must be at least 4, as this is the dimension of the smallest non-Gorenstein algebra which can appear in our case. This extends the results of [Kilford 2002], where the dimensions of the Hecke

algebras $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_2}(S_2(\Gamma_0(431)))$ and $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_2}(S_2(\Gamma_0(503)))$ localised at the non-Gorenstein maximal ideals are shown to be 4.

In this table we see exactly how many times each dimension appears in our data. We observe that every even integer between 4 and 32 appears, and that the largest dimension is 60. The most common dimension is 4, which appears about half of the time. However, as the dimension of the Hecke algebra attached to $S_k(\Gamma_1(N))$ increases with N and with k, this may be an artifact of the data being collected for "small" levels N and primes p.

Dimension	4	6	8	10	12	14	16	18	20	22
Number of algebras	206	58	25	3	24	6	20	3	12	3

Dimension	24	26	28	30	32	36	40	46	56	60
Number of algebras	5	4	2	1	2	2	4	1	2	1

It seems reasonable that there should be infinitely many cases with dimension 4, and plausible that every even integer greater than or equal to 4 should appear as a dimension infinitely many times. From the tables, we see that dimension 4 algebras appear at very high levels, so they do not appear to be becoming rare as the dimension increases, but this may, of course, be an artifact of our data.

We note that not every example that arises from an elliptic curve in characteristic $p = 2$ has Hecke algebra with dimension 4; for example the algebra $\mathbb{T}_{\mathbb{Z}\to\mathbb{F}_2}(S_2(\Gamma_0(2089)))$ localised at its non-Gorenstein maximal ideal has dimension 18. In level 18097 there is a dimension 36 example arising from an elliptic curve.

On the residue degree

We will now solve an easy aspect of the question of the possible structures of non-Gorenstein local algebras occurring as local Hecke algebras. We assume for the couple of lines to follow the Generalised Riemann Hypothesis (GRH).

We claim that then the residue degrees of $\mathbb{T}_{\mathfrak{m}}$ (in the notation of Question 1.9) are unbounded, if we let p and N run through the primes such that $p \neq N$ and N is congruent to 3 modulo 4.

For, class groups of imaginary quadratic fields $\mathbb{Q}(\sqrt{-N})$ have arbitrarily large cyclic factors of odd order, as the exponent of these class groups is known to go to infinity as N does, by the main result of [Boyd and Kisilevsky 1972], which assumes GRH. So the discussion on dihedral forms in Section 4 immediately implies the claim.

On the embedding dimension

One can ask whether the embedding dimension of the local Hecke algebras in the situation of Question 1.9 is bounded, if we allow p and N to vary. This, however, seems to be a difficult problem. The embedding dimensions occurring in our tables are 3 (299 times), 4 (78 times) and 5 (7 times).

The embedding dimension d is related to the number of Hecke operators needed to generate the local Hecke algebra, in the sense that at least d Hecke operators are needed. Probably, d Hecke operators can be found that do generate, but they need not be the first d prime Hecke operators,

of course. However, as our tables suggest, in most cases the actual computations were done using very few operators, and there are 99 of the 384 cases when the computation already finished after d operators.

6 Acknowledgements

The authors would like to thank Kevin Buzzard for informing them about the level 23 and weight 59 example, for many helpful conversations and communications, and for his comments on a first draft of this paper. They would like to thank Amod Agashe for comments on an early version and William Stein for the use of his computers MECCAH and NERON for computations; without these, they would not have been able to pursue these computations as far as they did. The authors are grateful to Gunter Malle for providing them with a very useful list of A_5-polynomials. The first author would also like to thank Edray Goins for helpful conversations. The second author is indebted to Bas Edixhoven for very enlightening explanations.

The authors would also like to thank the referees for suggesting improvements to the paper.

References

[Agashe et al. 2006] Agashe, A., Ribet, K. A., and Stein, W. A. (2006). The Modular Degree, Congruence Primes and Multiplicity One. *http://modular.math.washington.edu/papers/ars-congruence/*.

[Bosma et al. 1997] Bosma, W., Cannon, J., and Playoust, C. (1997). The Magma algebra system I: The user language. *J. Symb. Comp.*, 24(3–4):235–265. *http://magma.maths.usyd.edu.au*.

[Boston et al. 1991] Boston, N., Lenstra, Jr., H. W., and Ribet, K. A. (1991). Quotients of group rings arising from two-dimensional representations. *C. R. Acad. Sci. Paris Sér. I Math.*, 312(4):323–328.

[Boyd and Kisilevsky 1972] Boyd, D. W. and Kisilevsky, H. (1972). On the exponent of the ideal class groups of complex quadratic fields. *Proc. Amer. Math. Soc.*, 31:433–436.

[Buzzard 1999] Buzzard, K. (1999). Appendix to *Lectures on Serre's Conjectures*, [Ribet and Stein 2001]. In *IAS/ Park City Mathematics Institute Lecture Series*.

[Diamond and Im 1995] Diamond, F. and Im, J. (1995). Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI.

[Edixhoven 1992] Edixhoven, B. (1992). The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594.

[Edixhoven 1997] Edixhoven, B. (1997). Serre's conjecture. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 209–242. Springer, New York.

[Edixhoven 2006] Edixhoven, B. (2006). Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. *J. Inst. Math. Jussieu*, 5(1):1–34. With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese.

[Eisenbud 1995] Eisenbud, D. (1995). *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York. With a view toward algebraic geometry.

[Emerton 2002] Emerton, M. (2002). Supersingular elliptic curves, theta series and weight two modular forms. *J. Amer. Math. Soc.*, 15(3):671–714 (electronic).

[Gross 1990] Gross, B. (1990). A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. Journal*, 61(2):445–517.

[Hida 1981] Hida, H. (1981). On congruence divisors of cusp forms as factors of the special values of their zeta functions. *Invent. math.*, 64:221–262.

[Kilford 2002] Kilford, L. J. P. (2002). Some non-Gorenstein Hecke algebras attached to spaces of modular forms. *J. Number Theory*, 97(1):157–164.

[Malle 2006] Malle, G. (2006). Personal communication.

[Mazur 1977] Mazur, B. (1977). Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186 (1978).

[Mazur and Ribet 1991] Mazur, B. and Ribet, K. A. (1991). Two-dimensional representations in the arithmetic of modular curves. *Astérisque*, 196–197:6, 215–255 (1992). Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[Ribet 1990] Ribet, K. A. (1990). Multiplicities of Galois representations in Jacobians of Shimura curves. In *Festschrift in honor of I. I. Piatetski-Shapiro on the occasion of his sixtieth birthday, Part II (Ramat Aviv, 1989)*, volume 3 of *Israel Math. Conf. Proc.*, pages 221–236. Weizmann, Jerusalem.

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

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

[Tilouine 1987] Tilouine, J. (1987). Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke. *Bull. Soc. Math. France*, 115(3):329–360.

[Tilouine 1997] Tilouine, J. (1997). Hecke algebras and the Gorenstein property. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 327–342. Springer, New York.

[Wiese 2004] Wiese, G. (2004). Dihedral Galois representations and Katz modular forms. *Doc. Math.*, 9:123–133 (electronic).

[Wiese 2005] Wiese, G. (2005). On modular symbols and the cohomology of Hecke triangle surfaces. Accepted for publication in International J. of Number Theory.

[Wiese 2007a] Wiese, G. (2007a). Multiplicities of Galois representations of weight one. *Algebra & Number Theory*, 1(1):67–85. With an appendix by Niko Naumann.

[Wiese 2007b] Wiese, G. (2007b). On the faithfulness of parabolic cohomology as a Hecke module over a finite field. *J. reine angew. Math.*, 606:79–103.

[Wiles 1995] Wiles, A. (1995). Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551.

L. J. P. Kilford
Department of Mathematics
University of Bristol
Bristol BS8 1TW

United Kingdom
l.kilford@gmail.com

Gabor Wiese
Institut für Experimentelle Mathematik
Universität Duisburg-Essen
Ellernstraße 29
45326 Essen
Germany
gabor.wiese@uni-due.de
http://maths.pratum.net