THE UNIVERSITY OF CHICAGO

COMPUTING CRYSTALLINE DEFORMATION RINGS VIA THE TAYLOR–WILES–KISIN PATCHING METHOD

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY

CHENGYANG BAO

CHICAGO, ILLINOIS

JUNE 2024

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The author extends her deepest gratitude to her advisor, Frank Calegari, for suggesting the problem, outlining the patching strategy to approach it, and providing enormous help with technical details in Section 1.3. She also thanks Andrea Dotto for enlightening conversations about properties of the ring $R^k_{\bar{r}}[\alpha_p]$ and Matthew Emerton and John Voight for helpful discussions that lead to Lemma 1.3.3.3.

The author appreciates Trung Nguyen for his assistance with adapting the implementation of the algorithm for use on the high-performance cluster at the University of Chicago's Research Computational Center. Additional computational support was provided by the Department of Mathematics and the Department of Computer Science at the University of Chicago, with John Zekos offering steady technical support throughout.

This paper was funded in part by NSF Grant DMS-2001097.

The author is grateful to her parents and Dun Tang for their constant companionship and emotional support over the years. She also extends her thanks to all her family and friends for their love.

ABSTRACT

Fix a prime number $p > 2$. Let $\overline{r} : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be an absolutely irreducible residual representation. In this paper, we describe an algorithm to compute arbitrarily close approximations to the non-framed fixed-determinant crystalline deformation ring $R^k_{\overline{r}}$ of $\overline{r}$ whose $\overline{\mathbf{Q}}_p$-points parametrize crystalline representations with Hodge–Tate weights $(0, k-1)$ using the Taylor–Wiles–Kisin patching. We give an implementation of this algorithm in Magma and Python (with Sagemath imported). Based on the data we have collected, we formulate a conjecture on the Hilbert series of the special fiber of $R^k_{\overline{r}}$ when $k = 2 + n(p-1)$ for some non-negative integer n. The conjectural formula implies that the Hilbert series goes to $(1-x)^{-3}$ as n tends to ∞. This aligns with the expectation that, as n grows, the special fiber of $R^k_{\overline{r}}$ gradually "fills out" that of the universal fixed-determinant deformation ring of $\overline{r}$, which is a formal power series ring in three variables. We also formulate a conjecture on when $R^k_{\overline{r}}$ is Gorenstein.

CHAPTER 1

THESIS

1.1 Introduction

Throughout this paper, we fix a prime number $p > 2$ and a finite extension L of $\mathbf{Q}_p$ with its ring of integers $\mathcal{O}$, a uniformizer λ, and the residue field $\mathbf{F}$. Let $\bar{r}$ be a two dimensional representation of the absolute Galois group $G_{\mathbf{Q}_p}$ of $\mathbf{Q}_p$ over $\mathbf{F}$ that is Schur, i.e. $\mathrm{End}(\bar{r} \otimes \overline{\mathbf{F}}_p) = \overline{\mathbf{F}}_p$.

In Kisin [2008], Kisin constructed a quotient $R^k_{\bar{r}}$ of the fixed-determinant universal deformation ring $R^{\mathrm{univ}}_{\bar{r}}$ of $\bar{r}$, that is called the non-framed fixed-determinant crystalline deformation $\mathcal{O}$-algebra of $\bar{r}$. It is characterized by the property that its $\overline{\mathbf{Q}}_p$-points parametrize crystalline deformations of $\bar{r}$ with Hodge–Tate weights $(0, k-1)$ and a fixed determinant. For example, consider the Galois representation

$$\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$$

of the absolute Galois group $G_{\mathbf{Q}}$ of $\mathbf{Q}$ attached to a newform f of level N and weight k. If $p \nmid N$, then the restriction of ρ_f to $G_{\mathbf{Q}_p}$ is a crystalline representation of Hodge–Tate weights $(0, k-1)$. It gives rise to an aforementioned crystalline deformation of $\bar{r}$ if its reduction modulo p is isomorphic to $\bar{r}$.

Crystalline deformation rings play an important role in Kisin's proof of the Fontaine–Mazur conjecture Fontaine and Mazur [1995] in Kisin [2009a].

Theorem 1.1.0.1 (Kisin, Emerton, Pan)**.** *Fix $p \geq 5$. An irreducible Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ that is*

- *odd, i.e.* $\det(\rho(c)) = -1$ *where c is the complex conjugation,*
- *almost everywhere unramified, and*

- *crystalline at p with distinct Hodge–Tate weights*

comes from a modular form up to a twist.

Remark 1.1.0.2. Kisin first proved the conjecture assuming that $p \geq 3$, $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_p)}}$ is absolutely irreducible (known as the Taylor–Wiles condition) and that $\overline{\rho}|_{G_{\mathbf{Q}_p}}$ is not a twist of the extension of the trivial character by the mod-p cyclotomic character. Emerton gave another proof in Emerton [2011] in many cases using completed cohomology and local-global compatibility results. Lue Pan treated the other cases in Pan [2022].

Remark 1.1.0.3. The Fontaine–Mazur conjecture is stated for representations that are de Rham, or equivalently, potentially semistable, at p. In this paper, we only focus on the crystalline condition.

A crucial step in Kisin's argument is apply patching to reduce the problem to proving that the Hilbert–Samuel multiplicity of the special fiber of the crystalline deformation ring $R^k_{\overline{r}}$ is equal to a certain automorphic multiplicity, which is closely related to the following theorem.

Theorem 1.1.0.4 (Kisin, Paškūnas, Hu–Tan, Sander, Tung)**.** *The Hilbert–Samuel multiplicity of $R^k_{\overline{r}} \otimes \mathbf{F}$ is equal to the (weighted) sum of the multiplicities of the Serre weights in the semisimplification of the* $\mathrm{GL}_2(\mathbf{F}_p)$*-representation* $\mathrm{Sym}^{k-2}\mathbf{F}^2$.

Remark 1.1.0.5. The theorem is referred to as the Breuil–Mézard conjecture Breuil and Mézard [2002] in the literature. Kisin first proved most cases in Kisin [2009a] by using the Taylor–Wiles–Kisin patching and the p-adic local Langlands correspondence. Paškūnas Paškūnas [2015] gave a purely local proof. The remaining cases were proved in Hu and Tan [2013],Sander [2012],Tung [2021a] and Tung [2021b].

Denote by $\mathfrak{m}$ the maximal ideal of $R^k_{\overline{r}} \otimes \mathbf{F}$. Since $R^k_{\overline{r}}$ has relative of dimension one over $\mathcal{O}$ Kisin [2008], the theorem is equivalent to saying that the limit

$$\lim_{n\to\infty} \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

is equal to some number which can be explicitly understood by the representation theory of $\mathrm{GL}_2(\mathbf{F}_p)$.

We are interested in some other limits of these dimensions. Assume that $\bar{r}$ has a crystalline lift of Hodge–Tate weights $(0, k_0 - 1)$ for some integer k_0 in the Fontaine–Laffaille range $[2, p]$. For $k \geq 2$, given that $R^k_{\bar{r}}$ is nonzero if and only if $k \equiv k_0 \pmod{p-1}$, we consider the family of special fibers of crystalline deformation rings $\{R^k_{\bar{r}} \otimes \mathbf{F}\}_{k \equiv k_0 \mod p-1}$ and form the following table of dimensions.

	$\dim \mathfrak{m}^0/\mathfrak{m}^1$	$\dim \mathfrak{m}^1/\mathfrak{m}^2$	$\dim \mathfrak{m}^2/\mathfrak{m}^3$	$\dim \mathfrak{m}^3/\mathfrak{m}^4$	$\dim \mathfrak{m}^4/\mathfrak{m}^5$	$\dots$
k_0	1					
$k_0 + p - 1$	1					
$k_0 + 2(p-1)$	1					
$k_0 + 3(p-1)$	1					
$\vdots$						

As previously mentioned, for a fixed $k = k_0 + i(p-1)$, as n approaches ∞, the limit of the numbers in the corresponding row is explicitly predicted by the Breuil–Mézard conjecture.

Question. For a fixed n, as i goes to ∞, do the limits of the numbers in the corresponding column exist? If so, what are they?

The main difficulty of tackling this problem is that the presentation of $R^k_{\bar{r}}$ remains largely unknown when $k \geq 2p$. For $2 \leq k \leq p+1$, the Fontaine–Laffaille theory Fontaine and Laffaille [1982] provides a of comprehensive understanding. Beyond the Fontaine–Laffaille range, Kisin computed the explicit presentation of $R^k_{\bar{r}}[\alpha_p]$ for $p+2 \leq k \leq 2p-1$ when $\bar{r}$ is absolutely irreducible, using Breuil–Kisin modules based on previous works Berger et al. [2003], Berger and Breuil [2005]. While the Breuil–Kisin theory is applicable to general weights k, a monodromy condition, which grows increasingly complicated as k increases, hinders us from obtaining explicit presentations via this method.

In this paper, we present an explicit algorithm to compute arbitrarily close approximations to the non-framed fixed-determinant crystalline deformation ring $R^k_{\overline{r}}$. Our approach is to use the global method: the Taylor–Wiles–Kisin patching. Essentially, suppose that we can choose a sufficiently nice global representation $\overline{\rho}$ whose restriction to $G_{\mathbf{Q}_p}$ is isomorphic to $\overline{r}$. The Taylor–Wiles–Kisin patching generates a patched Hecke algebra which is isomorphic to a power series ring over the crystalline deformation ring $R^k_{\overline{r}}$. Therefore, by computing the local Hecke algebras, we get arbitrarily close approximations to the ring $R^k_{\overline{r}}$.

Theorem 1.1.0.6 (Corollary 1.3.2.17)**.** *Suppose that $\overline{r}$ is unobstructed, which implies that $R^k_{\overline{r}}$ is a quotient of $\mathcal{O}[\![x_1, x_2, x_3]\!]$. If $\overline{r}$ can be globalized to a global Galois representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ satisfying Assumption 1.3.2.4, then the dimension of the cotangent space of $R^k_{\overline{r}} \otimes \mathbf{F}$ is equal to three when $k \geq k_0 + 2p^2 + p - 3$ and $k \equiv k_0 \mod p - 1$.*

Remark 1.1.0.7.

1. Whether $\overline{r}$ is unobstructed can be checked by using Proposition 1.2.2.9. This condition is very mild and is satisfied by most residual representations $\overline{r}$, whether they are irreducible or not.

2. All conditions in Assumption 1.3.2.4 but the last one are standard for applying the minimal level Taylor–Wiles–Kisin patching. The final condition is most restrictive. It is imposed for optimal implementation of the algorithm.

3. Given that $R^k_{\overline{r}}$ is a quotient of $\mathcal{O}[\![x_1, x_2, x_3]\!]$, we have $\mathbf{F}[\![x_1, x_2, x_3]\!] \twoheadrightarrow \mathbf{R}^k_{\overline{r}} \otimes \mathbf{F}$. Thus $\dim \mathfrak{m}/\mathfrak{m}^2$ is always bounded by three. Our theorem implies that this upper bound is achieved as k tends to ∞ for $k \equiv k_0 \mod p - 1$.

We implement the algorithm in Magma Bosma et al. [1997] and Python (with Sagemath The Sage Developers [2023] imported) and we have collected some data when $p = 3$ and $p = 5$. Based on these, we are mostly interested in exploring a conjectural formula of the

Hilbert series $H_k(x)$ of $R_{\overline{r}}^k \otimes \mathbf{F}$ defined below

$$H_k(x) := \sum_{i=0}^{\infty} \dim(\mathfrak{m}^i/\mathfrak{m}^{i+1})x^i.$$

Conjecture 1.1.0.8. *When $k_0 = 2$ and $\overline{r}$ is absolutely irreducible, the Hilbert series of $R_{\overline{r}}^k \otimes \mathbf{F}$ is*

$$H_k(x) = \sum_{\substack{2 \leq i \leq k \\ p-1 | i-2}} Sh_i(x),$$

where the definition of the shift function $Sh_i(x)$ is given in §1.5.

Corollary 1.1.0.9. *Assume that the conjecture above is true. Then all of the following statements hold.*

1. *The sequence $\{H_k(x)\}_{k=2+n(p-1)}$ is an increasing sequence in k, i.e.*

$$H_k(x) \geq H_{k-(p-1)}(x).$$

2. *The limit of $H_k(x)$ as k goes to ∞ is the Hilbert–Samuel function of $R_{\overline{r}}^{\text{univ}} \otimes \mathbf{F} \xrightarrow{\sim} \mathbf{F}[\![x_1, x_2, x_3]\!]$, i.e.*

$$\lim_{\substack{k \to \infty \\ p-1 | k-2}} H_k(x) = \frac{1}{(1-x)^3} = \sum_{i=0}^{\infty} \binom{i+2}{2} x^i.$$

3. *The speed of convergence: Let m be a positive number with its unique p-adic expansion $\sum_{i=0}^{\infty}(a_i + 2b_i)p^i$ such that $0 \leq a_i + 2b_i < p$ with $a_i \in \{0, 1\}$ and b_i a non-negative integer. Set k to be the integer*

$$k := 2 + (p^2 - 1)(\sum_{i=0}^{\infty} a_i p^{2i} + \sum_{i=0}^{\infty} b_i p^{2i+1}).$$

Then k is the smallest integer such that the m-th coefficient of $H_k(x)$ is equal to $\binom{m+2}{2}$.

Remark 1.1.0.10.

1. Suppose that $\overline{\rho}: G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ is a modular Galois representation whose restriction to $G_{\mathbf{Q}_p}$ is isomorphic to the local representation $\overline{r}$. Multiplication by the Hasse invariant gives rise to a greater number of eigenforms of weight k whose associated p-adic Galois representations reduce to $\overline{\rho}$ modulo p, compared to those of weight $k-(p-1)$. This observation heuristically suggested that $\mathrm{Spf}(R_{\overline{r}}^{k})$ has more $\mathcal{O}$-points than $\mathrm{Spf}(R_{\overline{r}}^{k-(p-1)})$ does. Part (1) of the corollary states that from the viewpoint of the Hilbert series, the ring $R_{\overline{r}}^{k}$ does exhibit a greater degree of "complexity" in comparison to $R_{\overline{r}}^{k-(p-1)}$.

2. The question of whether the crystalline locus $\mathrm{Spf}(R_{\overline{r}}^{k})$ can "fill out" the universal deformation space $\mathrm{Spf}(R_{\overline{r}}^{\mathrm{univ}})$ as k grows has been of particular interest. For the generic fiber, Colmez Colmez [2008] and Kisin Kisin [2010] showed that the points of $\mathrm{Spec}(R_{\overline{r}}^{\mathrm{univ}}[1/p])$ corresponding to crystalline representations are dense in the Zariski topology. Part (2) of the corollary serves as an analogy for this phenomenon in the context of special fibers from the perspective of Hilbert functions.

We formulate another conjecture on when the crystalline deformation ring $R_{\overline{r}}^{k}$ is Gorenstein. By the fact [Eisenbud, 2013, Corollary 21.20], for dimension reason, the ring $R_{\overline{r}}^{k}$ is a complete intersection when it is Gorenstein.

Conjecture 1.1.0.11. *When $\overline{r}|_{I_p} \sim \begin{pmatrix} \omega_2 & 0 \\ 0 & \omega_2^p \end{pmatrix}$, the ring $R_{\overline{r}}^{k}$ is Gorenstein if and only if*

$$k = k_1 + (p^2-1)\left(ap^N - 1\right)$$

for some integers $2p \leq k_1 \leq p^2 - p + 2$ such that $k_1 \equiv 2 \mod p-1$, $N \geq 0$ and $1 \leq a \leq p$ with the exception that $k = 2$ and $k = p+1$, in which cases the crystalline deformation ring $R_{\overline{r}}^{k}$ is formally smooth over $\mathcal{O}$.

In particular, the conjecture implies that there are infinitely many weights k for which $R_{\overline{r}}^{k}$ is Gorenstein. Take $p = 5$ and $k_1 = 2p = 10$ for an example. A list of weights k is

$$10, 34, 58, 82, 106, 226, 346, 466, 586, 1186, 1786, 2386, 2986, \ldots.$$

Overview of the algorithm

Given the local Galois representation $\overline{r}$, assume that we can choose a global Galois representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ whose restriction to $G_{\mathbf{Q}_p}$ is isomorphic to $\overline{r}$ such that we can apply the minimal level Taylor–Wiles–Kisin patching. This patching process generates a patched module, denoted as M_{∞}^{k}, whose support is the patched Hecke algebra $\mathbb{T}_{\infty}^{k}$. The algebra is isomorphic to a formal power series ring over $R_{\overline{r}}^{k}$.

Specifically, the module M_{∞}^{k} is approximated by the localized modules, denoted as $M'(k, Q)$ (see Definition 1.2.3.8), which are certain submodules of $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ for certain congruence subgroups Γ_Q depending on a set Q of Taylor–Wiles primes. Denote by $\mathbb{T}(k, Q)$ the support of $M'(k, Q)$. We use Serre's conjecture to determine the conditions defining the submodule $M'(k, Q)$ in §1.3.1. In §1.3.2, we utilize Jochnowitz's theory to identify a finite set of Hecke operators, independent of k, whose images generate $\mathbb{T}(k, Q)$. We then compute $M'(k, Q)$ and the relations among these generators using linear algebra over $\mathcal{O}$ in §1.3.3. Finally, we approximate the Hecke algebra $\mathbb{T}_{\infty}^{k}$ with $\mathbb{T}(k, Q)$.

The primary challenge lies in the computation of $M'(k, Q)$, which involves the multiplication of matrices of large size, which can be up to 100,000 by 100,000. When the set Q of Taylor–Wiles primes remains fixed, our algorithm exhibits a computational complexity of $O(k^4)$ without using parallelization. This computational demand becomes notably burdensome as the value of k grows considerably. We discuss the parallel implementation of the algorithm in §1.3.5.

Organization of the paper

In Section 2, we provide an overview of key inputs. We begin by reviewing fundamental facts about the cohomology of congruence subgroups, which will be used in computing the submodule $M'(k,Q)$. We then review some Galois deformation theory with a focus on the tangent spaces, which will be used heavily in §1.3.2. Additionally, we review the setup and construction of Taylor–Wiles–Kisin patching, a foundation for our algorithm. By leveraging the Breuil-Mézard conjecture, we provide an exact formula for the rank of $M'(k,Q)$. Section 3 is dedicated to describing the algorithm and implementation in details. In Section 4, we present our work as follows: §1.4.1 provides a summarized prototype for computing an example. In §1.4.2, we present a detailed analysis of a specific example that we have successfully computed. Additionally, in §1.4.3, we gather other interesting examples for future exploration and research. Moving on to Section 5, we formulate conjectures based on the data we have collected. We conclude the paper by discussing our plans for future research in the final section.

Notation and Conventions

Throughout this paper, we make the assumption that the prime p is an odd integer, and the initial weight k_0 satisfies the condition $2 \leq k_0 \leq p$.

We denote the absolute Galois group of a field F by G_F. When F is a global field, and S is a finite set of places of F, we write $G_{F,S}$ for the Galois group of the maximal extension of F that is unramified outside S over F. Its abelianization is denoted as $G_{F,S}^{\mathrm{ab}}$. For a place v of F, let F_v be the local field at v and fix an embedding $G_{F_v} \hookrightarrow G_F$. The inertia subgroup of G_{F_v} is denoted by I_v.

We use the notation ω for the mod-p cyclotomic character and ω_2 for the fundamental character of level two. Additionally, we denote χ_{cyc} as the cyclotomic character of $G_{\mathbf{Q}}$.

We let v_p be the normalized p-adic valuation such that $v_p(p) = 1$.

In all the deformation problems we consider in this paper, we fix the determinant. We also refer to $\mathrm{ad}^0\overline{\rho}$ as the trace 0 adjoint representation.

Acknowledgements

The author extends her deepest gratitude to her advisor, Frank Calegari, for suggesting the problem, outlining the patching strategy to approach it, and providing enormous help with technical details in Section 1.3. She also thanks Andrea Dotto for enlightening conversations about properties of the ring $R_{\overline{r}}^{k}[\alpha_p]$ and Matthew Emerton and John Voight for helpful discussions that lead to Lemma 1.3.3.3.

The author appreciates Trung Nguyen for his assistance with adapting the implementation of the algorithm for use on the high-performance cluster at the University of Chicago's Research Computational Center. Additional computational support was provided by the Department of Mathematics and the Department of Computer Science at the University of Chicago, with John Zekos offering steady technical support throughout.

This paper was funded in part by NSF Grant DMS-2001097.

1.2 Preliminaries

1.2.1 Cohomology of congruence subgroups

As mentioned in the introduction, computing a certain submodule $M'(k, Q)$ (see Definition 1.2.3.8) of the cohomology of some congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$ is a crucial step in our algorithm. This subsection is dedicated to review the group cohomology of such groups and its equipped Hecke action and Galois action. We put an emphasis on explicit formulas rather than conceptual definitions because our ultimate goal is to develop an algorithm. The discussions presented are mostly based on results in Ash and Stevens [1986a], and we follow their notation.

If Γ is an arbitrary group and M is an $\mathcal{O}$-module with a Γ-action. By taking the long exact sequence on cohomology of the short exact sequence $0 \to M \xrightarrow{\cdot\lambda} M \to M \otimes_{\mathcal{O}} \mathbf{F} \to 0$, we obtain the following.

Proposition 1.2.1.1. *The λ-torsion of $H^1(\Gamma, M)$ is* $\mathrm{Im}\,(H^0(\Gamma, M \otimes \mathbf{F}) \to H^1(\Gamma, M))$.

Let Γ be a congruence subgroup of G of level N where G is either SL_2 or PSL_2. We list some basic properties of the cohomology groups of Γ when it is torsion free.

Lemma 1.2.1.2 (Borel–Serre)**.** *If Γ is torsion free, then the cohomology groups $H^i(\Gamma, M)$ vanish for all Γ-modules M and integers $i \geq 2$, i.e. the cohomological dimension of Γ is one.*

Remark 1.2.1.3. This is a special case of [Borel and Serre, 1973, Corollary 11.4.3] where we take the algebraic group G to be SL_2 or PSL_2 whose rank $r_{\mathbf{Q}}(G)$ is one, and X to be the upper half plane which has real dimension 2. Then the cohomological dimension of Γ is $2 - 1 = 1$.

Corollary 1.2.1.4.

1. *If $\Gamma \subset G$ is torsion free, then $H^1(\Gamma, M) \otimes \mathbf{F} \xrightarrow{\sim} H^1(\Gamma, M \otimes \mathbf{F})$.*
2. *When $G = \mathrm{SL}_2(\mathbf{Z})$ and the only torsion element of Γ is $-I$, then $H^1(\Gamma, M) \otimes \mathbf{F} \xrightarrow{\sim} H^1(\Gamma, M \otimes \mathbf{F})$.*

Proof. The first assertion follows directly from taking the long exact sequence on cohomology and applying the lemma above. By the inflation restriction sequence

$$0 \to H^1(\mathrm{P}\Gamma, M) \to H^1(\Gamma, M) \to H^1(\mathbf{Z}/2\mathbf{Z}, M) \to \dots,$$

where $\mathrm{P}\Gamma$ is the image of Γ in $\mathrm{PSL}_2(\mathbf{Z})$, we have the isomorphism

$$H^1(P\Gamma, M) \xrightarrow{\sim} H^1(\Gamma, M),$$

whenever M is a $\mathbf{Z}_p$-module. Then we can apply (1) to $H^1(\mathrm{P}\Gamma, M)$ and get

$$H^1(\Gamma, M) \otimes \mathbf{F} \xrightarrow{\sim} H^1(\mathrm{P}\Gamma, M) \otimes \mathbf{F} \xrightarrow{\sim} H^1(\mathrm{P}\Gamma, M \otimes \mathbf{F}) \xrightarrow{\sim} H^1(\Gamma, M \otimes \mathbf{F}).$$

$\square$

Now let M be a finite free $\mathcal{O}$-module on which Γ acts.

Proposition 1.2.1.5. *If Γ is torsion free, then the $\mathcal{O}$-module $Z^1(\Gamma, M)$ of cochains is finite free and*

$$Z^1(\Gamma, M) \otimes_{\mathcal{O}} \mathbf{F} \xrightarrow{\sim} Z^1(\Gamma, M \otimes_{\mathcal{O}} \mathbf{F}).$$

Proof. Since Γ is torsion free, the quotient space $\mathbb{C}/\Gamma$ is a holomorphic punctured curve and thus it has free fundamental group. On the other hand, it is a $K(\Gamma, 1)$ space; so we have Γ is free. Let $\{s_1, \ldots, s_n\}$ be a minimal set of generators of Γ and let $\{e_1, \ldots, e_m\}$ be an $\mathcal{O}$-basis of M. Suppose that R is either $\mathcal{O}$ or $\mathbf{F}$. Let $f_{i,j} : \Gamma \to M \otimes R$ be a cochain such that

$$f_{i,j}(s_l) = \begin{cases} e_j \otimes 1 & i = l \\ 0 & i \neq l \end{cases} \quad \text{for} \quad 1 \leq l \leq n.$$

It is not hard to verify that $\{f_{i,j}\}_{1 \leq i \leq n, 1 \leq j \leq m}$ is an R-basis of $Z^1(\Gamma, M \otimes R)$. Using the basis, it is straightforward to construct the isomorphism in the statement. $\square$

From now on we let $G = \mathrm{SL}_2$ and review the Hecke action on the group cohomology. Denote by S the subsemigroup of $\mathrm{GL}_2(\mathbf{Q})$ such that

1. $\Gamma \subseteq S$, and
2. Γ and $g^{-1}\Gamma g$ are commensurable for every $g \in S$.

When M is an S-module, there is a Hecke action on $H^i(\Gamma, M)$ for all integers i. For the sake of this paper, we only discuss the definition for $i = 0$ and $i = 1$. Let g be an element of

S. Then the double coset $\Gamma g \Gamma$ is a finite disjoint union $\sqcup \Gamma g_i$ for some $g_i \in S$. Suppose that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We denote by g^ι the element $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Define the double coset operator $[\Gamma g \Gamma]$ to act on $H^0(\Gamma, M)$ by the formula

$$m[\Gamma g \Gamma] = \sum_i g_i^\iota m \quad \text{for} \quad m \in H^0(\Gamma, M).$$

One can check the definition does not depend on the choice of the set of representatives $\{g_i\}$. We now explain the double coset action on $H^1(\Gamma, M)$. Let c be a cochain in $Z^1(G, M)$ that defines a cohomology class $[c]$. With respect to a fixed choice of representatives $\{g_i\}$, the double coset operator $[\Gamma g \Gamma]$ acts on $Z^1(\Gamma, M)$ by the following formula

$$\left(c\,[\Gamma g \Gamma]\right)(h) = \sum_i g_i^\iota c(g_i h g_{\sigma_h(i)}^{-1}) \quad \text{for} \quad c \in Z^1(\Gamma, M) \text{ and } h \in \Gamma \tag{1.2.1.6}$$

where σ_h is a permutation defined by $\Gamma g_i h = \Gamma g_{\sigma_h(i)}$. The formula induces an action of $[\Gamma g \Gamma]$ on $H^1(\Gamma, M)$ that is independent of the choice of representatives $\{g_i\}$. One can check that choosing another set of representatives $\{\gamma_i g_i\}$ for some γ_i's in Γ results in the difference by a coboundary defined by $\sum_i g_i^\iota c(\gamma_i^{-1}) \in M$.

Let H be a subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ and let Γ_H be the subgroup of $\Gamma_0(N)$ that consists of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ where $a, d \in H$. Let q be a prime dividing N and consider the double coset operator $[\Gamma_H g \Gamma_H]$ where $g = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$. We denote $[\Gamma_H g \Gamma_H]$ by U_q. Then

$$g^{-1} \Gamma_H g \cap \Gamma_H = \Gamma_H \cap \Gamma^0(q).$$

Thus $g_i := g \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$ for $i = 0, \ldots, q-1$ form a set of representatives of this double coset operator and we fix this choice when computing the action of U_q on $Z^1(\Gamma_H, \mathrm{Sym}^{k-2}\mathcal{O}^2)$. We take M to be $\mathrm{Sym}^{k-2}\mathcal{O}^2$, by which we mean the finite free $\mathcal{O}$-module of polynomials in $\mathcal{O}[u,v]$ of total degree $k-2$, equipped with the action of the semigroup $\mathrm{GL}_2(\mathbf{Q}) \cap M_2(\mathbf{Z})$ given by

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} P\right)(u,v) = P(au+cv, bu+dv).$$

When $\mathcal{O}$ is replaced with a general ring R, the action of the semigroup on $\mathrm{Sym}^{k-2}R^2$ follows a similar definition.

Proposition 1.2.1.7. *If $k > 2$, the module $\mathrm{Sym}^{k-2}\mathcal{O}^2$ has no nontrivial fixed points by Γ_H, i.e. $H^0(\Gamma_H, \mathrm{Sym}^{k-2}\mathcal{O}^2) = 0$.*

Proof. Let $P(u,v)$ be a homogeneous polynomial in $\mathrm{Sym}^{k-2}\mathcal{O}^2$. Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_H$, we have $P(u,v) = P(u, u+v)$. Thus the polynomial $P(u,v)$ equals u^{k-2} up to a scalar because $\mathrm{char}\,\mathcal{O} = 0$. Note that $\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$ is also in Γ_H. By the same reasoning, we deduce $P(u,v) = 0$. $\square$

Proposition 1.2.1.8. *If $q \in \mathbf{Z}$ is an integer that is congruent to 1 modulo p, then the eigenvalue of U_q on $B^1(\Gamma_H, \mathrm{Sym}^{k-2}\mathcal{O}^2) \otimes \mathbf{F}$ is 1.*

Proof. We point out that $q \equiv 1 \pmod{\lambda}$ because q is λ-adically close to 1 if and only it is p-adically close to 1.

Note that the map $\mathrm{Sym}^{k-2}\mathcal{O}^2 \to B^1(\Gamma, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ given by

$$P(u,v) \mapsto (\gamma \mapsto (\gamma P)(u,v) - P(u,v))$$

defines an isomorphism. To see this, it suffices to show that the image of the basis

$$\{u^i v^{k-2-i}\}_{i=0,\ldots,k_2}$$

is still linearly independent, which then follows from Proposition 1.2.1.7.

Suppose that b is a coboundary such that $b(\gamma) = (\gamma P)(u,v) - P(u,v)$ for some $P(u,v) \in \mathrm{Sym}^{k-2}\mathcal{O}^2$. With respect to our choice of representatives, we have

$$\begin{aligned}(bU_q)(\gamma) &= \sum_{i=0}^{q-1} g_i^\iota b(g_i\gamma g_{\sigma_\gamma(i)}^{-1}) = \sum_{i=0}^{q-1} g_i^\iota \left(g_i\gamma g_{\sigma_\gamma(i)}^{-1} P(u,v) - P(u,v)\right) \\ &= \sum_{i=0}^{q-1} \det(g_i)\gamma g_{\sigma_\gamma(i)}^{-1} P(u,v) - \sum_{i=0}^{q-1} g_i^\iota P(u,v) = \sum_{i=0}^{q-1} \gamma \det(g) g_i^{-1} P(u,v) - \sum_{i=0}^{q-1} g_i^\iota P(u,v) \\ &= \gamma \sum_{i=0}^{q-1} g_i^\iota P(u,v) - \sum_{i=0}^{q-1} g_i^\iota P(u,v).\end{aligned}$$

Since $g_i^\iota P(u,v) = \begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} P(u,v) = P(qu, v - iqu)$, we have

$$\sum_{i=0}^{q-1} g_i^\iota P(u,v) = \sum_{i=0}^{q-1} P(qu, v - iqu).$$

Define the U_q action on $\mathrm{Sym}^{k-2}\mathcal{O}^2$ by

$$(PU_q)(u,v) = \sum_{i=0}^{q-1} P(qu, v - iqu).$$

Then the aforementioned isomorphism is U_q-equivariant.

If $bU_q \equiv \alpha b \mod \lambda B^1(\Gamma, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ for some number $\alpha \in \mathcal{O}$, then

$$\alpha P(u,v) \equiv \sum_{i=0}^{q-1} P(qu, v - iqu) \equiv \sum_{i=0}^{q-1} P(u, v - iu) \mod \lambda \mathrm{Sym}^{k-2}\mathcal{O}^2$$

where the second congruence holds because $q \equiv 1 \pmod{\lambda}$. Write $P(u,v) = a_n(u)v^n + \ldots + a_1(u)v + a_0(u)$ for some $a_i(u) \in \mathcal{O}[u]$ with $a_n(u) \not\equiv 0 \pmod{\lambda}$ and integer $0 \leq n \leq k-2$.

Compare the coefficients of v^n on both sides and we conclude that $\alpha a_n(u) \equiv q a_n(u) \pmod{\lambda}$. Thus $\alpha \equiv 1 \pmod{\lambda}$.

□

Remark 1.2.1.9. The $\mathcal{O}$-module $H^1(\Gamma_H, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ can have torsion even when Γ_H is torsion free. For example, when $p = 5$, $k = 14$ and $\Gamma_H = \Gamma_1(11) \cap \Gamma_0(14)$, the Γ_H-fixed points of $\mathrm{Sym}^{k-2}\mathbf{F}^2$ is spanned by $y^2x^{10} + 3y^6x^6 + y^{10}x^2$. By Proposition 1.2.1.1, we have

$$H^0(\Gamma, \mathrm{Sym}^{k-2}\mathcal{O}^2)[\lambda] \xrightarrow{\sim} \mathrm{Im}\,(H^0(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}^2) \to H^1(\Gamma, \mathrm{Sym}^{k-2}\mathcal{O}^2)).$$

Since $\ker(H^0(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}^2) \to H^1(\Gamma, \mathrm{Sym}^{k-2}\mathcal{O}^2)) = H^0(\Gamma, \mathrm{Sym}^{k-2}\mathcal{O}^2) \otimes \mathbf{F} = 0$ by the long exact sequence on cohomology and Proposition 1.2.1.7, we conclude that

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathcal{O}^2)[\lambda] \xrightarrow{\sim} H^0(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}^2) = \mathbf{F} \cdot (y^2x^{10} + 3y^6x^6 + y^{10}x^2),$$

which is nontrivial.

To equip the group cohomology with a Galois action, we use the comparison theorem between the group cohomology and étale cohomology. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbf{Z})$ be a p-torsion free congruence subgroup and let M be a finite free $\mathcal{O}$-module on which Γ acts continuously. Let $\mathfrak{h}$ be the upper half plane and let Y_Γ be the algebraic modular curve whose set of $\mathbb{C}$-points $Y_\Gamma(\mathbb{C})$ is $\mathfrak{h}/\Gamma$. Then $M \otimes \mathcal{O}/\lambda^n$ (resp. M) defines a locally constant sheaf on Y_Γ, which we denote by $\widetilde{M \otimes \mathcal{O}/\lambda^n}$ (resp. $\widetilde{M}$). Given that Γ is p-torsion free, there is the isomorphism

$$H^i(Y_\Gamma(\mathbb{C}), \widetilde{M \otimes \mathcal{O}/\lambda^n}) \xrightarrow{\sim} H^i(\Gamma, M \otimes \mathcal{O}/\lambda^n)$$

for every integer $i \geq 0$ and $n \geq 1$. (See for example [Ash and Stevens, 1986a, §1.4].) By the comparison theorem between the torsion-coefficient singular cohomology and the étale cohomology, we have

$$H^i(Y_\Gamma(\mathbb{C}), \widetilde{M \otimes \mathcal{O}/\lambda^n}) \xrightarrow{\sim} H^i_{\text{ét}}(Y_{\Gamma,\overline{\mathbf{Q}}}, \widetilde{M \otimes \mathcal{O}/\lambda^n})$$

for every integer $i \geq 0$ and $n \geq 1$. These isomorphisms are Hecke equivariant where the Hecke action on the cohomology of modular curve is defined via correspondence.

Proposition 1.2.1.10. *Taking the inverse limit commutes with group cohomology, i.e.,*

$$H^i(\Gamma, M) \xrightarrow{\sim} \varprojlim_n H^i(\Gamma, M \otimes \mathcal{O}/\lambda^n)$$

for all integers $i \geq 0$.

Proof. When $i = 0$, it is straightforward to check that the isomorphism holds. When $i \geq 1$, by the corollary to [Tate, 1976, Proposition 2.2], it suffices to check the groups $H^{i-1}(\Gamma, M \otimes \mathcal{O}/\lambda^n)$ are finite for each n and $i \geq 1$, which is equivalent to showing that they are finitely generated. This then follows from the fact that Γ is finitely presented. □

Corollary 1.2.1.11. *We have* $H^i_{\text{ét}}(Y_{\Gamma,\overline{\mathbf{Q}}}, \widetilde{M}) \xrightarrow{\sim} H^i(\Gamma, M)$.

Proof. This is because

$$\begin{aligned} H^i_{\text{ét}}(Y_{\Gamma,\overline{\mathbf{Q}}}, \widetilde{M}) &= \varprojlim_n H^i_{\text{ét}}(Y_{\Gamma,\overline{\mathbf{Q}}}, \widetilde{M \otimes \mathcal{O}/\lambda^n}) \\ &\xrightarrow{\sim} \varprojlim_n H^i(Y_\Gamma(\mathbb{C}), \widetilde{M \otimes \mathcal{O}/\lambda^n}) \xrightarrow{\sim} \varprojlim_n H^i(\Gamma, M \otimes \mathcal{O}/\lambda^n) \xrightarrow{\sim} H^i(\Gamma, M), \end{aligned}$$

where the last step follows from the proposition above. □

By doing so, we equip $H^i(\Gamma, M)$ with a continuous Galois action of $G_{\mathbf{Q}}$, which commutes with the Hecke action. It is not hard to check that all the homomorphisms above preserve both actions. The Galois action on the group cohomology is rather simple in the following case [Buzzard et al., 2010, Lemma 2.2(a)].

Lemma 1.2.1.12 (Buzzard–Diamond–Jarvis)**.** *Let V be a finite dimensional vector space equipped with a Γ-action. The Galois action on $H^i(\Gamma, V)$ is abelian for $i \in \{0, 2\}$.*

Lemma 1.2.1.13. *If Γ is a p-torsion free congruence subgroup and $\mathfrak{n}$ is a non-Eisenstein maximal ideal of the Hecke algebra, then the functor $H^1(\Gamma, -)_{\mathfrak{n}}$ is an exact functor from the category of finite representations of $\mathrm{GL}_2(\mathbf{F}_p)$ to the category of abelian groups.*

Proof. Suppose that

$$0 \to V_1 \to V_2 \to V_3 \to 0$$

is a short exact sequence of finite representations of $\mathrm{GL}_2(\mathbf{F}_p)$ over $\overline{\mathbf{F}}_p$. Then we have the long exact sequence

$$\cdots \to H^0(\Gamma_{\varnothing}, V_3)_{\mathfrak{n}} \to H^1(\Gamma_{\varnothing}, V_1)_{\mathfrak{n}} \to H^1(\Gamma_{\varnothing}, V_2)_{\mathfrak{n}} \to H^1(\Gamma_{\varnothing}, V_3)_{\mathfrak{n}} \to H^2(\Gamma_{\varnothing}, V_1)_{\mathfrak{n}} \to \cdots .$$

By Lemma 1.2.1.12, the Galois action on H^0 and H^2 are abelian. If we assume $\mathfrak{n}$ is non-Eisenstein, then the image of $H^0(\Gamma_{\varnothing}, V_3)_{\mathfrak{n}}$ in $H^1(\Gamma_{\varnothing}, V_1)_{\mathfrak{n}}$ is trivial and so is the image of $H^1(\Gamma_{\varnothing}, V_3)_{\mathfrak{n}}$ in $H^2(\Gamma_{\varnothing}, V_1)$. □

1.2.2 Galois deformation theory

In this subsection, we review Galois deformation theory, which is essential for the discussion on patching in the sequel.

We fix a continuous representation $\overline{\rho} : G \to \mathrm{GL}_2(\mathbf{F})$ of some profinite group G and a character $\chi : G \to \mathcal{O}^\times$ such that $\chi \mod \lambda = \det(\overline{\rho})$. Let $\mathcal{C}_{\mathcal{O}}$ be the category of complete local Noetherian $\mathcal{O}$-algebras with residue field $\mathbf{F}$. By a lifting of $\overline{\rho}$ to a complete local Noetherian $\mathcal{O}$-algebra A, we mean a representation $\rho : G \to \mathrm{GL}_2(A)$ such that ρ reduces to $\overline{\rho}$ modulo the maximal ideal of A. Consider the functor $\mathbf{D}$ from $\mathcal{C}_{\mathcal{O}}$ to the category of sets that sends A to an equivalence class of liftings $\rho : G \to \mathrm{GL}_2(A)$ and $\det(\rho) = \chi$ where $\rho \sim \rho'$ if and only if $\rho' = g\rho g^{-1}$ for some $g \in 1 + M_2(A)$.

Theorem 1.2.2.1 (Mazur)**.** *If $\overline{\rho}$ is Schur and G satisfies Mazur's p-finiteness condition Φ_p, then the functor $\mathbf{D}$ is represented by an $\mathcal{O}$-algebra $R_{\overline{\rho}}^{\text{univ}}$, which we refer to as the universal deformation $\mathcal{O}$-algebra of $\overline{\rho}$.*

Remark 1.2.2.2. Recall that G satisfies Φ_p if for every open subgroup H of G, there are only finitely many continuous homomorphisms from H to $\mathbf{Z}_p$. For example, Mazur's p-finiteness condition is satisfied when G is the absolute Galois group of a local field or $G_{F,S}$ for some global field F and set S of finitely many places of F.

The tangent space of $\mathbf{D}$ is defined to be the set $\mathbf{D}(\mathbf{F}[\epsilon]/(\epsilon^2))$, which coincides with the notion of the Zariski tangent space of $\operatorname{Spec}(R_{\overline{\rho}}^{\text{univ}} \otimes \mathbf{F})$ and the group cohomology $H^1(G, \text{ad}^0\overline{\rho})$. Suppose that $\dim_{\mathbf{F}} H^1(G, \text{ad}^0\overline{\rho}) = d$. Then $R_{\overline{\rho}}^{\text{univ}}$ is a quotient of the power series ring $\mathcal{O}[\![x_1, \ldots, x_d]\!]$ by Nakayama's lemma.

We list some theorems that we use to compute the Galois cohomology with coefficients in $\text{ad}^0\overline{\rho}$.

Theorem 1.2.2.3 (Local Tate duality)**.** *Suppose that $G = G_{\mathbf{Q}_\ell}$ for a prime number ℓ. Then there is a perfect pairing*

$$H^i(G, \text{ad}^0\overline{\rho}) \times H^{2-i}(G, \text{ad}^0\overline{\rho}(1)) \to \mathbf{F}_p \quad \text{for} \quad i = 0, 1, 2$$

where $\text{ad}^0\overline{\rho}(1)$ stands for the module $\text{ad}^0\overline{\rho}$ on which the G-action is twisted by ω, the mod-p cyclotomic character.

For a proof, see [Milne, 2006, Theorem 2.1].

Theorem 1.2.2.4 (Local Euler characteristic formula)**.** *Suppose that $G = G_{\mathbf{Q}_p}$. Then*

$$\dim H^1(G, \text{ad}^0\overline{\rho}) = \dim H^0(G, \text{ad}^0\overline{\rho}) + \dim H^2(G, \text{ad}^0\overline{\rho}) + 3.$$

By the local Tate duality, this can be written into

$$\dim H^1(G, \mathrm{ad}^0\overline{\rho}) = \dim H^0(G, \mathrm{ad}^0\overline{\rho}) + \dim H^0(G, \mathrm{ad}^0\overline{\rho}(1)) + 3.$$

For a proof, see [Milne, 2006, Theorem 2.8].

Theorem 1.2.2.5 (Global Euler characteristic formula)**.** *Suppose that $G = G_{\mathbf{Q},S}$ for some finite set S of places of $\mathbf{Q}$ that contains p. Then*

$$\dim H^1(G, \mathrm{ad}^0\overline{\rho}) = \dim H^0(G, \mathrm{ad}^0\overline{\rho}) + \dim H^2(G, \mathrm{ad}^0\overline{\rho}) + 3 - \dim_{\mathbf{F}} H^0(G_{\mathbf{R}}, \mathrm{ad}^0\overline{\rho}).$$

For a proof, see [Milne, 2006, Theorem 5.1].

For a place v of $\mathbf{Q}$, we let I_v be the inertia subgroup of $G_{\mathbf{Q}_v}$ when v is finite and let I_v be the trivial group when v is infinite. Let $\mathcal{L} = \{L_v\}$ be a collection of subspaces $L_v \subseteq H^1(G_{\mathbf{Q}_v}, \mathrm{ad}^0\overline{\rho})$ where v runs over all the places of $\mathbf{Q}$ such that $L_v = H^1(G_{\mathbf{Q}_v}/I_v, (\mathrm{ad}^0\overline{\rho})^{I_v})$ for almost all v. Set $\mathcal{L}^* = \{L_v^\perp\}$ where $L_v^\perp$ is the annihilator of L_v under the Tate pairing, satisfies that $L_v^\perp = H^1(G_{\mathbf{Q}_v}/I_v, (\mathrm{ad}^0\overline{\rho}(1))^{I_v})$ for almost all v. We define the Selmer group $H_{\mathcal{L}}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ to be the subgroup of $H^1(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ that is the preimage of $\prod_v \mathcal{L}_v$ under the restriction map

$$H^1(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}) \to \prod_v H^1(G_{\mathbf{Q}_v}, \mathrm{ad}^0\overline{\rho}).$$

For example, the cohomology group $H^1(G_{\mathbf{Q},S}, \mathrm{ad}^0\overline{\rho})$ equals $H^1_{\mathcal{L}}(G_{\mathbf{Q},S}, \mathrm{ad}^0\overline{\rho})$ for $\mathcal{L} = \{L_v\}$ where $L_v = H^1(G_{\mathbf{Q}_v}/I_v, (\mathrm{ad}^0\overline{\rho}(1))^{I_v})$ if $v \notin S$ and $L_v = H^1(G_{\mathbf{Q}_v}, \mathrm{ad}^0\overline{\rho})$ otherwise.

Theorem 1.2.2.6 (Greenberg–Wiles)**.** *We have the formula*

$$\begin{aligned}\dim H^1_{\mathcal{L}}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}) - \dim H^1_{\mathcal{L}^*}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}(1)) = \dim(\mathrm{ad}^0\overline{\rho})^{G_{\mathbf{Q}}} - \dim(\mathrm{ad}^0\overline{\rho}(1))^{G_{\mathbf{Q}}} \\ + \sum_{v \le \infty} \left(\dim L_v - \dim(\mathrm{ad}^0\overline{\rho})^{G_{\mathbf{Q}_v}}\right),\end{aligned}$$

and we say $H^1_{\mathcal{L}}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ and $H^1_{\mathcal{L}^*}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}(1))$ are dual Selmer groups to each other.

For a proof, see [Darmon et al., 1995, Theorem 2.18].

Remark 1.2.2.7. When v is a finite place of $\mathbf{Q}$ and $L_v = H^1(G_{\mathbf{Q}_v}/I_v, (\mathrm{ad}^0\overline{\rho})^{I_v})$, we have that $\dim L_v = \dim(\mathrm{ad}^0\overline{\rho})^{G_{\mathbf{Q}_v}}$. Thus the sum in the theorem above is a finite sum.

The obstruction space of $\mathbf{D}$ is parametrized by $H^2(G, \mathrm{ad}^0\overline{\rho})$. When $H^2(G, \mathrm{ad}^0\overline{\rho}) = 0$, we say this deformation problem is unobstructed. In this case, the deformation ring $R^{\mathrm{univ}}_{\overline{\rho}}$ is isomorphic to the formal power series ring $\mathcal{O}[\![x_1, \ldots, x_d]\!]$.

Remark 1.2.2.8. If $\overline{\rho}$ is not Schur, we can consider the functor $\mathbf{D}^{\square}$ from $\mathcal{C}_{\mathcal{O}}$ to the category of sets that sends A to a lifting $\rho : G \to \mathrm{GL}_2(A)$ with $\det(\rho) = \chi$. This functor is represented by an $\mathcal{O}$-algebra $R^{\square}_{\overline{\rho}}$, which we refer to as the universal lifting ring. The Zariski tangent space of $\mathrm{Spec}(R^{\square}_{\overline{\rho}})$ is isomorphic to $Z^1(G, \mathrm{ad}^0\overline{\rho})$. The obstruction space is still parametrized by $H^2(G, \mathrm{ad}^0\overline{\rho})$. We can discuss whether a deformation functor is unobstructed, regardless of whether $\overline{\rho}$ is Schur.

Let $\overline{r} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathbf{F})$ be a local Galois representation. If $\overline{r}$ is irreducible, we assume $\overline{r} \sim \mathrm{Ind}^{G_{\mathbf{Q}_p}}_{G_K} \omega_2^{k_0-1}$ up to some twist. If $\overline{r}$ is reducible, we assume $\overline{r} \sim \begin{pmatrix} \omega^{k_0-1}\psi^{-1}\chi & b\psi \\ 0 & \psi \end{pmatrix}$ for some unramified characters ψ and χ and b a cochain in $Z^1(G_{\mathbf{Q}_p}, \omega^{k_0-1}\psi^{-2}\chi)$.

Proposition 1.2.2.9. *For the local Galois representation $\overline{r}$ as described, the deformation problem of $\overline{r}$ is unobstructed in the following cases:*

- *if $\overline{r}$ is irreducible and either $p \neq 3$ or $k_0 \neq 3$.*
- *if $\overline{r}$ is reducible and $k_0 \neq p - 1$.*

Proof. By definition of an unobstructed deformation problem and the Tate local duality, it suffices to compute when

$$\dim H^2(G_{\mathbf{Q}_p}, \mathrm{ad}^0\overline{r}) = \dim H^0(G_{\mathbf{Q}_p}, \mathrm{ad}^0\overline{r}(1)) = 0.$$

If $\overline{r}$ is irreducible, it follows from a direct computation that

$$\mathrm{ad}^0\overline{r} = \eta \oplus \mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega_2^{(p-1)(k_0-1)}$$

where η is the unramified character $\eta : G_{\mathbf{Q}_p} \to \mathrm{Gal}(K/\mathbf{Q}_p) \cong \{\pm 1\} \subset \mathbf{F}_p^\times$. Since $\eta(1)$ is a nontrivial character, it has no nontrivial fixed points. If $\left(\mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega_2^{(p-1)(k_0-1)}\right)(1)$ has nontrivial fixed points by $G_{\mathbf{Q}_p}$, it is reducible and thus

$$\omega_2^{(p-1)(k_0-1)} = \omega_2^{-(p-1)(k_0-1)}.$$

Given that ω_2 is cyclic of order $p^2 - 1$, the equality above is equivalent to

$$2(k_0 - 1) \equiv 0 \pmod{p+1}.$$

We deduce that $k_0 = (p+1)/2 + 1$ because $2 \le k_0 \le p$. Therefore, we have

$$\left(\mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega_2^{(p-1)(k_0-1)}\right)(1) = \left(\mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega^{(p-1)/2}\right)(1) = \omega^{(p+1)/2} \oplus \omega^{(p+1)/2} \otimes \eta.$$

Since $\omega^{(p+1)/2} \otimes \eta$ has no fixed points, the only fixed points of the induced representation are those of the character $\omega^{(p+1)/2}$. The condition $\omega^{(p+1)/2} = 1$ is true only when $p = 3$, which, in turn, implies that $k_0 = 3$.

If $\overline{r}$ is reducible, we want to find when the following equation in $x, y, z \in \mathbf{F}$ only has trivial solution.

$$\begin{pmatrix} \omega^{k_0-1}\psi^{-1}\chi & b\psi \\ 0 & \psi \end{pmatrix} \begin{pmatrix} x & y \\ z & -x \end{pmatrix} = \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \begin{pmatrix} \omega^{k_0}\psi^{-1}\chi & b\omega\psi \\ 0 & \omega\psi \end{pmatrix}.$$

The above equation of matrices is equivalent to the set of equations

$$\begin{cases} \omega^{k_0-1}\psi^{-1}\chi x + b\psi z = \omega^{k_0}\psi^{-1}\chi x \\ \omega^{k_0-1}\psi^{-1}\chi y - b\psi x = b\omega\psi x + \omega\psi y \\ \psi z = \omega^{k_0}\psi^{-1}\chi z \\ -\psi x = b\omega\psi z - \omega\psi x \end{cases}.$$

It follows from the third equation that $(\omega^{k_0} - \psi^2\chi^{-1})z = 0$. Since $p-1 \neq k_0$ and ω is cyclic of order $p-1$, the character ω^{k_0} is ramified. Hence, $z = 0$ because $\psi^2\chi^{-1}$ is unramified. Now we have $x(\omega - 1) = 0$ by the first equation. Thus x is also 0. We conclude from the second equation that $(\omega^{k_0-2} - \psi^2\chi^{-1})y = 0$. But $k_0 - 2 < p-1$ because $k_0 \leq p$. By a similar reasoning as with the third equation, we deduce that $y = 0$ and the proof is complete. □

For a finite extension E of $\mathbf{Q}_p$ with ring of integers $\mathcal{O}_E$, an $\mathcal{O}_E$-point of $\mathrm{Spec}(R_{\overline{r}}^{\mathrm{univ}})$ corresponds to an equivalence class of representations $r_E : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathcal{O}_E)$. After inverting p, we can say whether the deformation represented by r_E is crystalline of Hodge–Tate weights (a, b) for some integers a and b. Kisin defined $R_{\overline{r}}^k$ to be the quotient of $R_{\overline{r}}^{\mathrm{univ}}$ by the intersection of the kernels of the $\mathcal{O}_E$-points $R_{\overline{r}}^{\mathrm{univ}} \to \mathcal{O}_E$ such that the corresponding deformation r_E is crystalline of Hodge–Tate weights $(0, k-1)$. Kisin proved the following in [Kisin, 2008, (3.3.8)]

Proposition 1.2.2.10 (Kisin)**.** *The ring $R_{\overline{r}}^k$ is relative of dimension one over $\mathcal{O}$. Its generic fiber $R_{\overline{r}}^k[1/p]$ is formally smooth and equidimensional of dimension one.*

Example 1.2.2.11. The presentation of $R_{\overline{r}}^k$ is known when $\overline{r}$ is Schur and $2 \leq k \leq p+1$ by Fontaine–Laffaille theory Fontaine and Laffaille [1982]:

$$R_{\overline{r}}^k \xrightarrow{\sim} \mathcal{O}[\![x]\!].$$

When $\overline{r}$ is absolutely irreducible and $p+2 \leq k \leq 2p-1$, Kisin computed in Kisin [2007] that

$$R^k_{\overline{r}} \xrightarrow{\sim} \mathcal{O}[\![x,y]\!]/(xy-\lambda).$$

We now introduce notation for some global deformation rings. Let $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be an odd Galois representation that has the minimal ramification among all of its twists and satisfies the conditions outlined in Theorem 1.2.3.1. Denote by $\overline{r}$ and its restriction $\overline{\rho}|G_{\mathbf{Q}_p}$ is $\overline{r}$. Let S be the set $\{\ell, p, \infty\}_{\ell | N(\overline{\rho})}$. For a finite set Q of primes of $\mathbf{Q}$, we define R_Q as the global deformation $\mathcal{O}$-algebra that parametrizes deformations of $\overline{\rho}$ that are unramified outside $S \cup Q$, of types (A), (B), and (C) (for a detailed definition, refer to [Wiles, 1995, Chapter 1, Section 1]), at primes $\ell \in S$, and with a fixed determinant. We denote by R^k_Q the completed tensor product of R^k and R_Q over $R^{\mathrm{univ}}_{\overline{r}}$.

We can still make sense of the tangent space for these deformation rings. For a ring $R = R^k_{\overline{r}}, R_Q$ or R^k_Q, we denote by $\mathrm{Tan}(R)$ the $\mathbf{F}[\epsilon]/(\epsilon^2)$-points of R, i.e., $\mathrm{Hom}_{\mathcal{O}}(R, \mathbf{F}[\epsilon]/(\epsilon^2))$. We refer to $\mathrm{Tan}(R)$ the tangent space of R. The linear dual of $\mathrm{Tan}(R)$ is isomorphic to $\mathfrak{m}/\mathfrak{m}^2$ where $\mathfrak{m}$ is the maximal ideal of $R \otimes \mathbf{F}$. We call this the cotangent space of R and denote it by $\mathrm{Cot}(R)$. As before, the ring R is generated by $\dim_{\mathbf{F}} \mathrm{Tan}(R) = \dim_{\mathbf{F}} \mathrm{Cot}(R)$ many elements as an algebra over $\mathcal{O}$.

Proposition 1.2.2.12.

1. *The tangent space* $\mathrm{Tan}(R_Q)$ *is isomorphic to the Selmer group* $H^1(G_{\mathbf{Q},\{p,\infty\}\cup Q}, \mathrm{ad}^0\overline{\rho})$.

2. *The tangent space* $\mathrm{Tan}(R^k_Q)$ *is* $\mathrm{Tan}(R_Q) \times_{\mathrm{Tan}(R^{\mathrm{univ}}_{\overline{r}})} \mathrm{Tan}(R^k)$. *In particular, when* $R^{\mathrm{univ}}_{\overline{r}}$ *surjects onto* R_Q, *i.e.* $\mathrm{Tan}(R_Q) \subseteq \mathrm{Tan}(R^{\mathrm{univ}}_{\overline{r}})$, *we have* $\mathrm{Tan}(R^k_Q) = \mathrm{Tan}(R_Q) \cap \mathrm{Tan}(R^k)$.

Proof. Assertion (1) is proved by Wiles in [Wiles, 1995, (1.5)]. Assertion (2) follows from a general fact from the category theory that the covariant Hom functor turns a pushout diagram into a pullback diagram. □

1.2.3 Minimal level Taylor–Wiles–Kisin patching

In this subsection, we begin by outlining Theorem 1.2.3.1 which enables us to compute the crystalline deformation ring $R^k_{\overline{r}}$ by a certain Hecke algebra. We then review the setup and construction of the Taylor–Wiles–Kisin patching in the minimal level setting that will later be used in the algorithm's design.

Let $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be an odd absolutely irreducible Galois representation that has least ramification among all of its twists. Suppose that $\overline{r} := \overline{\rho}|_{G_{\mathbf{Q}_p}}$ is Schur and takes the form we have described in the previous subsection. We further assume when $\overline{r}$ is the extension of 1 by the cyclotomic character ω, the extension class is peu ramifié. By Serre's conjecture Serre [1987], Khare and Wintenberger [2009a,b], $\overline{\rho}$ is the reduction of the p-adic Galois representation attached to some newform f_0. Let $N(\overline{\rho})$ be the conductor of $\overline{\rho}$. The newform f_0 can be chosen so that it has level subgroup $\Gamma := \prod_{\ell \neq p} \Gamma_\ell$ where

$$\Gamma_\ell = \begin{cases} \Gamma_0(\ell) & \text{if } \ell \| N(\overline{\rho}) \text{ and } \det(\overline{\rho})|_{I_\ell} = 1 \\ \Gamma_1(\ell^r) & \text{if } \ell^r \| N(\overline{\rho}) \text{ and } r \geq 2 \text{ or } \det(\overline{\rho})|_{I_\ell} \neq 1 \end{cases},$$

and weight $2 \leq k_0 \leq p$. Then the Nebentypus character χ of f_0 satisfies $\chi|_{G_\ell} = 1$ if $\ell \| N(\overline{\rho})$ and $\chi|_{G_\ell} \equiv 1 \pmod{\lambda}$.

Theorem 1.2.3.1 (Taylor–Wiles–Kisin)**.** *Assume that $\overline{r}$ is Schur. If both of the following conditions hold:*

1. *$\overline{\rho}|_{G_{\mathbf{Q}(\zeta_p)}}$ is absolutely irreducible and*
2. *if $\ell \equiv -1 \mod p$ divides $N(\overline{\rho})$, then either $\overline{\rho}|_{G_{\mathbf{Q}_\ell}}$ is reducible over the algebraic closure or $\overline{\rho}|_{I_\ell}$ is absolutely irreducible,*

then the Taylor–Wiles–Kisin patching generates some patched module M^k_∞, whose support $\mathbb{T}^k_\infty$ is a formal power series ring over the crystalline deformation ring $R^k_{\overline{r}}$.

Remark 1.2.3.2. The theorem holds true without the assumption that $\overline{r}$ is Schur. In that case, the crystalline deformation ring $R_{\overline{r}}^{k}$ is replaced with the framed crystalline deformation ring $R_{\overline{r}}^{\square,k}$, which is constructed by Kisin in a similar manner as explained in the previous subsection with the universal deformation ring $R_{\overline{r}}^{\text{univ}}$ substituted with the universal lifting ring $R_{\overline{r}}^{\square}$ (see Remark 1.2.2.8). However, the framed deformation ring has a larger tangent space compared to the non-framed one. Currently we lack a way to identify the generators of the framed rings, unlike the method outlined in §1.3.2.

Let us briefly explain the two conditions in the theorem. The first condition is referred to as the Taylor–Wiles condition in the literature. It guarantees the adequacy of Taylor–Wiles primes (see Lemma 1.2.3.6), which is crucial for the construction of patching in Theorem 1.2.3.11. The second condition ensures that all the local deformation rings at places away from p are smooth. Without imposing condition (2), patching would yield a power series ring over the completed tensor product of all non-smooth local framed deformation rings, preventing us from obtaining a formal power series ring that is only over $R_{\overline{r}}^{k}$.

In practice, there are criteria to check when the Taylor–Wiles conditions hold. When the projective image of $\overline{\rho}$ contains $\mathrm{PSL}_2(\mathbf{F}_p)$ and $p \geq 5$, then (1) in (1.2.3.1) holds. But if the image happens to be small, there is a criterion [Calegari and Talebizadeh Sardari, 2021, Lemma 2.1.2(2)] to determine when this holds.

Lemma 1.2.3.3 (Calegari-Sardari)**.** *Assume that the local representation $\overline{r}$ is isomorphic to $\mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega_2^{k_0-1}$ up to a twist. The representation $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_p)}}$ is absolutely irreducible if $k_0 - 1$ is not divisible by $(p+1)/2$.*

For condition (2), if none of the prime divisors of $N(\overline{\rho})$ are congruent to -1 module p, then it automatically holds. There is also the following criterion from Wiles [1995]:

Lemma 1.2.3.4 (Wiles)**.** *If N is square-free, then (2) holds.*

We now review the construction of patching in more details, which is important in designing the algorithm. From now on we assume that $\overline{r}$ is Schur.

Definition 1.2.3.5. Define the following two Selmer groups.

- Denote by $H^1_\Sigma(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ the subspace of $H^1(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ that consists of cohomology classes that are unramified outside p and split at p.

- Denote by $H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ the subspace of $H^1(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ that consists of cohomology classes that are unramified outside $Q \cup \{p, \infty\}$ and split at p for a finite set Q of primes.

It is immediate from the definition that $H^1_\Sigma(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}) \subseteq H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$.

A set of level n Taylor–Wiles primes is a finite set Q_n of $\#Q_n$ primes q such that all of the following conditions hold:

1. if $q \in Q_n$, then q does not divide Np;

2. the cardinality of Q_n is $\#Q_n = \dim H^1(G_{\mathbf{Q},\{p,\infty\}}, \mathrm{ad}^0\overline{\rho}(1))$;

3. for all $q \in Q_n$, we have $q \equiv 1 \mod p^n$;

4. the element $\overline{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues $\overline{\alpha}_q$ and $\overline{\beta}_q$;

5. the Selmer groups $H^1_\Sigma(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ and $H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$ have the same dimension, which we denote as h.

It follows from Greenberg–Wiles formula that $\#Q_n = h + 1$.

Lemma 1.2.3.6 (Kisin [2009b])**.** *For each positive integer n, there is a set Q_n as above if condition (1) in Theorem 1.2.3.1 holds.*

We now introduce the notation for the Hecke algebras and modules that patch to $\mathbb{T}^k_\infty$ and M^k_∞, respectively. Recall that $\overline{\rho}$ comes from a newform f_0 of weight k_0, level $N(\overline{\rho})$ and Nebentypus character χ. Let $\widetilde{\mathbb{T}}^{\mathrm{univ}}$ be the polynomial ring $\mathcal{O}[T_\ell, \langle \ell \rangle]_{\ell \nmid N}$ in the indicated variables and let $\mathbb{T}^{\mathrm{univ}}$ be the sub-algebra of $\widetilde{\mathbb{T}}^{\mathrm{univ}}$ generated by all the variables but T_p. For a set Q of Taylor-Wiles primes, let N_Q be the product of all the primes q in Q. If $Q = \varnothing$, we set $N_Q = 1$. Denote by Γ_Q the intersection of the level group Γ of f_0 with the congruence subgroup $\Gamma_1(N_Q)$. We have the maximal ideal $\widetilde{\mathfrak{m}}_Q$ (resp. $\mathfrak{m}_Q$) of $\widetilde{\mathbb{T}}^{\text{univ}}$ (resp. $\mathbb{T}^{\text{univ}}$) that is generated by $\lambda, T_\ell - a_\ell(f), \langle \ell \rangle - \chi(\ell), T_q - \alpha_q, T_p$ for $\ell \nmid N(\overline{\rho})N_Q p$ and $q \in Q$ (resp. by $\lambda, T_\ell - a_\ell(f), \langle \ell \rangle - \chi(\ell), T_q - \alpha_q$, for $\ell \nmid N(\overline{\rho})N_Q p$ and $q \in Q$), where T_q acts by U_q and α_q is a lift of $\overline{\alpha}_q$ that is an eigenvalue of $\overline{\rho}(\text{Frob}_q)$. Since $\overline{\alpha}_q$ and $\overline{\beta}_q$ are distinct, we may and do assume that $\overline{\alpha}_q \neq 1$.

The choice of modules we patch can vary. The general idea is to patch modules on which Hecke algebras act faithfully. We consider (at least) two types of modules: the space of classical modular forms $S_k(\Gamma_Q, \overline{\mathbf{Q}}_p)$ and the space of group cohomology $H^1(\Gamma_Q, \text{Sym}^{k-2}\overline{\mathbf{Q}}_p{}^2)$. The Hecke algebra $\mathbf{Z}[T_\ell, \langle \ell \rangle]_{\ell \text{ prime}}$ acts on both modules by the double coset operators:

$$T_\ell := \left[\Gamma_Q \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \Gamma_Q\right] \quad \text{and} \quad \langle \ell \rangle := \left[\Gamma_Q \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma_Q\right]$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(NN_Q)$ and $d \equiv \ell \pmod N$. Let $g \in \text{GL}_2(\mathbf{Q})$ such that $g^{-1}\Gamma g$ and Γ are commensurable. Then $\Gamma_Q g \Gamma_Q$ is the finite disjoint union $\sqcup_i \Gamma g_i$ for some $g_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \text{GL}_2(\mathbf{Q})$. The double coset operator $[\Gamma_Q g \Gamma_Q]$ acts on $S_k(\Gamma, \overline{\mathbf{Q}}_p)$ by the following formula:

$$f[\Gamma_Q g \Gamma_Q] = \sum_i f[g_i] \quad \text{for} \quad f \in S_k(\Gamma, \overline{\mathbf{Q}}_p) \quad \text{where} \quad (f[g_i])(z) = \det(g_i)^{k-1}(c_i z + d_i)^{-k} f(g_i z).$$

The Hecke action on $H^1(\Gamma_Q, \text{Sym}^{k-2}\overline{\mathbf{Q}}_p^2)$ has been discussed in §1.2.1. We fix a field isomorphism $\mathbb{C} \xrightarrow{\sim} \overline{\mathbf{Q}}_p$. Over $\mathbb{C}$, the two modules are related by the following theorem.

Theorem 1.2.3.7 (Eichler-Shimura)**.** *Let Γ be a congruence subgroup of $\text{SL}_2(\mathbf{Z})$ and $k \geq 2$*

an integer. The map

$$f \mapsto \left(\gamma \mapsto \int_{z_0}^{\gamma z_0} f(z)(zu+v)^{(k-2)}\, dz\right)$$

induces an isomorphism

$$M_k(\Gamma,\mathbb{C}) \oplus \overline{S_k(\Gamma,\mathbb{C})} \xrightarrow{\sim} H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbb{C}^2)$$

that respects the Hecke action.

On both sides, the Hecke action is faithful. Thus in the process of patching, we can either use the module $S_k(\Gamma_Q,\mathcal{O})$ of classical modular forms of weight k, level Γ_Q with coefficients in $\mathcal{O}$ or the module $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$. The localizations of $S_k(\Gamma_Q,\mathcal{O})$ (resp. $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$) at $\widetilde{\mathfrak{m}}_Q$ and at $\mathfrak{m}_Q$ are the same when $\bar{r}$ is irreducible because T_p is automatically nilpotent modulo λ. When $\bar{r}$ is reducible, the module $S_k(\Gamma_Q,\mathcal{O})_{\mathfrak{m}_Q}$ splits into the direct sum $S_k(\Gamma_Q,\mathcal{O})_{\widetilde{\mathfrak{m}}_Q} \oplus S_k(\Gamma_Q,\mathcal{O})_{\widetilde{\mathfrak{m}}'_Q}$ where $\widetilde{\mathfrak{m}}'_Q$ is the maximal ideal of $\widetilde{\mathbb{T}}^{\mathrm{univ}}$ generated by $\lambda, T_\ell - a_\ell(f), \langle \ell\rangle - \chi(\ell), T_q - \alpha_q$ for all $\ell \nmid N(\bar{\rho})N_Q$.

Definition 1.2.3.8. Let $M(k,Q)$ be the localization $S_k(\Gamma_Q,\mathcal{O})_{\mathfrak{m}_Q}$ and let $M'(k,Q)$ be the localization $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)_{\mathfrak{m}_Q}$. Denote by $\widetilde{\mathbb{T}}(k,Q)$ the image of $\widetilde{\mathbb{T}}^{\mathrm{univ}}_{\widetilde{\mathfrak{m}}_Q}$ in the endomorphism ring of $M(k,Q)$ or $M'(k,Q)$ and by $\mathbb{T}(k,Q)$ the image of $\mathbb{T}^{\mathrm{univ}}_{\mathfrak{m}_Q}$ in the endomorphism ring of $M(k,Q)$ or $M'(k,Q)$.

Remark 1.2.3.9. Concretely, $M(k,Q)$ is the direct summand of $S_k(\Gamma_Q,\mathcal{O})$ determined by the condition that the action of $T \in \widetilde{\mathfrak{m}}_Q$ is topologically nilpotent. A similar characterization holds for $M'(k,Q) \subseteq H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$.

Let us recall the construction of the map from a formal power series ring over the crystalline deformation ring to Hecke algebras:

$$R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!] \twoheadrightarrow \mathbb{T}(k,Q).$$

First of all, since h is the dimension of the Selmer group

$$H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}) = \ker(H^1(G_{\mathbf{Q},S\cup Q}, \mathrm{ad}^0\overline{\rho}) \to H^1(G_{\mathbf{Q}_p}, \mathrm{ad}^0\overline{\rho})) = \ker(\mathrm{Tan}(R_Q) \to \mathrm{Tan}(R^{\mathrm{univ}}_{\overline{r}})),$$

there is a surjection

$$R^{\mathrm{univ}}_{\overline{r}}[\![t_1, \dots, t_h]\!] \twoheadrightarrow R_Q$$

and therefore a surjection

$$R^k_{\overline{r}}[\![t_1, \dots, t_h]\!] \twoheadrightarrow R^k_Q.$$

Note that h is independent of Q by the construction of Q.

It remains to construct the homomorphism $\varphi : R^k_Q \to \mathbb{T}(k, Q)$. Since the algebra $\mathbb{T}(k, Q)$ is finite free over $\mathcal{O}$, given a minimal prime ideal $\mathfrak{p}$ of $\mathbb{T}(k, Q)$, the quotient $\mathbb{T}(k, Q)/\mathfrak{p}$ is embedded in the ring of integers of a finite extension of L. Such an embedding corresponds to a system of Hecke eigenvalues, or equivalently, a Galois orbit of an eigenform f and thus a Galois representation ρ_f by Deligne's construction Deligne [1969]. Let S be the set containing p, ∞ and primes dividing $N(\overline{\rho})$. There is the representation

$$\rho^{k,\mathrm{mod}}_Q : G_{\mathbf{Q},S\cup Q} \to \prod_{\mathfrak{p} \text{ minimal}} \mathrm{GL}_2(\mathbb{T}(k, Q)/\mathfrak{p}),$$

with the trace of Frob_ℓ being $T_\ell \in \mathbb{T}(k, Q)$ where ℓ is a prime not in $S \cup Q$. It follows from Chebotarev's density theorem that the trace of $\rho^{k,\mathrm{mod}}_Q$ lands in $\mathbb{T}(k, Q)$. Since $\overline{\rho}$ is absolutely irreducible, by Carayol's lemma Carayol [1994], we may and do assume that $\rho^{k,\mathrm{mod}}_Q$ has its image in $\mathrm{GL}_2(\mathbb{T}(k, Q))$. We then obtain a homomorphism $\varphi : R^k_Q \to \mathbb{T}(k, Q)$ by the universal property of R^k_Q.

Lemma 1.2.3.10. *The Hecke operator U_q is in $\mathrm{Im}\,(\varphi)$ for every prime $q \in Q$.*

Proof. Let f be an eigenform in its Galois orbit corresponding to a minimal prime ideal $\mathfrak{p}$ of $\mathbb{T}(k, Q)$. Then by construction of $\mathbb{T}(k, Q)$, the eigenform f is either new at $q \in Q$

of conductor 1 or an old form with trivial conductor because the level group at $q \in Q$ is $\Gamma_1(q)$. It follows from [LOEFFLER and WEINSTEIN, 2012, Table 1] that the q-component automorphic representation $\pi_{f,q}$ of f is a principal series $\pi(\chi_{f,1}, \psi_{f,q}/\chi_{f,1})$ where $\chi_{f,1}$ is an unramified character of $\mathbf{Q}_q^\times$ and $\psi_{f,q}$ is the q-component of the Nebentypus character of f. When f is new at q, $\chi_{f,1}$ sends q to $a_q(f)q^{-(k-1)/2}$. When f is an old form, $\chi_{f,1}(q)$ sends q to $\alpha_q q^{-(k-1)/2}$ where α_q is determined by $U_q f = \alpha_q f$. Again, by construction of $\mathbb{T}(k,Q)$, the numbers $a_q(f)$ and α_q are congruent to $\overline{\alpha}_q$ modulo λ, which is equivalent to saying U_q is congruent to $\overline{\alpha}_q$ modulo $\mathfrak{m}_Q$. By the classical local Langlands correspondence and Grothendieck's monodromy theorem, the Galois representation attached to f has trace $(\chi_{f,1} + \psi_{f,q}/\chi_{f,1})\chi_{\text{cyc}}^{(k-1)/2}$. Thus for a lift $\sigma \in G_{\mathbf{Q}_q}$ of Frob_q, we have

$$U_q + \frac{q^{k-1}(\psi_{f,q}(\sigma))_f}{U_q} = A \qquad \text{for some } A \in \text{Im}\,(\varphi),$$

where we note that $(\psi_{f,q}(\sigma))_f$ is also in $\text{Im}\,(\varphi)$ as it comes from the determinant of ρ_Q^{mod}. Now we have a quadratic equation

$$X^2 - AX + q^{k-1}(\psi_{f,q}(\sigma))_f = 0$$

with two distinct roots $\overline{\alpha}_q$ and $\overline{\beta}_q$ after modulo $\mathfrak{m}_Q$. By Hensel's lemma, the equation has a unique root in $\mathbb{T}(k,Q)$ which is U_q and a unique root in $\text{Im}\,(\varphi) \subseteq \mathbb{T}(k,Q)$. Therefor U_q is in $\text{Im}\,(\varphi)$. (Since $\text{Im}\,(\varphi)$ is the image of $R^k_{\overline{\rho},Q}$, it is automatically a complete local Noetherian ring with maximal ideal being the quotient of the maximal ideal $\mathfrak{m}$ of $R^k_{\overline{\rho},Q}$. On the other hand, the map φ comes from universal property, and thus it is a local map, meaning that the preimage of $\mathfrak{m}_Q$ is $\mathfrak{m}$. Thus the subspace topology on $\text{Im}\,(\varphi)$ coincided with the quotient topology on $\text{Im}\,(\varphi)$, so there is no ambiguity with applying Hensel's lemma to $\text{Im}\,(\varphi)$ here.) $\square$

As a result of the lemma, the composition $R^k_{\overline{r}}[\![t_1, \ldots, t_h]\!] \twoheadrightarrow R^k_{\overline{\rho},Q} \to \mathbb{T}(k,Q)$ is surjective.

There are no canonical maps between $\mathbb{T}(k, Q)$ and $\mathbb{T}(k, Q')$ when Q and Q' are two distinct non-empty sets of Taylor–Wiles primes. However, patching gives identification on some finite quotients of $\mathbb{T}(k, Q)$. Using the notation above, there is a reformulation of Theorem 1.2.3.1 as follows.

Theorem 1.2.3.11 (Reformulation of Theorem 1.2.3.1)**.** *Under the assumption of (1.2.3.1), there exists a sequence $\{Q_n\}$ of sets of Taylor-Wiles primes such that*

$$M^k_\infty \xrightarrow{\sim} \varprojlim_n M(k, Q_n) \otimes \mathcal{O}/\lambda^n \quad \text{and} \quad {M'}^k_\infty \xrightarrow{\sim} \varprojlim_n M'(k, Q_n) \otimes \mathcal{O}/\lambda^n$$

and both modules have support

$$\mathbb{T}^k_\infty \xrightarrow{\sim} \varprojlim_n \mathbb{T}(k, Q_n) \otimes \mathcal{O}/\lambda^n \xrightarrow{\sim} R^k_{\bar{r}}[\![t_1, \dots, t_h]\!]$$

for some non-canonical surjective transition maps between the Hecke modules and Hecke algebras.

The homomorphisms above all preserve the action of an Iwasawa algebra, which we now describe. Let Δ_q be the maximal p-power quotient of $\mathbf{F}_q^\times$ and denote by Δ_Q the product of Δ_q for q in a set Q of Taylor–Wiles primes. There is a ring homomorphism $\mathcal{O}[\Delta_Q] \to R^k_Q$ that comes from the Taylor–Wiles deformation ring. Since Δ_Q is a group of diamond operators of p-power order, it embeds in the Hecke algebra $\mathbb{T}(k, Q)$. By [Gee, 2013, Proposition 5.8], φ is an $\mathcal{O}[\Delta_Q]$-homomorphism. Let $\mathcal{O}[\![\Delta_\infty]\!] := \mathcal{O}[\![d_1, \dots, d_{\#Q}]\!]$ be the formal power series ring over $\mathcal{O}$ in $\#Q$ variables. We have a commutative diagram

$$\begin{array}{ccccc} & & R^k_{\bar{r}}[\![t_1, \dots, t_h]\!] & \xrightarrow{\sim} & \mathbb{T}^k_\infty \\ & \nearrow^{\cdots} & \downarrow\!\!\!\!\downarrow & & \downarrow\!\!\!\!\downarrow \\ \mathcal{O}[\![\Delta_\infty]\!] & \longrightarrow & R_Q & \twoheadrightarrow & \mathbb{T}(k, Q) \end{array} \tag{1.2.3.12}$$

The dotted map exists because $\mathcal{O}[\![\Delta_\infty]\!]$ is formally smooth. Denote by $\mathfrak{a}_Q$ the kernel of

$\mathcal{O}[\![\Delta_\infty]\!] \twoheadrightarrow \mathcal{O}[\Delta_Q]$. Then we have

$$R^k_Q \xrightarrow{\sim} R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!]/\mathfrak{a}_Q R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!].$$

On the finite level, Kisin proved the following in Kisin [2009a].

Corollary 1.2.3.13 ($R[1/p] = \mathbb{T}[1/p]$, Taylor–Wiles–Kisin)**.** *The surjection $R_Q \to \mathbb{T}(k,Q)$ induces an isomorphism $R_Q[1/p] \xrightarrow{\sim} \mathbb{T}(k,Q)[1/p]$.*

Remark 1.2.3.14. Let Q be a set of level n Taylor–Wiles primes. The images of $\lambda, (1+d_1)^{p^n} - 1, \ldots, (1+d_{\#Q})^{p^n} - 1$ in $R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!]$ form a system of parameters of $R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!]$ because

$$R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!]/(\lambda, (1+d_1)^{p^n} - 1, \ldots, (1+d_{\#Q})^{p^n} - 1) \xrightarrow{\sim} R^k_Q \otimes \mathbf{F}$$

is Artinian. The ring $R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!]$ is Cohen–Macaulay if and only if $\lambda, (1+d_1)^{p^n} - 1, \ldots, (1+d_{\#Q})^{p^n} - 1$ is a regular sequence. The latter implies that

$$R^k_Q \xrightarrow{\sim} R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!]/((1+d_1)^{p^n} - 1, \ldots, (1+d_{\#Q})^{p^n} - 1)$$

is λ-torsion free. We can then upgrade the $R[1/p] = \mathbb{T}[1/p]$ in the corollary above to an $R = \mathbb{T}$ theorem. For instance, the $R = \mathbb{T}$ theorem holds in the situations described in Example 1.2.2.11.

Proposition 1.2.3.15. *Under assumptions in Theorem 1.2.3.1, the following are equivalent:*

1. *$R^k_{\bar{r}}$ is Cohen–Macaulay;*
2. *$R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!] \otimes \mathbf{F}$ is finite free over $\mathbf{F}[\![d_1,\ldots,d_{\#Q}]\!]$.*

The same statement holds true for $R^k_{\bar{r}}[\alpha_p]$.

Proof. If (2) holds, then $(\lambda, d_1, \ldots, d_{\#Q})$ is a regular sequence of $R^k_{\bar{r}}[\![t_1,\ldots,t_h]\!]$ and (1) follows. Conversely, if $R^k_{\bar{r}}$ is Cohen–Macaulay, then the system of parameters $(\lambda, d_1, \ldots, d_{\#Q})$

is a regular sequence of the Cohen–Macaulay ring $R^k_{\bar{r}}[\![t_1, \dots, t_h]\!]$. Thus $R^k_{\bar{r}}[\![t_1, \dots, r_h]\!] \otimes \mathbf{F}$ is Cohen–Macaulay with a regular sequence $(d_1, \dots, d_{\#Q})$. As a result, $R^k_{\bar{r}}[\![t_1, \dots, r_h]\!] \otimes \mathbf{F}$ is a Cohen–Macaulay module over $\mathbf{F}[\![d_1, \dots, d_{\#Q}]\!]$. Apply the Auslander–Buchsbaum formula to $R^k_{\bar{r}}[\![t_1, \dots, r_h]\!] \otimes \mathbf{F}$ and we see that the projective dimension of $R^k_{\bar{r}}[\![t_1, \dots, r_h]\!] \otimes \mathbf{F}$ is 0. Thus $R^k_{\bar{r}}[\![t_1, \dots, r_h]\!] \otimes \mathbf{F}$ is projective as an $\mathbf{F}[\![d_1, \dots, d_{\#Q}]\!]$-module and therefore free because $\mathbf{F}[\![d_1, \dots, d_{\#Q}]\!]$ is local. □

We can also patch $\widetilde{\mathbb{T}}(k, Q)$ to get a power series ring over a ring slightly different from the crystalline deformation ring $R^k_{\bar{r}}$ which we now explain. Recall that $G_{\mathbf{Q}_p}$-crystalline representations are classified by weakly adimissible filtered φ-modules. Let $(R^k_{\bar{r}})^{\mathrm{an}}$ be the ring of rigid analytic functions on the generic fiber of the rigid analytic space associated to $\mathrm{Spf}(R^k_{\bar{r}})$. Over $(R^k_{\bar{r}})^{\mathrm{an}}$, we may consider the universal filtered φ-module and the universal Weil group representation (obtained by forgetting the filtration). The trace of φ determines an element in $R^k_{\bar{r}}$ which we will denote by α_p. The following theorem follows from Caraiani et al. [2018]. All the homomorphisms here also respect the $\mathcal{O}[\![\Delta_\infty]\!]$-action.

Theorem 1.2.3.16 (Caraiani–Emerton–Gee–Geraghty–Paškūnas–Shin)**.** *Under the assumption of (1.2.3.1), there is a sequence $\{Q_n\}$ of sets of Taylor-Wiles primes such that*

$$\varprojlim_n \widetilde{\mathbb{T}}(k, Q_n) \otimes \mathcal{O}/\lambda^n \xrightarrow{\sim} R^k_{\bar{r}}[\alpha_p][\![t_1, \dots, t_h]\!].$$

The element α_p is mapped to $T_p \in \widetilde{\mathbb{T}}(k, Q_n)$ under this identification. The ring $R^k_{\bar{r}}[\alpha_p]$ is in the normalization of $R^k_{\bar{r}}$ in $R^k_{\bar{r}}[1/p]$.

In particular, we have

$$R^k_{\bar{r}} \xrightarrow{\sim} R^k_{\bar{r}}[\alpha_p]$$

when $\bar{r}$ is absolutely irreducible and $2 \leq k \leq 2p-1$ because the crystalline deformation ring $R^k_{\bar{r}}$ is normal by Example 1.2.2.11.

The key idea of the algorithm is to apply the patching theorems to compute arbitrarily close approximations of the rings R^k and $R^k_{\overline{r}}[\alpha_p]$ by computing $\mathbb{T}(k, Q_n)$ and $\widetilde{\mathbb{T}}(k, Q_n)$.

1.2.4 The Breuil–Mézard conjecture and the rank of $M(k,Q)$ and $M'(k,Q)$

In this subsection, we study the rank of $M(k,Q)$ and $M'(k,Q)$ using the geometric Breuil–Mézard conjecture.

The Eichler–Shimura isomorphism 1.2.3.7 does not preserve the integral structure of both sides. The space of classical modular forms $S_k(\Gamma_Q, \mathcal{O})$ is a finite free $\mathcal{O}$-module and it follows that $M(k,Q) \subseteq S_k(\Gamma_Q, \mathcal{O})$ is automatically finite free over $\mathcal{O}$. But $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ usually contains torsion, as we pointed out in Remark 1.2.1.9; so it is not clear whether $M'(k,Q)$ is torsion-free.

Proposition 1.2.4.1.

1. *If Γ_Q is p-torsion free, then $M'(k,Q)$ is a free $\mathcal{O}$-module;*

2. $2\,\mathrm{rank}_{\mathcal{O}} M(k,Q) = \mathrm{rank}_{\mathcal{O}} M'(k,Q)$.

Proof. Recall from Remark 1.2.3.9 that $M'(k,Q)$ is a submodule of $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$. Thus by Proposition 1.2.1.1, we have

$$M'(k,Q)[\lambda] \subseteq H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)[\lambda] = \mathrm{Im}\,(H^0(\Gamma_Q, \mathrm{Sym}^{k-2}\mathbf{F}^2) \to H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)).$$

The Galois action on $H^0(\Gamma_Q, \mathrm{Sym}^{k-2}\mathbf{F}^2)$ is abelian by Lemma 1.2.1.12 and therefore reducible. However, the Galois action on $M'(k,Q)$ is absolutely irreducible because it is obtained from localization at a non-Eisenstein maximal ideal $\mathfrak{m}_Q$. Thus $M'(k,Q)[\lambda] = 0$ and (1) is proved. Assertion (2) follows directly from the Eichler–Shimura isomorphism and the assumption that $\mathfrak{m}_Q$ is non-Eisenstein. $\square$

The rank of $M(k,Q)$ or $M'(k,Q)$ can be described using the geometric Breuil–Mézard conjecture studied by Emerton–Gee in Emerton and Gee [2014]. In the rest of the subsection, we will work with $\overline{r}$ not necessarily Schur and we switch to the framed crystalline deformation ring $R_{\overline{r}}^{\square,k}$. Denote by $Z(\mathrm{Spec}(R_{\overline{r}}^{\square,k}\otimes\mathbf{F}))$ the four-dimensional algebraic cycle of the special fiber of $R_{\overline{r}}^{\square,k}$. Suppose that the semisimplification of the $\mathrm{GL}_2(\mathbf{F}_p)$-representation $\mathrm{Sym}^{k-2}\mathbf{F}^2$ decomposes into the direct sum of irreducible representations

$$\left(\mathrm{Sym}^{k-2}\mathbf{F}^2\right)^{\mathrm{ss}} \xrightarrow{\sim} \bigoplus_{m,n}(\det{}^m\otimes\mathrm{Sym}^n\mathbf{F}^2)^{\oplus b_{m,n}}$$

where $0\le m\le p-2$ and $0\le n\le p-1$ are integers and $b_{m,n}$'s are multiplicities. Emerton and Gee formulated the geometric Breuil-Mézard conjecture [Emerton and Gee, 2014, Conjecture 3.1.4] and proved it in many cases([Emerton and Gee, 2014, Theorem 3.1.6]):

Theorem 1.2.4.2 (Emerton-Gee). *If* $\overline{r}\not\sim\begin{pmatrix}\omega\chi & *\\ 0 & \chi\end{pmatrix}$ *for any character* χ*, then for each* $0\le m\le p-2$ *and* $0\le n\le p-1$*, there is a cycle* $\mathcal{C}_{m,n}$ *depending only on* m,n *and* $\overline{r}$ *such that*

$$Z(\mathrm{Spec}(R_{\overline{r}}^{k,\square}\otimes\mathbf{F}))=\sum_{m,n}a_{m,n}\mathcal{C}_{m,n},$$

where $a_{m,n}$ *equals* $b_{m,n}$ *if* $\det^m\otimes\mathrm{Sym}^{n-2}\mathbf{F}^2$ *is a Serre weight of* $\overline{r}$ *and vanishes otherwise.*

We now can describe the $\mathcal{O}$-rank of the module $M'(Q,k)$.

Lemma 1.2.4.3. *Assume that the torsion of the initial level group* $\Gamma_\varnothing$ *is a subgroup of* $\{\pm I\}$*. Then*

$$\mathrm{rank}_{\mathcal{O}}M'(Q,k)=\#\Delta_Q\cdot\sum_{m,n}a_{m,n}\dim_{\mathbf{F}}H^1(\Gamma_\varnothing,\mathrm{Sym}^n\mathbf{F}^2)_{\mathfrak{m}_\varnothing[-m]},$$

where $\mathfrak{m}_\varnothing[-m]$ *stands for the maximal ideal* $(\lambda,T_\ell-\ell^{-m}a_\ell(f),\langle\ell\rangle-\chi(\ell))_{\ell\nmid Np}$ *of* $\mathbb{T}^{\mathrm{univ}}$.

Proof. Since $M'(Q,k)$ is finite free over $\mathcal{O}[\Delta_Q]$ of rank equal to the $\mathcal{O}$-rank of $M'(\varnothing,k)$, it suffices to show

$$\operatorname{rank}_{\mathcal{O}} M'(\varnothing, k) = \sum_{m,n} a_{m,n} \dim_{\mathbf{F}} H^1(\Gamma_\varnothing, \operatorname{Sym}^n \mathbf{F}^2)_{\mathfrak{m}_\varnothing[-m]}.$$

Since $M'(\varnothing, k)$ is torsion free by Proposition 1.2.4.1 (1), we have

$$\operatorname{rank}_{\mathcal{O}} M'(\varnothing, k) = \dim_{\mathbf{F}} M'(\varnothing, k) \otimes \mathbf{F} = \dim_{\mathbf{F}} H^1(\Gamma_\varnothing, \operatorname{Sym}^{k-2} \mathcal{O}^2)_{\mathfrak{m}_\varnothing} \otimes \mathbf{F}.$$

It follows from Corollary 1.2.1.4 that

$$H^1(\Gamma_\varnothing, \operatorname{Sym}^{k-2} \mathcal{O}^2)_{\mathfrak{m}_\varnothing} \otimes \mathbf{F} = H^1(\Gamma_\varnothing, \operatorname{Sym}^{k-2} \mathbf{F}^2)_{\mathfrak{m}_\varnothing}.$$

By Lemma 1.2.1.13, the dimensions satisfy

$$\dim H^1(\Gamma_\varnothing, \operatorname{Sym}^{k-2} \mathbf{F}^2)_{\mathfrak{m}_\varnothing} = \sum_{m,n} b_{m,n} \dim_{\mathbf{F}} H^1(\Gamma_\varnothing, \det^m \otimes \operatorname{Sym}^n \mathbf{F}^2)_{\mathfrak{m}_\varnothing}$$

Since $\dim_{\mathbf{F}} H^1(\Gamma, \det^m \otimes \operatorname{Sym}^n \mathbf{F}^2)_{\mathfrak{m}_Q} = 0$ unless $\det^m \otimes \operatorname{Sym}^n \mathbf{F}^2$ is a Serre weight of $\overline{\rho}$, the quantity above is equal to

$$\sum_{m,n} a_{m,n} \dim_{\mathbf{F}} H^1(\Gamma_\varnothing, \det^m \otimes \operatorname{Sym}^n \mathbf{F}^2)_{\mathfrak{m}_\varnothing} = \sum_{m,n} a_{m,n} \dim_{\mathbf{F}} H^1(\Gamma_\varnothing, \operatorname{Sym}^n \mathbf{F}^2)_{\mathfrak{m}_\varnothing[-m]},$$

and we conclude the equality in the lemma. □

Remark 1.2.4.4. In all the examples in the paper, the dimension of $H^1(\Gamma_\varnothing, \det^m \otimes \operatorname{Sym}^n \mathbf{F}^2)_{\mathfrak{m}_\varnothing}$ is always 2 if $\det^m \otimes \operatorname{Sym}^n \mathbf{F}^2$ is a Serre weight of $\overline{r}$.

Proposition 1.2.4.5. *The multiplicity μ of the component of $\operatorname{Spec}(R^k_{\overline{r}} \otimes \mathbf{F})$ corresponding to $\overline{r}$ is 3 when $k = k_0 + p^2 - 1$ and $\mu = 2$ when $k_0 + p - 1 < k < k_0 + p^2 - 1$.*

Proof. For simplicity, we write Sym^i for $\operatorname{Sym}^i \mathbf{F}^2$.

Let $n_0 = p+1-k_0$. For any integer $n \in [0, p-2]$, the Serre weights of $\mathrm{Sym}^{k_0-2+n(p+1)}$ are $\mathrm{Sym}^{[k_0-2+2n]}$ and $\det^{[k_0-2+2n]} \otimes \mathrm{Sym}^{p-1-[k_0-2+2n]}$, where $[x] \in \{0, 1, \ldots, p-2\}$ represents the residue class of x in $\mathbf{Z}/(p-1)$. The factor $\det^n \otimes \mathrm{Sym}^{k_0-2}$ appears as a Serre weight of $\mathrm{Sym}^{k_0-2+n(p+1)}$ only if

$$\begin{cases} n = [k_0 - 2 + 2n] \\ n + k_0 - 2 = p - 1 \end{cases}.$$

It follows that this can only happen when $n = n_0$.

Suppose that $k_0 \geq 3$. We first show that when $0 \leq n \leq n_0 - 1$, the factor $\mathrm{Sym}^{k_0-2} \otimes \det^n$ appears with multiplicity 1 in the semisimplification of $\mathrm{Sym}^{k_0-2+n(p+1)}$. This is clear when $n = 0$ and then we proceed by induction on n. We have the recurrence relation

$$\mathrm{Sym}^{k_0-2+n(p+1)} \sim \det \otimes \mathrm{Sym}^{k_0-2+(n-1)(p+1)} + \mathrm{Sym}^{[k_0-2+2n]} \\ + \det^{[k_0-2+(n-1)(p+1)]} \otimes \mathrm{Sym}^{p-1-[k_0-2+(n-1)(p+1)]}.$$

Since $\mathrm{Sym}^{k_0-2} \otimes \det^{n-1}$ appears with multiplicity 1 in $\mathrm{Sym}^{k_0-2+(n-1)(p+1)}$ and $\mathrm{Sym}^{k_0-2} \otimes \det^n$ is not a Serre weight of $\mathrm{Sym}^{k_0-2+n(p-1)}$, the conclusion follows. It follows from a similar argument that the factor $\mathrm{Sym}^{k_0-2} \otimes \det^n$ appears with multiplicity 2 in the semisimplification of $\mathrm{Sym}^{k_0-2+n(p+1)}$, when $n_0 \leq n \leq p-2$. And once again by the recurrence relation, the factor Sym^{k_0-2} appears with multiplicity 3 in the semisimplification of $\mathrm{Sym}^{k_0-2+p^2-1}$ and we have proved the first half of the statement when $3 \leq k_0 \leq p$. For the second half, by a similar argument, when $0 \leq n \leq p - k_0 - 1$, the factor $\det^{n+1} \otimes \mathrm{Sym}^{k_0-2}$ appears in $\mathrm{Sym}^{k_0+n(p+1)}$ with multiplicity 0; when $p - k_0 \leq n \leq p-3$, the factor $\det^{n+1} \otimes \mathrm{Sym}^{k_0-2}$ appears in $\mathrm{Sym}^{k_0+n(p+1)}$ with multiplicity 1; and the factor Sym^{k_0-2} appears in $\mathrm{Sym}^{k_0+(p-2)(p+1)} = \mathrm{Sym}^{k_0-2+p(p-1)}$ with multiplicity 2.

In the case where $k_0 = 2$, the Serre weights are 1 and $\mathrm{Sym}^{p-1}\mathbf{F}^2$. We show that for $1 \leq i \leq p-2, i \in \mathbf{Z}$, the semisimplification of $\mathrm{Sym}^{(p+1)i-(p-1)}$ does not contain the factors

$\det^i$ or $\det^i \otimes \mathrm{Sym}^{p-1}$. When $i = 1$, this is obvious. For $2 \leq i \leq p-2$, we have

$$\mathrm{Sym}^{(p+1)i-(p-1)} \sim \det \otimes \mathrm{Sym}^{(p+1)(i-1)-(p-1)} + \mathrm{Sym}^{[(p+1)i]} + \det^{[(p+1)i]} \otimes \mathrm{Sym}^{(p-1)-[(p+1)i]},$$

where $[r] \in \{0, 1, \ldots, p-2\}$ is the representative of the image of r in $\mathbf{Z}/(p-1)\mathbf{Z}$. Since $1 \leq i \leq p-2$, we have $i \neq 0$ and $(p+1)i \not\equiv i \pmod{p-1}$. Hence $\det^i \neq 1$ and $\det^i \neq \det^{[(p+1)i]}$. By induction on i, we are done. In the same way, we show that for $0 \leq i \leq p-2, i \in \mathbf{Z}$, the semisimplification of $\mathrm{Sym}^{(p+1)i}$ contains $\det^i$ with multiplicity 1 and contains no $\det^i \otimes \mathrm{Sym}^{p-1}$. Now

$$\mathrm{Sym}^{p(p-1)} \sim \det \otimes \mathrm{Sym}^{(p+1)(p-2)-(p-1)} + 1 + \mathrm{Sym}^{p-1}$$

contains 1 and Sym^{p-1} with multiplicity 1 and

$$\mathrm{Sym}^{(p+1)(p-1)} \sim \det \otimes \mathrm{Sym}^{(p+1)(p-2)} + 1 + \mathrm{Sym}^{p-1}$$

contains 1 with multiplicity 2 and Sym^{p-1} with multiplicity 1. $\square$

1.3 The Algorithm

Let $\overline{r} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathbf{F})$ be a local residual representation as described in §1.2.2 that is Schur and the deformation problem of $\overline{r}$ is unobstructed. Assume the extension class to be peu ramifié if $\overline{r}$ is the extension of 1 by the cyclotomic character ω. Suppose that we can choose an odd global representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ such that $\overline{r} \xrightarrow{\sim} \overline{\rho}|_{G_{\mathbf{Q}_p}}$. Assume that $\overline{\rho}$ has the least ramification among all of its twists and it satisfies the conditions in Theorem 1.2.3.1. The representation $\overline{\rho}$ comes from a newform f of level Γ, Nebentypus character χ and weight $2 \leq k_0 \leq p$ as described in §1.2.3. Given $\overline{\rho}$ as an input, we present an algorithm to compute the presentations of local Hecke algebras $\mathbb{T}(k, Q_n)$ and $\widetilde{\mathbb{T}}(k, Q_n)$ with arbitrary

p-adic precision for every weight k and every set Q_n of level n Taylor–Wiles primes. The algorithm consists of three steps. First, we determine the local conditions that cut out $M(k,Q)$ from $S_k(\Gamma_Q,\chi,\mathcal{O})$ or $M'(k,Q)$ from $H^1(\Gamma_Q,\mathrm{Sym}^{k-2}\mathcal{O}^2)$. Next, we determine a set of generators for $\mathbb{T}(k,Q_n)$ and $\widetilde{\mathbb{T}}(k,Q_n)$ as $\mathcal{O}$-algebras using classical modular forms $M(k,Q)$. At last, we compute the relations among these generators using cohomological modular forms $M'(k,Q)$. We require extra assumptions on $\overline{\rho}$ in the second step, but the third step involves purely linear algebra and relies solely on the output of the first two steps.

1.3.1 Local conditions

This step is to determine the local conditions that cut out $M(k,Q)$ from $S_k(\Gamma_Q,\chi,\mathcal{O})$ or $M'(k,Q)$ from $H^1(\Gamma_Q,\mathrm{Sym}^{k-2}\mathcal{O}^2)$. It is equivalent to computing a finite set of the generators of the image of the maximal ideal $\mathfrak{m}_Q$ in $\mathrm{End}_{\mathcal{O}}(S_k(\Gamma_Q,\chi,\mathcal{O}))$. We start with assuming $Q=\varnothing$. Denote by $\mathbb{T}_k$ the image of $\mathbb{T}^{\mathrm{univ}}$ in $\mathrm{End}_{\mathcal{O}}(S_k(\Gamma_\varnothing,\chi,\mathcal{O}))$.

Remark 1.3.1.1. The generators of $\mathfrak{m}_\varnothing\mathbb{T}_k$ can be different from the those of $\mathfrak{m}_\varnothing\mathbb{T}(k,\varnothing)$. This is because after localization, the number of generators usually goes down. A typical example is the localization of the ring of integers of a number field. This ring is usually not a principal ideal domain, but its localization at every maximal ideal is a discrete valuation ring.

Proposition 1.3.1.2. *A set of generators of $\mathfrak{m}_\varnothing\mathbb{T}_k$ is determined by the generators of $\mathfrak{m}_\varnothing\mathbb{T}_{k'}$ for some $2\le k'\le p^2-1$.*

Proof. Note that the generators of $\mathfrak{m}_\varnothing$ depend only on $\overline{\rho}$. By the weight part of Serre's conjecture, there are only finitely many residual representations that come from eigenforms of $S_k(\Gamma,\chi,\mathbf{F})$ for all k. And they all appear when $k\le p^2-1$. Now for these eigenforms of weight $k\le p^2-1$, there exists a constant integer $C>0$ depending only on p such that the first C Fourier coefficients determine an eigenform. Thus given $\overline{\rho}$, we find $2\le k'\le p^2-1$ such that $\overline{\rho}$ comes from a form of weight k'. Then the first C Hecke operators together with the Fourier coefficients determine the generators of $\mathfrak{m}_\varnothing\mathbb{T}_k$. □

In general, the image of the maximal ideal $\mathfrak{m}_Q$ is generated by generators of $\mathfrak{m}_\varnothing \mathbb{T}_k$ and $U_q - \alpha_q$ for $q \in Q$. So there is a finite generating set of the image of the maximal ideal $\mathfrak{m}_Q$.

1.3.2 Generators and the Zariski tangent spaces

In the subsection, we assume k to be a positive integer that is congruent to k_0 unless otherwise noted. Since $\overline{r}$ is Schur and unobstructed, the deformation ring $R_{\overline{r}}^{\text{univ}}$ is formally smooth and it follows from the local Euler characteristic formula that $\dim_{\mathbf{F}} \operatorname{Tan}(R_{\overline{r}}^{\text{univ}}) = 3$. Thus $R_{\overline{r}}^{\text{univ}} \xrightarrow{\sim} \mathcal{O}[\![x_1, x_2, x_3]\!]$ is a formal power series ring in three variables.

Recall from §1.2.3 that the Hecke algebras $\mathbb{T}(k, Q)$ is a quotient of

$$R_{\overline{r}}^{k}[\![t_1, \ldots, t_h]\!] \xrightarrow{\sim} \mathcal{O}[\![x_1, x_2, x_3, t_1, \ldots, t_h]\!].$$

In order to minimize the number of generators of $\mathbb{T}(k, Q)$, we would like $h = 0$ in practice, which is equivalent to $R_{\overline{r}}^{\text{univ}} \twoheadrightarrow R_\varnothing$.

Proposition 1.3.2.1. *If $M(k_0, \varnothing) = \mathcal{O} f_0$, then $R_{\overline{r}}^{\text{univ}}$ surjects onto $R_\varnothing$. In this case, $\operatorname{Tan}(R_\varnothing)$ has dimension 2.*

Proof. Extending the coefficient ring $\mathcal{O}$ if necessary, we assume that $\mathcal{O} \supseteq \mathbf{Z}_p[a_n(f_0)]_{n \geq 0}$. By Nakayama's lemma, the ring homomorphism $R_{\overline{r}}^{\text{univ}} \to R_\varnothing$ is a surjection if and only if the ring homomorphism induces a surjection on the cotangent spaces of their special fibers, or equivalently, an injection on the tangent spaces $\operatorname{Tan}(R_\varnothing) \to \operatorname{Tan}(R_{\overline{r}}^{\text{univ}})$. Suppose for the sake of contradiction that v is a nontrivial tangent vector in $\ker(\operatorname{Tan}(R_\varnothing) \to \operatorname{Tan}(R_{\overline{r}}^{\text{univ}}))$. By Proposition 1.2.2.12, the vector $(v, 0) \in \operatorname{Tan}(R_\varnothing) \times_{\operatorname{Tan}(R_{\overline{r}}^{\text{univ}})} \operatorname{Tan}(R_{\overline{r}}^{k_0})$ defines a nontrivial tangent vector in $\operatorname{Tan}(R_\varnothing^{k_0})$ which is isomorphic to $\operatorname{Tan}(\mathbb{T}(\varnothing, k_0))$ by the $R = \mathbb{T}$ theorem as remarked in Remark 1.2.3.14. But since $M(k_0, \varnothing) = \mathcal{O} f_0$, the Hecke algebra $\mathbb{T}(k_0, \varnothing)$ is isomorphic to $\mathcal{O}$, which has a trivial tangent space, a contradiction.

For the second assertion, by Proposition 1.2.2.12, the tangent space of $R_\varnothing$ is the cohomology group $H^1(G_{\mathbf{Q},\{p,\infty\}}, \mathrm{ad}^0\overline{\rho})$. Since $\overline{\rho}$ is odd and absolutely irreducible, we deduce from the global Euler characteristic formula

$$\dim H^1(G_{\mathbf{Q},\{p,\infty\}}, \mathrm{ad}^0\overline{\rho}) = \dim H^2(G_{\mathbf{Q},\{p,\infty\}}) + 2 \geq 2.$$

On the other hand, as pointed out above, the vector space $\mathrm{Tan}(R_\varnothing)$ intersects with $\mathrm{Tan}(R_{\overline{r}}^{k_0})$ trivially in a three dimensional vector space $\mathrm{Tan}(R_{\overline{r}}^{\mathrm{univ}})$. Given that the tangent space $\mathrm{Tan}(R_{\overline{r}}^{k_0})$ is one-dimensional because $R_{\overline{r}}^{k_0}$ is isomorphic to $\mathcal{O}[\![x]\!]$ by Example 1.2.2.11, we have

$$\dim \mathrm{Tan}(R_\varnothing) \leq 2.$$

Combining the two inequalities, we obtain the desired statement.

□

Proposition 1.3.2.2. *If $h = \dim H^1_\Sigma(G_\mathbf{Q}, \mathrm{ad}^0\overline{\rho})$ is zero, i.e. if $R_{\overline{r}}^{\mathrm{univ}}$ surjects onto $R_\varnothing$, then $\#Q = 1$.*

Proof. Recall from §1.2.3 that the size of Q is equal to the dimension of the Selmer group $H^1(G_{\mathbf{Q},\{p,\infty\}}, \mathrm{ad}^0\overline{\rho}(1))$, which has dual Selmer group $H^1_\Sigma(G_\mathbf{Q}, \mathrm{ad}^0\overline{\rho})$ of dimension h. It follows from the Greenberg–Wiles formula from §1.2.2 that

$$\begin{aligned}\#Q - h &= \dim H^1(G_{\mathbf{Q},\{p,\infty\}}, \mathrm{ad}^0\overline{\rho}(1)) - \dim H^1_\Sigma(G_\mathbf{Q}, \mathrm{ad}^0\overline{\rho}) \\ &= \dim(\mathrm{ad}^0\overline{\rho}(1))^{G_\mathbf{Q}} - \dim(\mathrm{ad}^0\overline{\rho})^{G_\mathbf{Q}} + \dim H^1(G_{\mathbf{Q}_p}, \mathrm{ad}^0\overline{\rho}(1)) - \dim(\mathrm{ad}^0\overline{\rho}(1))^{G_{\mathbf{Q}_p}} \\ &\quad + \dim H^1(G_\mathbf{R}, \mathrm{ad}^0\overline{\rho}(1)) - \dim(\mathrm{ad}^0\overline{\rho}(1))^{G_\mathbf{R}}.\end{aligned}$$

Since $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_p)}}$ is Schur, we have $\dim(\mathrm{ad}^0\overline{\rho}(1))^{G_\mathbf{Q}} = \dim(\mathrm{ad}^0\overline{\rho})^{G_\mathbf{Q}} = 0$. The local Euler characteristics formula gives

$$\dim H^1(G_{\mathbf{Q}_p}, \mathrm{ad}^0\overline{\rho}(1)) - \dim(\mathrm{ad}^0\overline{\rho}(1))^{G_{\mathbf{Q}_p}} = \dim(\mathrm{ad}^0\overline{\rho})^{G_{\mathbf{Q}_p}} + 3 = 3,$$

where the second equality follows from the assumption that $\overline{r}$ is Schur. The term $H^1(G_{\mathbf{R}}, \mathrm{ad}^0\overline{\rho}(1))$ is trivial because the order of $G_{\mathbf{R}}$ is 2, which is coprime to $p > 2$. Since $\overline{\rho}$ is modular, it is an odd representation, meaning that the determinant of the complex conjugation is -1. Up to change of basis, the action of complex conjugation τ on $\mathrm{ad}^0\overline{\rho}(1)$ is given by

$$\tau\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The fixed points of τ are $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$ for $b, c \in \overline{\mathbf{F}}$, which form a two-dimensional vector space. Combining the computation above, we conclude

$$\#Q = h + 3 - 2 = 0 + 1 = 1.$$

□

Remark 1.3.2.3. In this case, Diagram 1.2.3.12 becomes

$$\begin{array}{ccccc} & & R^k_{\overline{r}} & \xrightarrow{\sim} & \mathbb{T}^k_\infty \\ & \nearrow & \downarrow & & \downarrow \\ \mathcal{O}[\![d]\!] & \longrightarrow & R^k_Q & \twoheadrightarrow & \mathbb{T}(k, Q) \end{array}.$$

For simplicity, we refer to the diamond operator as d though it is actually $1+d$. When $k = k_0$ is within the Fontaine–Laffaille range, by Example 1.2.2.11, the crystalline deformation ring $R^{k_0}_{\overline{r}}$ is isomorphic to a formal power series ring over $\mathcal{O}$ in one variable. Thus the dotted map is an isomorphism and the cotangent space of $R^k_{\overline{r}}$ is spanned by the image of d.

From now on we make the following assumption unless otherwise specified.

Assumption 1.3.2.4. Suppose that $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ is a modular Galois representation such that

1. the restriction $\overline{\rho}|_{G_{\mathbf{Q}_p}} = \overline{r}$ takes the form described in §1.2.2 and is Schur; and its universal deformation problem is unobstructed;

2. when $\overline{r}$ is the extension of 1 by the cyclotomic character, the extension class is peu ramifié;

3. the universal deformation problem of $\overline{r}$ is unobstructed;

4. the representation $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_p)}}$ is absolutely irreducible;

5. if $\ell \equiv -1 \mod p$ divides $N(\overline{\rho})$, then either $\overline{\rho}|_{G_{\mathbf{Q}_\ell}}$ is reducible over the algebraic closure or $\overline{\rho}|_{I_\ell}$ is absolutely irreducible.

6. the torsion of the level group Γ defined in §1.2.3 is a subset of $\{\pm I\}$;

7. $M(k_0, \varnothing) = \mathcal{O} f_0$ for some eigenform $f_0 \in S_k(\Gamma_1(N(\overline{\rho})), \chi, \mathcal{O})$.

When the assumption holds, the Hecke algebra $\mathbb{T}(k, Q)$ is generated by at most three elements over $\mathcal{O}$ as an $\mathcal{O}$-algebra because it is a quotient of $R_{\overline{r}}^{\mathrm{univ}} \xrightarrow{\sim} \mathcal{O}[\![x_1, x_2, x_3]\!]$ by Proposition 1.3.2.1. It follows that the set Q consists of only one Taylor–Wiles prime q by Proposition 1.3.2.2. The Hecke algebra $\widetilde{\mathbb{T}}(k, Q) = \mathbb{T}(k, Q)[T_p]$ is then generated by at most four elements as an $\mathcal{O}$-algebra.

Remark 1.3.2.5. By Assumption 1.3.2.4 (1) and the weight part of Serre's conjecture Edixhoven [1992], we have $M(1, \varnothing) = 0$.

Remark 1.3.2.6. We have $M(2, \varnothing) \otimes \mathbf{F} \xrightarrow{\sim} M(p + 1, \varnothing) \otimes \mathbf{F}$ by a theorem in Bao [2023a] under Assumption 1.3.2.4 and so there is no form of filtration $p+1$. In fact, this is even true without (7) in Assumption 1.3.2.4. By Lemma 1.2.4.3, we conclude that

$$\dim M(k, \varnothing) \otimes \mathbf{F} = e(R_{\overline{r}}^k \otimes \mathbf{F}) \cdot \dim M(k_0, \varnothing),$$

where $e(R^k_{\bar{r}} \otimes \mathbf{F})$ is the Hilbert–Samuel multiplicity of $R^k_{\bar{r}} \otimes \mathbf{F}$. If we also assume (7), then

$$\dim M(k, \varnothing) \otimes \mathbf{F} = e(R^k_{\bar{r}} \otimes \mathbf{F}).$$

Proposition 1.3.2.7. *Under Assumption 1.3.2.4 (6), for every integer $k \geq k_0$ that is congruent to k_0 modulo $p-1$ and every set of Taylor-Wiles primes Q, the surjection*

$$\widetilde{\mathbb{T}}(k, Q) \otimes \mathbf{F} \twoheadrightarrow \widetilde{\mathbb{T}}(k_0, Q) \otimes \mathbf{F}$$

constructed in Bao [2023a] induces a surjection

$$\mathbb{T}(k, Q) \otimes \mathbf{F} \twoheadrightarrow \mathbb{T}(k_0, Q) \otimes \mathbf{F}.$$

Proof. The assumption 1.3.2.4 (6) is used so that $\widetilde{\mathbb{T}}(k, Q)$ is the linear dual of the space of mod-p modular forms $M(k, Q) \otimes \mathbf{F}$, which is an essential step in the construction of the surjection $\widetilde{\mathbb{T}}(k, Q) \otimes \mathbf{F} \twoheadrightarrow \widetilde{\mathbb{T}}(k_0, Q) \otimes \mathbf{F}$. We have the composition of maps

$$\mathbb{T}(k, Q) \otimes \mathbf{F} \to \widetilde{\mathbb{T}}(k, Q) \otimes \mathbf{F} \twoheadrightarrow \widetilde{\mathbb{T}}(k_0, Q) \otimes \mathbf{F}$$

and the image of $\mathbb{T}(k, Q) \otimes \mathbf{F}$ in $\widetilde{\mathbb{T}}(k_0, Q) \otimes \mathbf{F}$ equals the image of $\mathbb{T}(k_0, Q) \otimes \mathbf{F}$ in $\widetilde{\mathbb{T}}(k_0, Q) \otimes \mathbf{F}$. Therefore, it suffices to show that

$$\mathbb{T}(k_0, Q) \otimes \mathbf{F} \to \widetilde{\mathbb{T}}(k_0, Q) \otimes \mathbf{F}$$

is a surjection. Taking the linear dual, by [Jochnowitz, 1982b, Lemma 6.5], this is equivalent to

$$M(k_0, Q) \otimes \mathbf{F} \to M(k_0, Q) \otimes \mathbf{F}/(\operatorname{Im} V)$$

being an injection, i.e., $\operatorname{Im} V = 0$, where V is the operator on the space of mod-p modular forms that sends $\sum_{n=1}^{\infty} a_n q^n$ to $\sum_{n=1}^{\infty} a_n q^{np}$. The mod-$p$ modular forms in $\operatorname{Im} V$ have filtration at least p by [Jochnowitz, 1982a, Fact 1.7]. When $2 \le k_0 \le p-1$, $\operatorname{Im} V$ is then automatically trivial. It remains to prove $\operatorname{Im} V = 0$ for $k_0 = p$. Suppose that there is some $g \in S_1(\Gamma_Q, \mathbf{F})$ such that $Vg \in M(p, Q) \otimes \mathbf{F}$. Since V is Hecke equivariant, g is an eigenform in the subspace $M(1, Q) \otimes \mathbf{F} \subseteq S_1(\Gamma_Q, \mathbf{F})$, which means that 1 is a Serre weight of $\overline{\rho}$. This is not possible by the weight part of Serre's conjecture [Edixhoven, 1992, Theorem 4.5] when $\overline{r}$ is Schur. □

Remark 1.3.2.8. When Assumption 1.3.2.4 holds and $Q \neq \varnothing$, the Hecke algebra $\mathbb{T}(k_0, Q)$ is a quotient of $\mathcal{O}[\![d]\!]$ that is not isomorphic to $\mathcal{O}$ and so $\operatorname{Cot}(\mathbb{T}(k_0, Q))$ is generated by d. Since the map in the proposition above sends the diamond operator d in $\mathbb{T}(k, Q) \otimes \mathbf{F}$ to that in $\mathbb{T}(k_0, Q) \otimes \mathbf{F}$, d spans a nontrivial one-dimensional subspace of $\operatorname{Cot}(\mathbb{T}(k, Q))$.

Proposition 1.3.2.9. *Under Assumption 1.3.2.4, the tangent spaces of the Hecke algebras satisfy*

$$\dim \operatorname{Tan}(\mathbb{T}(k, Q)) \ge \dim \operatorname{Tan}(\mathbb{T}(k, \varnothing)) + 1$$

for all $k \equiv k_0 \mod p-1$ *and sets of Taylor-Wiles primes* $Q \neq \varnothing$.

Proof. When $k = k_0$ is the initial weight, since $M(k_0, \varnothing) = \mathcal{O} f_0$, the Hecke algebra $\mathbb{T}(k_0, \varnothing)$ is isomorphic to $\mathcal{O}$. It follows that $\dim \operatorname{Tan}(\mathbb{T}(k_0, \varnothing)) = 0$. We have

$$\operatorname{rank}_{\mathcal{O}} \mathbb{T}(k_0, Q) = \operatorname{rank}_{\mathcal{O}} \widetilde{T}(k_0, Q) = \operatorname{rank}_{\mathcal{O}} M(k_0, Q) = \#\Delta_Q \operatorname{rank}_{\mathcal{O}} M(k_0, \varnothing) = \#\Delta_Q > 1.$$

Thus $\operatorname{Tan}(\mathbb{T}(k_0, Q))$ is at least one-dimensional and the statement holds for k_0. For k congruent to k_0 modulo $p-1$, by Proposition 1.3.2.7, we have

$$\operatorname{Tan}(\mathbb{T}(k_0, \varnothing)) \subseteq \operatorname{Tan}(\mathbb{T}(k, \varnothing)) \quad \text{and} \quad \operatorname{Tan}(\mathbb{T}(k_0, Q)) \subseteq \operatorname{Tan}(\mathbb{T}(k, Q)).$$

Since the Hecke algebras are the quotients of Galois deformation rings, the intersection

$\mathrm{Tan}(\mathbb{T}(k_0, Q)) \cap \mathrm{Tan}(\mathbb{T}(k, \varnothing))$ is contained in $\mathrm{Tan}(R_Q^{k_0}) \cap \mathrm{Tan}(R_\varnothing)$. We apply Proposition 1.2.2.12 to write the latter as

$$\begin{aligned}\mathrm{Tan}(R_Q^{k_0}) \cap \mathrm{Tan}(R_\varnothing) &= \left(\mathrm{Tan}(R_{\overline{r}}^{k_0}) \cap \mathrm{Tan}(R_Q)\right) \cap \mathrm{Tan}(R_\varnothing) = \mathrm{Tan}(R_{\overline{r}}^{k_0}) \cap \mathrm{Tan}(R_\varnothing) \\ &= \mathrm{Tan}(R_\varnothing^{k_0}) = \mathrm{Tan}(\mathbb{T}(k_0, \varnothing)) = 0,\end{aligned}$$

where the second line follows from Remark 1.3.2.3. Hence, $\mathrm{Tan}(\mathbb{T}(k_0, Q)) \cap \mathrm{Tan}(\mathbb{T}(k, \varnothing)) = 0$ and we have

$$\mathrm{coker}\ (\mathrm{Tan}(\mathbb{T}(k_0, \varnothing)) \hookrightarrow \mathrm{Tan}(\mathbb{T}(k_0, Q)) \hookrightarrow \mathrm{coker}\ (\mathrm{Tan}(\mathbb{T}(k, \varnothing)) \hookrightarrow \mathrm{Tan}(\mathbb{T}(k, Q))\,.$$

It then follows from the case of $k = k_0$ that

$$\dim \mathrm{Tan}(\mathbb{T}(k, Q)) - \dim \mathrm{Tan}(\mathbb{T}(k, \varnothing)) \geq \dim \mathrm{Tan}(\mathbb{T}(k_0, Q)) - \dim \mathrm{Tan}(\mathbb{T}(k_0, \varnothing)) \geq 1$$

and the proof is complete. □

Theorem 1.3.2.10 (Jochnowitz)**.** *If* $\widetilde{\mathbb{T}}(k, \varnothing) \otimes \mathbf{F}$ *is not an exceptional component, i.e. if* $k \not\equiv 2 \pmod{p-1}$, *then*

$$\dim \mathrm{Tan}(\mathbb{T}(k, \varnothing)) \geq 2$$

when $k \geq k_0 + 2p^2 + p - 3$ *and*

$$\dim \mathrm{Tan}(\widetilde{\mathbb{T}}(k, \varnothing)) \geq 3$$

when $k \geq k_0 p^2$.

Proof. For the original proof in the case $N(\overline{\rho}) = 1$, see [Jochnowitz, 1982b, Theorem 8.1, Theorem 8.1'] where the filtration $w(f)$ automatically could not be $1, 2$ or 3. By Remark 1.3.2.5, we still do not have any mod-p modular form f such that $w(f) = 1$. Jochnowitz's proof still works for general level $N(\overline{\rho})$ that is coprime to p when $w(f) \neq 2$. Jochnowitz did not include the lower bounds for k in her original statement, so we follow her proof and make these explicit here. When $k \geq k_0 + p^2 - 1$, we have $\theta^{p-1} f_0 \in M(k, \varnothing) \otimes \mathbf{F}$, where $\mathbf{F} f_0 = M(k_0, \varnothing) \otimes \mathbf{F}$.

If $a_p(f_0) = 0 \in \mathbf{F}$, Jochnowitz constructed modular forms $g, h \in \ker U_p \cap M(2(p^2-1) + k_0, \varnothing) \otimes \mathbf{F}$ where

$$k_0 + 2p^2 + p - 3 = \max\{(k_0+1)p + 1 + (p-2)(p+1), (p+4-k_0)p + 1 + (p-1+k_0-3)(p+1)\}$$

It follows from [Jochnowitz, 1982b, Lemma] that the image C_k of $\mathbb{T}(k, \varnothing) \otimes \mathbf{F}$ in $\widetilde{\mathbb{T}}(k, \varnothing) \otimes \mathbf{F}$ has tangent space of dimension at least two. In fact, the algebra $C_k/(\ker U_p)^{\perp}$ has tangent space of dimension two from the proof of [Jochnowitz, 1982b, Lemma 8.2]. (We have $\ker U_p \cap \operatorname{Im} V = 0$ thus $\ker U_p \hookrightarrow \overline{S_k}$ with her notation.) When $k \geq k_0 + 2(p^2-1) \geq p^2$, we have $V f_0 \in M(k, \varnothing) \otimes \mathbf{F}$. Let T be an operator in C_k. Then

$$(T - \lambda(T)) V f_0 = 0 \quad \text{and} \quad U_p^2 V f_0 = U_p f_0 = 0.$$

Denote by $\mathfrak{m}$ the maximal ideal of $\widetilde{\mathbb{T}}(k, \varnothing) \otimes \mathbf{F}$. If there exist $c_i \in \mathbf{F}$ such that

$$c_0 U_p + \sum_{i=1}^{n} c_i (T_i - \lambda(T_i)) \in \mathfrak{m}^2,$$

then

$$c_0 f_0 = \left(c_0 U_p + \sum_{i=1}^{n} c_i (T_i - \lambda(T_i)) \right) V f_0 \in \mathfrak{m}^2 f_0 = 0.$$

Hence, we have $c_0 = 0$ and

$$\sum_{i=1}^{n} c_i (T_i - \lambda(T_i)) \in \mathfrak{m}^2.$$

Now restrict this to $\ker U_p$ and combine with the result that $C_k/(\ker U_p)^{\perp}$ has tangent space of dimension two, the proof is complete when $a_p(f_0) = 0$.

If $a_p(f_0) \in \mathbf{F}^\times$, the first assertion holds when k is at least

$$k_0+2(p^2-1) = \max\{(k_0+1)p+1+(p-2)(p+1), (p+2-k_0)p+1+(p-1+k_0-2)(p+1)\}$$

The rest of the argument works the same except that we replace Vf_0 by $Vf_0 - a_p(f_0)V^2f_0 \in \ker U_p^2$ which has filtration $p^2k_0 \leq p^3$.

Since $k_0+2p^2+p-3 \geq k_0+2(p^2-1)$ and $k_0p^2 \geq k_0p$, we obtain the lower bounds for k as in the statement. □

Proposition 1.3.2.11. *If* $k \equiv 2 \pmod{p-1}$, *under Assumption 1.3.2.4, the conclusion above holds true for* $\mathbb{T}(k,\varnothing)$ *when* $k \geq p^2+2p-1$ *and for* $\widetilde{\mathbb{T}}(k,\varnothing)$ *when* $k \geq 2p^2$.

Proof. In this proof, by abuse of notation, when we say a Hecke operator, we mean its image in $\mathrm{End}_{\mathbf{F}}(M(k,\varnothing)\otimes\mathbf{F})$ for some weight k. The T_p operator in $\widetilde{\mathbb{T}}(k,\varnothing)$ acts as U_p in characteristic p. As pointed out in Remark 1.3.2.6, there are no forms of filtration $p+1$; thus it suffices to prove the statement when f_0 has filtration 2. We first analyze the filtration given by multiplication by the Hasse invariant on the space $M(p^2+2p-1,\varnothing)\otimes\mathbf{F}$ and $M(2p^2,\varnothing)\otimes\mathbf{F}$. We have

$$\mathbf{F}f_0 = M(2,\varnothing)\otimes\mathbf{F} \xrightarrow{\sim} M(p+1,\varnothing)\otimes\mathbf{F}.$$

By Proposition 1.2.4.5 and Remark 1.3.2.6, it follows that

$$\dim M(2p,\varnothing)\otimes\mathbf{F} = \dim M(3p-1,\varnothing)\otimes\mathbf{F} = \ldots = \dim M(p^2-p+2)\otimes\mathbf{F} = 2$$

and

$$\dim M(p^2+1,\varnothing)\otimes\mathbf{F} = \dim M(p^2+p,\varnothing)\otimes\mathbf{F} = 3.$$

The space $M(2p,\varnothing)\otimes\mathbf{F}$ is spanned by f_0 and Vf_0 because $w(Vf_0) = pw(f_0) = 2p$; and there is some g of filtration p^2+1 such that $U_p g = Vf_0$. Indeed, since

$$w(U_p g) = \frac{w(g)-1}{p} + p = 2p$$

by [Jochnowitz, 1982b, Lemma 1.9], there exists $a \in \mathbf{F}$ and $b \in \mathbf{F}^\times$ such that $U_p g = af_0 + bVf_0$. Now

$$U_p((g - aVf_0)/b) = a/b \cdot f_0 + Vf_0 - a/b \cdot U_p V f_0 = a/b \cdot f_0 + Vf_0 - a/b \cdot f_0 = Vf_0$$

and we may replace g by $(g - af_0)/b$. It follows from Proposition 1.3.4.8 that

$$\dim M(p^2+2p-1, \varnothing) \otimes \mathbf{F} = \dim M(p^2+3p-2, \varnothing) \otimes \mathbf{F} = \ldots = \dim M(2p^2-p+1\varnothing) \otimes \mathbf{F} = 4$$

and

$$\dim M(2p^2, \varnothing) \otimes \mathbf{F} = 5.$$

Hence, there exists a modular form h of filtration p^2+2p-1 and $\{f_0, Vf_0, g, h\}$ is a basis of $M(p^2+2p-1, \varnothing) \otimes \mathbf{F}$. It follows that $\{f_0, Vf_0, g, h, V^2 f_0\}$ is a basis of $M(2p^2, \varnothing) \otimes \mathbf{F}$. Note that

$$w(U_p h) < \frac{w(h)-1}{p} + p = 2p + 2 - \frac{2}{p} < p^2 + 1.$$

Thus

$$U_p h = a_1 f_0 + a_2 V f_0$$

for some $a_1, a_2 \in \mathbf{F}$. Denote by $\lambda(T)$ the eigenvalue of $T \in \mathbb{T}(2p^2, \varnothing) \otimes \mathbf{F}$ on $M(2p^2, \varnothing) \otimes \mathbf{F}$.

With respect to this basis, the operator U_p and T have matrices

$$U_p = \begin{pmatrix} a_p(f_0) & 1 & 0 & a_1 & 0 \\ 0 & 0 & 1 & a_2 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} \lambda(T) & 0 & b_1(T) & b_3(T) & 0 \\ 0 & \lambda(T) & b_2(T) & b_4(T) & 0 \\ 0 & 0 & \lambda(T) & b_5(T) & 0 \\ 0 & 0 & 0 & \lambda(T) & 0 \\ 0 & 0 & 0 & 0 & \lambda(T) \end{pmatrix}$$

for some $b_i(T) \in \mathbf{F}$ for $i = 1, 2, \ldots, 5$. Since U_p and T commute, we conclude that

$$b_2(T) = -a_p(f_0)b_1(T), \quad b_4(T) = -a_p(f_0)b_3(T) \quad \text{and} \quad b_5(T) = 0.$$

If $a_p(f_0) = 0 \in \mathbf{F}$, then $\widetilde{\mathbb{T}}(2p^2, \varnothing) \otimes \mathbf{F}$ is the matrix subalgebra generated by the matrices for U_p and T as above. Note that $\operatorname{Im} V \cap M(p^2 + 2p - 1, \varnothing) \otimes \mathbf{F} = \mathbf{F}Vf_0$. In $M(p^2 + 2p - 1, \varnothing) \otimes \mathbf{F}$, we obviously have $h \notin \mathbb{T}(p^2 + 2p - 1, \varnothing)g + \mathbf{F}Vf_0$ for filtration reason. Conversely, if there is $T \in \mathbb{T}(p^2 + 2p - 1, \varnothing)$ such that

$$g = Th + aVf_0 = \lambda(T)h + b_3(T)f_0 + aVf_0$$

for some $a \in \mathbf{F}$, then the filtration of the right hand side is either $p^2 + 2p - 1$ or $2p$ or 2 while the filtration of the left hand side is $p^2 + 1$, a contradiction. By [Jochnowitz, 1982b, Lemma 8.2], the image of $\mathbb{T}(p^2 + 2p - 1, \varnothing)$ in $\widetilde{\mathbb{T}}(p^2 + 2p - 1, \varnothing) \otimes \mathbf{F}$ has tangent space of dimension at least two. For $k = 2p^2$, we then let T_1 and T_2 be the two Hecke operators in $\mathbb{T}(2p^2, \varnothing)$ such that they span a two dimensional vector space in the cotangent space of $\operatorname{Im}(\mathbb{T}(2p^2, \varnothing) \to \widetilde{\mathbb{T}}(2p^2, \varnothing) \otimes \mathbf{F})$. In particular, the matrices of $T_1 - \lambda(T_1)$ and $T_2 - \lambda(T_2)$ acting on $M(2p^2, \varnothing)$ are linearly independent. We now show $T_1 - \lambda(T_1), T_2 - \lambda(T_2)$ and U_p span a three dimensional vector space in the cotangent space of $\widetilde{\mathbb{T}}(2p^2, \varnothing) \otimes \mathbf{F}$. Indeed, from the matrices of these operators as above, we directly calculate that

$$U_p^3 = U_p(T - \lambda(T)) = (T - \lambda(T))^2 = (T - \lambda(T))(T' - \lambda(T')) = 0$$

for all $T, T' \in \mathbb{T}(2p^2, \varnothing)$, which implies that the square of maximal ideal of $\widetilde{\mathbb{T}}(2p^2, \varnothing)$ is just $\mathbf{F}U_p^2$. If there are $c_1, c_2, c_3 \in \mathbf{F}$ such that

$$c_1(T_1 - \lambda(T_1)) + c_2(T_2 - \lambda(T_2)) + c_3 U_p \in \mathbf{F}U_p^2,$$

then

$$c_3 V f_0 = c_1 V^2(T_1 - \lambda(T_1))f_0 + c_2 V^2(T_2 - \lambda(T_2))f_0 + c_3 V f_0 \in \mathbf{F}U_p^2 V^2 f_0 = \mathbf{F} f_0$$

because f_0 is an eigenform in characteristic p. Compare the filtration on both sides and we have $c_3 = 0$. Hence,

$$c_1(T_1 - \lambda(T_1)) + c_2(T_2 - \lambda(T_2)) = aU_p^2$$

for some $a \in \mathbf{F}$. Again by using the matrices of T_1, T_2 and U_p, we see that $a = 0$ and $c_1 = c_2 = 0$ because of the linear independence assumption.

If $a_p(f_0) \in \mathbf{F}^\times$, then $\widetilde{\mathbb{T}}(2p^2, \varnothing) \otimes \mathbf{F}$ is the matrix subalgebra generated by the lower diagonal block matrices for U_p and T:

$$U_p = \begin{pmatrix} 0 & 1 & a_2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} \lambda(T) & -a_p(f_0)b_1(T) & -a_p(f_0)b_3(T) & 0 \\ 0 & \lambda(T) & 0 & 0 \\ 0 & 0 & \lambda(T) & 0 \\ 0 & 0 & 0 & \lambda(T) \end{pmatrix}.$$

The rest of the proof works the same as in the case $a_p(f_0) = 0 \in \mathbf{F}$ except that in $\widetilde{\mathbb{T}}(2p^2, \varnothing) \otimes$

$\mathbf{F}$, we check that

$$U_p^2 = U_p(T - \lambda(T)) = (T - \lambda(T))^2 = (T - \lambda(T))(T' - \lambda(T')) = 0$$

for all $T, T' \in \mathbb{T}(2p^2, \varnothing)$, which implies that the square of maximal ideal of $\widetilde{\mathbb{T}}(2p^2, \varnothing)$ is 0. If there are $c_1, c_2, c_3 \in \mathbf{F}$ such that

$$c_1(T_1 - \lambda(T_1)) + c_2(T_2 - \lambda(T_2)) + c_3 U_p = 0,$$

then $c_3 = 0$ by comparing the entries on both sides. Then $T_1 - \lambda(T_1)$ and $T_2 - \lambda(T_2)$ are linearly dependent, which contradicts our assumption on T_1 and T_2. □

Corollary 1.3.2.12. *Under Assumption 1.3.2.4, we have*

$$\dim \mathrm{Tan}(\mathbb{T}(k, \varnothing)) = 2$$

when $k \geq 2p^2 + p + k_0 - 3$ *and*

$$\dim \mathrm{Tan}(\widetilde{\mathbb{T}}(k, \varnothing)) = 3$$

when $k \geq k_0 p^2$.

Proof. By Jochnowitz's theorem and the proposition above, it suffices to give upper bounds of the dimensions. Since $R_\varnothing \twoheadrightarrow \mathbb{T}(k, \varnothing)$, we have $\dim \mathrm{Tan}(\mathbb{T}(k, \varnothing)) \leq \dim \mathrm{Tan}(R_\varnothing) = 2$ by Proposition 1.3.2.1. For the full Hecke algebra $\widetilde{\mathbb{T}}(k, \varnothing) = \mathbb{T}(k, \varnothing)[T_p]$, it follows that $\dim \mathrm{Tan}(\widetilde{\mathbb{T}}(k, \varnothing)) \leq \dim \mathrm{Tan}(\mathbb{T}(k, \varnothing)) + 1 \leq 2 + 1 = 3$. □

Now we outline the algorithm for determining the generators of $\mathbb{T}(k, Q)$ under assumption 1.3.2.4. By the Sturm bound [Stein, 2007, Theorem 9.23], the Hecke algebra $\widetilde{\mathbb{T}}(k, \varnothing)$ is generated by T_n for $n \leq r$ where $r = \frac{km}{12} - \frac{m-1}{N(\overline{\rho})}$ and $m := [\mathrm{SL}_2(\mathbf{Z}) : \Gamma]$. It then follows from the corollary above that for some $k_1 \geq k_0 p^2$ there are $T_{\ell_1}, T_{\ell_2}, T_{\ell_3}$ for some primes $\ell_1, \ell_2, \ell_3 \leq r$ such that they form a minimal set of generators of the Hecke algebra $\widetilde{\mathbb{T}}(k_1, Q)$. If none of the three primes equal p, then $\mathbb{T}(k_1, \varnothing) = \widetilde{\mathbb{T}}(k_1, \varnothing)$, which is a contradiction because the dimensions of the tangent spaces are not the same. We assume that $\ell_3 = p$.

Proposition 1.3.2.13. *Under assumption 1.3.2.4, the Hecke algebra* $\mathbb{T}(k_1, \varnothing)$ *is generated by* T_{ℓ_1} *and* T_{ℓ_2}.

Proof. Let $\mathbb{T}'$ be the subalgebra of $\widetilde{\mathbb{T}}(k_1, \varnothing)$ generated by T_{ℓ_1} and T_{ℓ_2} over $\mathcal{O}$. Since $\{T_{\ell_1}, T_{\ell_2}\}$ is a minimal set of generators for $\mathbb{T}'$, the commutative diagram

$$\begin{array}{ccc} \mathbb{T}(k_1, \varnothing) & \longrightarrow & \widetilde{\mathbb{T}}(k_1, \varnothing) \\ \uparrow & \nearrow & \\ \mathbb{T}' & & \end{array}$$

induces a commutative diagram on the cotangent spaces

$$\begin{array}{ccc} \mathrm{Cot}(\mathbb{T}(k_1, \varnothing)) & \longrightarrow & \mathbf{F}T_{\ell_1} \oplus \mathbf{F}T_{\ell_2} \oplus \mathbf{F}T_p \\ \uparrow & \nearrow & \\ \mathbf{F}T_{\ell_1} \oplus \mathbf{F}T_{\ell_2} & & \end{array} .$$

It is immediate that the vertical map is an injection as well. But by the corollary above, we have $\dim \mathrm{Cot}(\mathbb{T}(k_1, \varnothing) \otimes \mathbf{F}) = \dim \mathrm{Tan}(\mathbb{T}(k_1, \varnothing)) = 2$. The vertical map is then also a surjection. It follows from Nakayama's lemma that the inclusion $\mathbb{T}' \subseteq \mathbb{T}(k_1, \varnothing)$ is actually a surjection. $\square$

Proposition 1.3.2.14. *Under assumption 1.3.2.4, the Hecke algebra* $\mathbb{T}(k, \varnothing)$ *is generated by* T_{ℓ_1} *and* T_{ℓ_2} *for all weights* $k \equiv k_0 \mod p-1$.

Proof. If ℓ_i does not divide $N(\overline{\rho})$, then $T_{\ell_i} = \mathrm{tr}\,(\rho_{\varnothing}^{k,\mathrm{mod}}(\mathrm{Frob}_{\ell_i}))$. If ℓ_i divides $N(\overline{\rho})$, then there are three cases from the proof of a lemma in Bao [2023a] . The only case where $T_{\ell_i} = U_{\ell_i}$ is not a scalar is when the conductor at ℓ_i is one and the ℓ_i-component χ_{ℓ_i} of the

Nebentypus character is ramified at ℓ_i. In this case, we have made the choice of σ_1 and σ_2 which is independent of k. Thus we have the set of linear equations in T_{ℓ_i} and $T_{\ell_i}^{-1}$

$$\begin{cases} \operatorname{tr}(\rho_{\varnothing}^{k,\mathrm{mod}}(\sigma_1)) = T_{\ell_i} + \frac{\chi_\ell(\sigma_1)\ell^{k-1}}{T_{\ell_i}} \\ \operatorname{tr}(\rho_{\varnothing}^{k,\mathrm{mod}}(\sigma_2)) = T_{\ell_i} + \frac{\chi_\ell(\sigma_2)\ell^{k-1}}{T_{\ell_i}} \end{cases}.$$

Recall the construction of $R_\varnothing \twoheadrightarrow R_\varnothing^{k_1} \twoheadrightarrow \mathbb{T}(k_1, \varnothing)$ from §1.2.3. Then $\operatorname{tr}(\rho_\varnothing(\mathrm{Frob}_{\ell_i}))$'s when $\ell_i \nmid N(\overline{\rho})$ and $\operatorname{tr}(\rho_\varnothing(\sigma_1))$ and $\operatorname{tr}(\rho_\varnothing(\sigma_2))$ when $\ell_i | N(\overline{\rho})$ span a subspace in $\mathrm{Cot}(R_\varnothing)$ of dimension at least $\dim \mathrm{Cot}(\mathbb{T}(k_1, \varnothing)) = 2$. Since $\dim \mathrm{Cot}(R_\varnothing) = 2$, these elements generate $R_\varnothing$. When $k \neq k_1$, the image of these trace elements under the map $R_\varnothing \twoheadrightarrow \mathbb{T}(k, \varnothing)$ are still the linear combinations of the corresponding Hecke operators. Thus T_{ℓ_1} and T_{ℓ_2} generate $\mathbb{T}(k, \varnothing)$ for all k that are congruent to k_0 modulo $p - 1$. □

Lemma 1.3.2.15. *Let* $r = \frac{k_1 m}{12} - \frac{m-1}{N(\overline{\rho})}$ *and* $m := [\mathrm{SL}_2(\mathbf{Z}) : \Gamma]$. *Under assumption 1.3.2.4, for every* $k \equiv k_0 \mod p - 1$ *and every set* Q *of Taylor–Wiles primes, the Hecke algebra* $\mathbb{T}(k, Q)$ *is generated by* T_{ℓ_1}, T_{ℓ_2} *and the diamond operator* d *for some primes* $\ell_1, \ell_2 \leq r$.

Proof. By Proposition 1.3.2.9, the dimension of $\mathrm{Tan}(\mathbb{T}(k_1, Q))$ is at least 3. But since $R_{\overline{r}}^{\mathrm{univ}} \twoheadrightarrow R_Q \twoheadrightarrow \mathbb{T}(k_1, Q)$, the dimension of $\mathrm{Tan}(\mathbb{T}(k_1, Q))$ is at most 3. So $\dim \mathrm{Cot}(\mathbb{T}(k_1, Q)) = \dim \mathrm{Tan}(\mathbb{T}(k_1, Q)) = 3$. The kernel of $\mathrm{Cot}(\mathbb{T}(k_1, Q)) \to \mathrm{Cot}(\mathbb{T}(k_1, \varnothing))$ is then one dimensional and is spanned by the diamond operator d. To see this, note that d is in the kernel and it spans a nontrivial direction in the cotangent space as explained in Remark 1.3.2.8. The statement now follows from Proposition 1.3.2.14. □

Using this lemma, the generators of $\mathbb{T}(k, Q)$ is the Hecke operators $\{T_{\ell_1}, T_{\ell_2}, d, U_q\}_{q \in Q}$ where ℓ_1 and ℓ_2 are determined by the generators of the Hecke algebra $\mathbb{T}(k_1, \varnothing)$ by using the Sturm bound r for some $k_1 \geq k_0 p^2$.

Remark 1.3.2.16. In fact, any k_1 such that $\dim \mathrm{Tan}\widetilde{\mathbb{T}}(k_1, \varnothing) = 3$ works. But having the bound k_0p^2 improves the stability of implementation of the algorithm. Note that any computation at the initial level is relatively light. So this is practical.

We can apply the patching functor discussed in §1.2.3 to the Hecke algebras and obtain the following.

Corollary 1.3.2.17. *Under assumption (1.3.2.4), we have the following.*

1. *For every integer $k \geq 2$ that is congruent to k_0 modulo $p-1$, there is a surjection*

$$R_{\bar{r}}^{k} \twoheadrightarrow R_{\bar{r}}^{k_0}.$$

2. *We have*

$$\lim_{\substack{n\to\infty \\ k=k_0+n(p-1)}} \dim \mathrm{Tan}(R_{\bar{r}}^{k}) = \dim \mathrm{Tan}(R_{\bar{r}}^{\mathrm{univ}}) = 3$$

and the limit is achieved when $k \geq k_0 + 2p^2 + p - 3$.

3. *We have*

$$\lim_{\substack{n\to\infty \\ k=k_0+n(p-1)}} \dim \mathrm{Tan}((R_{\bar{r}}^{k}[\alpha_p])_{(\lambda,\alpha_p)}) = 4.$$

Proof. Assertion (1) follows from Proposition 1.3.2.9 and Theorem 1.2.3.1. Assertion (2) follows from Proposition 1.3.2.9, Corollary 1.3.2.12 and Theorem 1.2.3.1. To see (3), it suffices to show that $\dim \mathrm{Tan}(\widetilde{\mathbb{T}}(k,Q)) = 4$ and then we apply Theorem 1.2.3.16. Since we have proved that $\dim \mathrm{Tan}(\mathbb{T}(k,Q)) = 3$ when k is large enough, we only need to establish $\dim \mathrm{Tan}(\widetilde{\mathbb{T}}(k,Q)) = \dim \mathrm{Tan}(\mathbb{T}(k,Q)) + 1$, which is proved in [Jochnowitz, 1982b, Reduction to Theorem 8.1']. □

Remark 1.3.2.18. We actually expect the limit in (2) to be achieved when $k \geq k_0 + p^2 - 1$ as predicted by Corollary 1.5.0.1, which will be discussed in more details in §1.5. But this result guarantees that the algorithm can determine the generators of the Hecke algebras within finitely many steps.

1.3.3 Relations

In this subsection, we describe an algorithm to compute the presentation of the Hecke algebra $\mathbb{T}(k, Q)$ (resp. $\widetilde{\mathbb{T}}(k, Q)$) modulo arbitrary power of λ when Q is nonempty. The input is assumed to be a finite set $\mathcal{T}$ of generators of $\mathfrak{m}_{\varnothing}\mathbb{T}_k$ (determined in §1.3.1) and generators of $\mathbb{T}(k, Q)$ (resp. $\widetilde{\mathbb{T}}(k, Q)$). For example, when Assumption 1.3.2.4 is satisfied, the set of generators of $\mathbb{T}(k, Q)$ is $\{\delta, T_{\ell_1}, T_{\ell_2}, U_q\}$ (resp. $\{\delta, T_{\ell_1}, T_{\ell_2}, U_q, T_p\}$) where ℓ_1 and ℓ_2 are prime numbers determined in the previous subsection. Note that the set $\mathcal{T}$ is independent of k or Q.

The algorithm involves three main steps. We first compute how the Hecke operators in $\mathcal{T}$ act on cohomology group $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$. Then we restrict the action to the $\mathcal{O}$-module $M'(k, Q)$ that consists of integral cohomology classes localized at the global residual Galois representation $\overline{\rho}$. At last, we compute the relations of the finite $\mathbf{F}$-algebra $\mathbb{T}(k, Q)/\lambda$ (resp. $\widetilde{\mathbb{T}}(k, Q)/\lambda$) from computing the relations among the matrices previously computed. We will use some basic propositions and lemmas on linear algebra over $\mathcal{O}$. We claim no originality of the proofs but we include them for the sake of completeness.

Step 1: Hecke action on $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$

The action of Hecke operators on $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ can be computed by formula (1.2.1.6). But as we point out in Remark 1.2.1.9, the $\mathcal{O}$-module $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ can have non-trivial torsion even though $\Gamma_Q \subseteq \Gamma_1(N_Q)$ is torsion free because $N_Q \geq 7$. Thus we cannot simply pick a basis of $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ and compute the corresponding matrices of the Hecke operators.

Instead, we work with cochains and coboundaries. Since Γ_Q is torsion free, the $\mathcal{O}$-module of cochains $Z^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ is free and has a basis indexed by a set of free generators of Γ_Q by the proof of Proposition 1.2.1.5. Both MAGMA Bosma et al. [1997] and SageMath The Sage Developers [2023] can compute a set of free generators of $\mathrm{P}\Gamma_Q \xrightarrow{\sim} \Gamma_Q$. Thus we can compute the matrices of the Hecke operators with respect to the aforementioned basis of $Z^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$. On the other hand, the $\mathcal{O}$-module of coboundaries $B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ is either trivial when $k = 2$ or a finite free $\mathcal{O}$-module when $k \geq 3$ by the proof of Proposition 1.2.1.8. We record $B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ as a submodule of $Z^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$. This way, we keep track of the Hecke action on

$$H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2) = \frac{Z^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)}{B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)}$$

using matrices with coefficients in $\mathcal{O}$.

Step 2: Localization

We then need to compute the $\mathcal{O}$-submodule $M'(k, Q)$ of $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ and restrict the Hecke action to $M'(k, Q)$.

Definition 1.3.3.1. Suppose that M is a finitely generated $\mathcal{O}$-module and let T be an $\mathcal{O}$-linear endomorphism of M. We say that T acts topologically nilpotently on an $\mathcal{O}[T]$-submodule M_1 if for every integer $m > 0$, there exists an integer $N_m > 0$ such that for all $n \geq N_m$, we have

$$T^n M_1 \subseteq M_1 \cap \lambda^m M.$$

Remark 1.3.3.2. By Artin–Rees lemma, we can replace the subspace topology with the λ-adic topology of M_1 in the definition above.

Since M is a Noetherian $\mathcal{O}$-module, there exists a maximal $\mathcal{O}[T]$-submodule M_T of M such that the T action on M_T is topologically nilpotent. Recall that the module $M'(k, Q)$ is exactly the intersection of all the maximal $\mathcal{O}[T]$-submodule of $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ on which the T action is topologically nilpotent as T runs through all the Hecke operators in $\mathfrak{m}_Q\mathbb{T}(k)$. Therefore, in the process of computing $M'(k, Q)$, we will repeatedly compute the maximal sub-module M_T where the T-action is topologically nilpotent for some suitable modules M

as T runs through the finite set $\mathcal{T}$ of certain Hecke operators. In the rest of the subsection, we will first explain how to find the submodule M_T for a general finite free $\mathcal{O}$-module M and an $\mathcal{O}$-endomorphism T of M. Then we will outline how to adapt the method to the case of computing $M'(k, Q)$ because $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ is not always a free $\mathcal{O}$-module as we point out in the previous step.

Lemma 1.3.3.3. *Suppose that M is a finite free $\mathcal{O}$-module and T is an endomorphism of M. Let $\mu_1, \ldots, \mu_m \in \overline{\mathbf{F}}_p$ denote the nonzero eigenvalues of the operator T when it acts on the reduction $M \otimes \mathbf{F}$ and let γ be some integer such that $\mu_i^\gamma = 1$ for all i. Then the limit*

$$E := \lim_{i \to \infty} (T^\gamma)^{p^i}$$

exists and it acts as an idempotent on M. The submodule M_T is the image of $(1 - E)$ on M.

Proof. Denote T^γ by A. It is immediate that A has eigenvalues 0 and 1 when it acts on $M \otimes \mathbf{F}$. By considering its Jordan canonical form in characteristic p, we conclude that A^{p^i} is semisimple and therefore is an idempotent when it acts on $M \otimes \mathbf{F}$. Without loss of generality, we may and do assume A itself is an idempotent in characteristic p. It follows that

$$A^p - A = O(\lambda)$$

in characteristic 0. Suppose that $A^{p^i} - A^{p^{i-1}} = O(\lambda^i)$. Then

$$A^{p^{i+1}} - A^{p^i} = \left(A^{p^i}\right)^p - \left(A^{p^{i-1}}\right)^p = \left(A^{p^{i-1}} + O(\lambda^i)\right)^p - \left(A^{p^{i-1}}\right)^p = pO(\lambda^i) = O(\lambda^{i+1}).$$

By induction on i, we see that $\{A^{p^i}\}$ forms a Cauchy sequence and thus it converges to some limit that defines an $\mathcal{O}[T]$-linear operator $E : M \to M$. To check E that E is an idempotent, we suppose that

$$(A^{p^i})^2 = A^{p^i} + O(\lambda^i).$$

Then

$$\left(A^{p^{i+1}}\right)^2 - A^{p^{i+1}} = \left(A^{2p^i}\right)^p - \left(A^{p^i}\right)^p = \left(A^{p^i} + O(\lambda^i)\right)^p - \left(A^{p^i}\right)^p = pO(\lambda^i) = O(\lambda^{i+1}).$$

Again by induction on i, we conclude that $E^2 = E$.

At last, we need to verify that $(1 - E)M = M_T$. The decomposition

$$M = EM \oplus (1 - E)M$$

respects the T-action because E and T commute. The operator T is invertible when it restricts to EM because in characteristic p,

$$TEM = TAM$$

and A is the idempotent that singles out the generalized eigenspaces for all the nonzero eigenvalues $\mu_1, \ldots, mu_m$ of T in characteristic p. Suppose for the sake of contradiction that $v \in M_T \setminus (1 - E)M$. Then we write $v = v_1 + v_2$ for some $v_1 \in EM$ and $v_2 \in (1 - E)M$. Now $v_1 = v - v_2$ is also in M_T. But the intersection of M_T and EM is trivial. Thus $M_T = (1 - E)M$. $\square$

We now describe how to compute $M'(k, Q)$. We first take M to be the finite free $\mathcal{O}$-module $Z^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ and we let the operator be $U_q - \alpha_q$ for some Taylor–Wiles prime $q \in Q$. By the lemma above, we can find the maximal submodule $M_{U_q - \alpha_q}$. Now we consider the $\mathcal{O}[U_q - \alpha_q]$-module

$$W := B^1(G, \mathrm{Sym}^{k-2}\mathcal{O}^2) + M_{U_q - \alpha_q}.$$

Though Hecke operators do not commute when they act on the space of cochains, we still have the following.

Proposition 1.3.3.4. *Every operator $T' \in \mathcal{T}$ preserves W.*

Proof. Since $U_q - 1$ acts topologically nilpotently on $B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ by Proposition 1.2.1.8 and α_q is not congruent to 1 modulo λ by our choice, the module $M_{U_q-\alpha_q}$ intersects $B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ trivially. Thus

$$W/B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2) \xrightarrow{\sim} M_{U_q-\alpha_q}$$

is the maximal submodule of $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ on which $U_q - \alpha_q$ acts topologically nilpotently. For every operator $T \in \mathcal{T}$, the operator $U_q - \alpha_q$ acts on $T(W/B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2))$ topologically nilpotently because U_q and T commute when they act on the group cohomology $H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$. Thus

$$T(W/B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)) \subseteq W/B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$$

and therefore $TW \subseteq W$. $\square$

Thus we are able to compute the matrices representing the action of each $T \in \mathcal{T}$ when restricted to the free module W and thus on $W/B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$, which is isomorphic to another finite free module $M_{U_q-\alpha_q}$. We now set $M = W/B^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ and choose a Hecke operator $T \in \mathcal{T}$ other than $U_q - \alpha_q$. Again by Lemma 1.3.3.3, we find $M_{T-a} \subseteq H^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ for some $a \in \mathcal{O}$ such that $T - a \in \mathfrak{m}_Q$ and we restrict the Hecke action to M_{T-a}. Given that $\mathcal{T}$ is a finite set, this iterative process concludes after a limited number of steps. The resulting finite free $\mathcal{O}$-module is $M'(k, Q)$ that we desire and we also obtain the finite set $\mathcal{S}$ of matrices of Hecke operators in $\mathcal{T}$ when they act on $M'(k, Q)$.

Step 3: Presentation of the Hecke algebras

We outline the algorithm to compute the presentation of the finite $\mathcal{O}$-algebra $\mathbb{T}(k,Q)$ with the input being the finite set $\mathcal{S}$ of matrices obtained from the last step. The process for $\widetilde{\mathbb{T}}(k,Q)$ is identical. The rough idea is to view $\mathbb{T}(k,Q)$ as a finite free $\mathcal{O}$-module and write products of matrices in $\mathcal{S}$ into linear combinations of products of lower degree terms.

Theoretically, the matrices $S \in \mathcal{S}$ are in $M_r(\mathcal{O})$ where r is the rank of $M'(k,Q)$ as predicted by (1.2.4.3). But the computer stores data only up to a certain precision. That is to say, using a computer, we are actually computing

$$\mathbb{T}(k,Q,l) := \operatorname{Im}\left(\mathbb{T}(k,Q) \to M_r(\mathcal{O}/\lambda^l)\right)$$

for some finite precision l instead of $\mathbb{T}(k,Q)$. The following lemma justifies that to study $\mathbb{T}(k,Q)\otimes\mathbf{F}$, it is enough to understand $\mathbb{T}(k,Q,l)$ as long as l is big enough.

Proposition 1.3.3.5. *There is a positive integer prec such that*

$$\mathbb{T}(k,Q)\otimes\mathbf{F} \xrightarrow{\sim} \mathbb{T}(k,Q,l)\otimes\mathbf{F}$$

for all $l \geq prec$.

Proof. Since the transition maps among $\{\mathbb{T}(k,Q,l)\}_l$ are surjective, the projective limit commutes with mod λ-reduction:

$$\varprojlim_l \left(\mathbb{T}(k,Q,l)\otimes\mathbf{F}\right) = \left(\varprojlim_l \mathbb{T}(k,Q,l)\right)\otimes\mathbf{F} = \mathbb{T}(k,Q)\otimes\mathbf{F}.$$

Note that the right hand side is a finite dimensional $\mathbf{F}$-vector space. There exists some l on the left hand side so that $\dim(\mathbb{T}(k,Q,l)/\lambda) = \dim(\mathbb{T}(k,Q)/\lambda)$. We can take *prec* to be the smallest such l because the dimension of $\mathbb{T}(k,Q,l)/\lambda$ is monotone in l. $\square$

As one can see, the proof of the proposition is not effective; it does not construct *prec* explicitly. But we know that l is enough precision if and only if

$$\dim_{\mathbf{F}} \mathbb{T}(k, Q, l) \otimes \mathbf{F} = \dim_{\mathbf{F}} \mathbb{T}(k, Q) \otimes \mathbf{F} = r/2.$$

Since $\mathbb{T}(k, Q, l)$ is a finitely generated torsion module over $\mathcal{O}$, it is isomorphic to

$$(\mathcal{O}/\lambda^l)^{n_l} \oplus (\mathcal{O}/\lambda^{l-1})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda)^{n_1},$$

and we have

$$\dim_{\mathbf{F}} \mathbb{T}(k, Q, l) \otimes \mathbf{F} = \sum_{i=1}^{l} n_i.$$

Once we can determine the $\mathcal{O}$-module structure of $\mathbb{T}(k, Q, l)$, we can tell whether l is a large enough precision, and furthermore, we will be able to compute from the module structure the presentation of the $\mathcal{O}$-algebra $\mathbb{T}(k, Q, l)$. In order to do this, we first recall some basis propositions on finite $\mathcal{O}$-algebras.

Let M be a finitely generated $\mathcal{O}$-module that is isomorphic to

$$(\mathcal{O}/\lambda^l)^{n_l} \oplus (\mathcal{O}/\lambda^{l-1})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda)^{n_1}$$

for some non-negative integers n_i for $1 \leq i \leq l$.

Proposition 1.3.3.6. *Suppose that $\{v_1, \ldots, v_s\}$ where $s = n_l + \ldots + n_1$ is a set of generators of M that corresponds to the decomposition as above. Then there is an algorithm to write every $v \in M$ as an explicit linear combination of v_i's.*

Proof. Suppose that we have found explicit $a_i \in \mathcal{O}$ such that $v - \sum_{i=1}^{s} a_i v_i \in M[\lambda^{t_0}]$ for some integer $1 \leq t_0 \leq l$. Then

$$\lambda^{t_0-1}\left(v - \sum_{i=1}^{s} a_i v_i\right) \in M[\lambda].$$

Since $M[\lambda]$ is a vector space with basis $\{\lambda^{l-1}v_1, \ldots, v_s\}$, we can find $b_i \in \mathcal{O}$ such that

$$\lambda^{t_0-1}\left(v - \sum_{i=1}^{s} a_i v_i\right) = \sum_{i=1}^{s} b_i \left(\mathrm{ord}(v_i)/\lambda\right) v_i = \sum_{\mathrm{ord}(v_i)<\lambda^{t_0}} b_i \left(\mathrm{ord}(v_i)/\lambda\right) v_i$$
$$+ \sum_{\mathrm{ord}(v_i)\geq\lambda^{t_0}} b_i \left(\mathrm{ord}(v_i)/\lambda\right) v_i.$$

Thus

$$v - \sum_{i=1}^{s} a_i v_i - \sum_{\mathrm{ord}(v_i)\geq\lambda^{t_0}} b_i(\mathrm{ord}(v_i)/\lambda^{t_0})v_i \in M[\lambda^{t_0-1}].$$

By induction on t_0, we can eventually write v as an explicit linear combination of $v_1, \ldots, v_s$.

□

Proposition 1.3.3.7. *If for some integer $0 \leq m \leq l$,*

$$\lambda^m M \xrightarrow{\sim} (\mathcal{O}/\lambda^{l-m})^{n_l} \oplus (\mathcal{O}/\lambda^{l-1-m})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda)^{n_{m+1}}$$

such that the corresponding generators are $\lambda^m v_1, \ldots, \lambda^m v_s$ where $s = \sum_{i=m+1}^{l} n_i$. Then

$$\sum_{i=1}^{s} \mathcal{O}v_i \xrightarrow{\sim} (\mathcal{O}/\lambda^l)^{n_l} \oplus (\mathcal{O}/\lambda^{l-1})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda^{m+1})^{n_{m+1}}.$$

Proof. It is straightforward that if $\lambda^m v_i$ has order λ^n, then v_i has order λ^{n+m}. We need to justify that the sum on the left hand side is a direct sum. Suppose that

$$\sum_{i=1}^{s'} a_i v_i = 0$$

for some $a_i \in \mathcal{O}/\mathrm{ord}(v_i)$ and some integer $1 \leq s' \leq s$ such that $a_{s'} \neq 0$. Then

$$\sum_{i=1}^{s'} a_i(\lambda^m v_i) = \lambda^m \sum_{i=1}^{s'} a_i v_i = 0.$$

Thus $a_i = 0 \in \mathcal{O}/\mathrm{ord}(v_i)\lambda^{-m}$ for all $1 \leq i \leq s'$ because $\sum_{i=1}^{s} \mathcal{O}\lambda^m v_i = \bigoplus_{i=1}^{s} \mathcal{O}\lambda^m v_i$ by our assumption. Since $\mathrm{ord}(v_i) \geq \mathrm{ord}(v_{s'})$ for all $1 \leq i \leq s'$, we have $a_i = 0 \in \mathcal{O}/\mathrm{ord}(v_{s'})\lambda^{-m}$ for all $1 \leq i \leq s'$. Thus $\mathrm{ord}(v_{s'})\lambda^{-m}|a_i$ for all $1 \leq i \leq s'$. In particular, $\lambda|a_i$. Now if $m \geq 1$, we have

$$\sum_{i=1}^{s'} \frac{a_i}{\lambda}\lambda^m v_i = \lambda^{m-1} \sum_{i=1}^{s} a_i v_i = 0.$$

By the same argument, we conclude that $\mathrm{ord}(v_{s'})\lambda^{-m+1}|a_i$ for all i. Repeat this argument and we see that $\mathrm{ord}(v_{s'})|a_i$ for every $1 \leq i \leq s'$. Thus $a_{s'} = 0$, which contradicts the choice of s'. Hence, there is no such linear combination and the proof is complete. □

From now on we assume M is also a finite $\mathcal{O}$-algebra generated by $m_1, \ldots, m_n$. For every non-negative integer d, denote by M_d the $\mathcal{O}$-submodule generated by the set

$$\{m_1^{d_1} \cdots m_n^{d_n}\}_{\sum_i d_i \leq d}.$$

Suppose that $\{\lambda^{t_0} v_1, \ldots, \lambda^{t_0} v_{s'}\}$ is a set of $\mathcal{O}$-module generators of $\lambda^{t_0} M$ for some $1 \leq t_0 \leq l$ and $s' = n_{t_0+1} + \ldots + n_l$ such that

$$\lambda^{t_0} M = \bigoplus_{i=1}^{s'} \mathcal{O}v_i = \lambda^{t_0} M \xrightarrow{\sim} (\mathcal{O}/\lambda^{l-t_0})^{n_l} \oplus (\mathcal{O}/\lambda^{l-1-t_0})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda)^{n_{t_0+1}}. \quad (1.3.3.8)$$

By Proposition 1.3.3.7, we have

$$M' := \sum_{i=1}^{s'} \mathcal{O}v_i \xrightarrow{\sim} (\mathcal{O}/\lambda^l)^{n_l} \oplus (\mathcal{O}/\lambda^{l-1})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda^{t_0+1})^{n_{t_0+1}}.$$

In particular,

$$\lambda^{t_0-1}M' = \sum_{i=1}^{s'} \mathcal{O}\lambda^{t_0-1}v_i \xrightarrow{\sim} (\mathcal{O}/\lambda^{l-t_0+1})^{n_l} \oplus (\mathcal{O}/\lambda^{l-t_0})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda^2)^{n_{t_0+1}}.$$

Consider the finite dimensional $\mathbf{F}$-vector space $(\lambda^{t_0-1}M)[\lambda]$. It has a subspace V with a basis $\{\lambda^{l-1}v_1, \ldots, \lambda^{t_0}v_{s'}\}$.

Proposition 1.3.3.9. *If we can extend the basis of V to a basis*

$$\{\lambda^{l-1}v_1, \ldots, \lambda^{t_0}v_{s'}, \lambda^{t_0-1}v_{s'+1}, \ldots, \lambda^{t_0-1}v_{s'+n_{t_0}}\}$$

of $(\lambda^{t_0-1}M)[\lambda]$, then

$$\lambda^{t_0-1}M = \lambda^{t_0-1}M' \oplus \mathcal{O}\lambda^{t_0-1}v_{s'+1} \cdots \oplus \mathcal{O}\lambda^{t_0-1}v_{s'+n_{t_0}}. \tag{1.3.3.10}$$

Proof. Denote by W the $\mathbf{F}$-vector space spanned by $\{\lambda^{t_0-1}v_{s'+1}, \ldots, \lambda^{t_0-1}v_{s'+n_{t_0}}\}$. For every polynomial f in M, by our assumption, we have $\lambda^{t_0}f = \sum_{i=1}^{s'} a_i\lambda^{t_0}v_i$. Thus

$$\lambda^{t_0-1}\left(f - \sum_{i=1}^{s'} a_i v_i\right) \in (\lambda^{t_0-1}M)[\lambda].$$

Therefore, $\lambda^{t_0-1}M = \lambda^{t_0-1}M' + (\lambda^{t_0-1}M)[\lambda] = \lambda^{t_0-1}M' + \mathcal{O}\lambda^{t_0-1}v_{s'+1} \cdots + \mathcal{O}\lambda^{t_0-1}v_{s'+n_{t_0}}$. It suffices to show that it is a direct sum. If

$$\lambda^{t_0-1}m' = \sum_{i=1}^{n_{t_0}} a_i\lambda^{t_0-1}v_{s'+i}$$

for some $m' \in M'$ and $a_i \in \mathcal{O}$, then $\lambda^{t_0-1}m' \in \lambda^{t_0-1}M' \cap W = V \cap W = 0$ and the proof is complete. $\square$

Definition 1.3.3.11. For a fixed choice of a family of compatible lifting maps $\{\mathcal{O}/\lambda^{t_0} \to$

$\mathcal{O}\}_{t_0 \geq 1}$ such that 0 and 1 are lifted to 0 and 1 respectively and a choice of generators of $\lambda^{t_0} M$ that correspond to a decomposition as in (1.3.3.8), we define a map $D_{t_0-1} : M \to (\lambda^{t_0-1}M)[\lambda]$ to be

$$D(f) = \lambda^{t_0-1}(f - \sum_{i=1}^{s'} a_i v_i)$$

for $f \in M$ if $\lambda^{t_0} f = \lambda^{t_0} \sum_{i=1}^{s'} a_i v_i$. Here the a_i is an element in $\mathcal{O}$ that is determined by the family of lifting maps.

Remark 1.3.3.12. The map D is not linear because the lifting maps $\mathcal{O}/\lambda^n \to \mathcal{O}$ are not linear, but it becomes linear after we compose it with the quotient map $(\lambda^{t_0-1}M)[\lambda] \twoheadrightarrow (\lambda^{t_0-1}M)[\lambda]/V$. To see this, let f and g be elements in M. Then there exist a_i, b_i and c_i in $\mathcal{O}$ such that

$$D(f) = \lambda^{t_0-1}\left(f - \sum_{i=1}^{s'} a_i v_i\right), \quad D(g) = \lambda^{t_0-1}\left(g - \sum_{i=1}^{s'} b_i v_i\right),$$
$$D(f+g) = \lambda^{t_0-1}\left(f - \sum_{i=1}^{s'} c_i v_i\right).$$

We have

$$D(f+g) - D(f) - D(g) = \lambda^{t_0-1}\sum_{i=1}^{s'}(a_i + b_i - c_i)v_i \in \lambda^{t_0-1}M' \cap (\lambda^{t_0-1}M)[\lambda] = V.$$

For every non-negative integer d, we denote by K_d the $\mathbf{F}$-subspace spanned by

$$\lambda^{t_0-1}\left(f - \sum_{i=1}^{s'} a_i v_i\right)$$

for all f that are monomials in M_d.

Proposition 1.3.3.13. *Suppose that* $\{v_1, \ldots, v_{s'}\}$ *is contained in* $M_{d'}$ *for some integer* $d' \geq$

1.

1. $D_{t_0-1}(M_d) \subseteq K_d + V$.

2. *If* $\lambda^{t_0-1} f \in (\lambda^{t_0-1} M)[\lambda]$, *then* $D_{t_0-1}(f) = \lambda^{t_0-1} f$.

3. *If* $d \geq d'$, *then* $K_d \subseteq \lambda^{t_0-1} M_d$.

Proof.

1. Since $D_{t_0-1} : M \to (\lambda^{t_0-1} M)[\lambda]$ is $\mathcal{O}$-linear after we quotient out V, we have $D_{t_0-1}(M_d)/V = K_d$ and thus $D_{t_0-1}(M_d) \subseteq K_d + V$.

2. Let $f \in M$ be an element such that $\lambda^{t_0-1} f \in (\lambda^{t_0-1} M)[\lambda]$. Then $\lambda^{t_0} f = 0$ and thus

$$D_{t_0-1}(f) = \lambda^{t_0-1} f - 0 = \lambda^{t_0-1} f$$

because we fix the lifting maps so that 0 is always lifted to 0.

3. Let f be a monomial in M_d such that $\lambda^{t_0} f = \sum_{i=1}^{s'} a_i \lambda^{t_0} v_i$. Then

$$D_{t_0-1}(f) = \lambda^{t_0-1} \left(f - \sum_{i=1}^{s'} a_i v_i \right) \in \lambda^{t_0-1} M_d + \lambda^{t_0-1} M_{d'} = \lambda^{t_0-1} M_d$$

since $d \geq d'$.

□

Proposition 1.3.3.14. *If for some* $d_0 \geq d'$, *the vector spaces* $K_{d_0} + V = K_{d_0+1} + V$, *then*

$$(\lambda^{t_0-1} M)[\lambda] = K_{d_0} + V.$$

Proof. By Proposition 1.3.3.13 (1), it is enough to establish $K_d + V = K_{d_0} + V$ for all $d \geq d_0$ and so it suffices to prove the case where $d = d_0 + 2$. Let f be a monomial of degree $d_0 + 2$.

Without loss of generality, we may and do assume that $f = m_1 f_1$ for some monomial f_1 of degree $d_0 + 1$. Suppose that

$$D_{t_0-1}(f) = \lambda^{t_0-1}\left(f - \sum_{i=1}^{s'} a_i v_i\right) \quad \text{and} \quad D_{t_0-1}(f_1) = \lambda^{t_0-1}\left(f_1 - \sum_{i=1}^{s'} b_i v_i\right).$$

Now we have

$$\begin{aligned} D_{t_0-1}(f) = \lambda^{t_0-1}\left(f - \sum_{i=1}^{s'} a_i v_i\right) &= \lambda^{t_0-1}\left(m_1 f_1 - \sum_{i=1}^{s'} a_i v_i\right) \\ &= m_1 D_{t_0-1}(f_1) + \lambda^{t_0-1}\sum_{i=1}^{s'} b_i m_1 v_i - \lambda^{t_0-1}\sum_{i=1}^{s'} a_i v_i \\ &\in m_1(K_{d_0+1} + V) + \lambda^{t_0-1} M_{d'+1} \subseteq m_1(K_{d_0} + V) + \lambda^{t_0-1} M_{d_0+1}. \end{aligned}$$

We have

$$K_{d_0} \subseteq \lambda^{t_0-1} M_{d_0}$$

by Proposition 1.3.3.13 (3) and V is obviously a submodule of $\lambda^{t_0-1} M_{d'} \subseteq \lambda^{t_0-1} M_{d_0}$. Thus

$$D_{t_0-1}(f) \in m_1(K_{d_0} + V) + \lambda^{t_0-1} M_{d_0+1} \subseteq \lambda^{t_0-1} m_1 M_{d_0} + \lambda^{t_0-1} M_{d_0+1} = \lambda^{t_0-1} M_{d_0+1}.$$

Let g be an element of M_{d_0+1} such that $D_{t_0-1}(f) = \lambda^{t_0-1} g$. Then g is an element that satisfies the condition in Proposition 1.3.3.13 (3) and thus $D_{t_0-1}(g) = \lambda^{t_0-1} g$. Now we have

$$D_{t_0-1}(f) = \lambda^{t_0-1} g = D_{t_0-1}(g) \in D_{t_0-1}(M_{d_0+1}) \subseteq K_{d_0+1} + V = K_{d_0} + V.$$

□

Proposition 1.3.3.15. *There is an algorithm to find a set $\{v_1, \ldots, v_s\}$ of $\mathcal{O}$-module gener-*

ators of M that corresponds to the decomposition

$$M \xrightarrow{\sim} (\mathcal{O}/\lambda^l)^{n_l} \oplus (\mathcal{O}/\lambda^{l-1})^{n_{l-1}} \oplus \ldots \oplus (\mathcal{O}/\lambda)^{n_1}$$

in terms of polynomials in $m_1, \ldots, m_n$. Here $s = n_1 + \ldots + n_l$.

Proof. Suppose that we have found a set $\{v_1, \ldots, v_{s'}\}$ such that a decomposition of $\lambda^{t_0} M$ as in (1.3.3.8) holds for some $1 \le t_0 \le l$ and $s' = n_{t_0+1} + \ldots + n_l$. By Proposition 1.3.3.9, it suffices to extend the basis of V to a basis of $(\lambda^{t_0-1}M)[\lambda]$. Note that the morphism D_{t_0-1} is computable by Proposition 1.3.3.6. We can then calculate the dimension of $K_d + V$ for $d \ge d'$. Whenever the sequence stabilizes, we have extended the basis by Proposition 1.3.3.14. By induction on t_0 we are done. □

Suppose that $\{v_1, \ldots, v_s\}$ is the set of $\mathcal{O}$-module generators we have found from the proposition above and the set is in M_{d_0} for some positive integer d_0. We denote by ϕ_i a polynomial of degree at most d_0 in $\mathcal{O}[x_1, \ldots, x_n]$ such that $\phi_i(m_1, \ldots, m_n) = v_i$. For an element $f \in M$, we apply Proposition 1.3.3.6 to find $a_i(f) \in \mathcal{O}$ such that

$$f = \sum_{i=1}^{s} a_i(f) v_i.$$

Lemma 1.3.3.16. *The finite $\mathcal{O}$-algebra M has presentation*

$$M \xrightarrow{\sim} \mathcal{O}[\![x_1, \ldots, x_n]\!]/I$$

where I is generated by

$$\mathrm{ord}(v_i)\phi_i$$

for $i = 1, \dots s$ together with

$$\phi(m_1, \dots, m_n) - \sum_{i=1}^{s} a_i(\phi(m_1, \dots, m_n))\phi_i$$

for all monomials $\phi \in \mathcal{O}[x_1, \dots, x_n]$ of degree at most $d_0 + 1$.

Proof. Suppose that $M \xrightarrow{\sim} \mathcal{O}[\![x_1, \dots, x_n]\!]/I$. Denote by I_{d_0+1} the ideal generated by

$$\phi(m_1, \dots, m_n) - \sum_{i=1}^{s} a_i(\phi(m_1, \dots, m_n))\phi_i$$

for all monomials $\phi \in \mathcal{O}[x_1, \dots, x_n]$ of degree at most $d_0 + 1$. We want to show $I = I_{d_0+1}$. It is clear that $I_{d_0+1} \subseteq I$. We now prove the other inclusion. Let $\psi(x_1, \dots, x_n) \in I$ be a polynomial of degree $d \geq d_0 + 2$. We write $\psi = \mu(x_1, \dots, x_n) + \psi_1(x_1, \dots, x_n)$ where $\mu(x_1, \dots, x_n)$ is the sum of the highest degree terms of ψ and ψ_1 has degree at most $d - 1 \geq d_0 + 1$. By analyzing $\mu(x_1, \dots, x_n)$ term by term, we have $\mu(x_1, \dots, x_n)$ is congruent to a polynomial of degree at most $d_0 + 1$ modulo I_{d_0+1}. By induction on d, we can and do assume that ψ has degree at most $d_0 + 1$. Modulo I_{d_0+1}, we can replace every single term of ψ by a linear combination of ϕ_i. Thus we can further assume that

$$\psi = \sum_{i=1}^{s} a_i\phi_i$$

for some $a_i \in \mathcal{O}$. Since $\psi \in I$, we have

$$\sum_{i=1}^{s} a_i\phi_i(m_1, \dots, x_n) = \sum_{i=1}^{s} a_i v_i = 0.$$

But because $M \xrightarrow{\sim} \bigoplus_{i=1}^{s} \mathcal{O}v_i$, we have $\mathrm{ord}(v_i)|a_i$ for all i. Thus $\mathrm{ord}(v_i)\phi_i|a_i\phi_i$ and ψ is in I_{d_0+1}. □

1.3.4 Data processing

In this subsection, we record propositions that we use in analyzing the data we collect from the algorithm.

We are interested in whether the crystalline deformation ring $R_{\bar{r}}^{k}$ is Cohen–Macaulay, which by Proposition 1.2.3.15 and Remark 1.3.2.3 is equivalent to $R_{\bar{r}}^{k} \otimes \mathbf{F}$ being a finite free $\mathbf{F}[\![d]\!]$-algebra. This implies that $\mathbb{T}(k, Q_n) \otimes \mathbf{F}$ is finite free over $\mathbf{F}[d]/d^{p^n}$, which we can check by the following proposition.

Proposition 1.3.4.1. *A finitely generated $\mathbf{F}[d]/d^{p^n}$-module M is free if and only if the $d^{p^n-1}M$ has dimension* $(\dim_{\mathbf{F}} M)/p^n$.

Proof. Let $v_1, \ldots, v_n$ be a basis of the image of $d^{p^n-1}M$. Then there exists w_i such that $v_i = d^{p^n-1}w_i$. Suppose that $\sum_{i,j} a_{i,j} d^j w_i = 0$ for some $a_{i,j} \in \mathbf{F}$. Then

$$0 = d^{p^n-1} \sum_{i,j} a_{i,j} d^j w_i = \sum_i a_{i,0} d^{p^n-1} w_i = \sum_i a_{i,0} v_i.$$

This implies that $a_{i,0} = 0$ for all i. By multiplying by lower powers of d, we can show that $a_{i,j} = 0$ for all i, j. Thus $\{d^j w_i\}$ is a linearly independent set of $p^n(\dim_{\mathbf{F}} M)/p^n = \dim_{\mathbf{F}} M$ elements. It is an $\mathbf{F}$-basis of M and so $\{w_i\}$ is an $\mathbf{F}[d]$-basis of M, showing that M is free over $\mathbf{F}[d]/d^{p^n}$. □

If we assume that $R_{\bar{r}}^{k}$ is Cohen–Macaulay, it is natural to ask when it is Gorenstein or a complete intersection. The two properties are in fact equivalent for $R_{\bar{r}}^{k}$ by [Hu and Paškūnas, 2019, Proposition 7.8].

Lemma 1.3.4.2 (Hu–Paškūnas)**.** *The crystalline deformation ring $R_{\bar{r}}^{k}$ is Gorenstein if and only if it is a complete intersection.*

Thus we have the following.

Proposition 1.3.4.3. *If* (λ, d) *is a regular sequence,* $R_{\bar{r}}^{k}/(\lambda, d) \xrightarrow{\sim} \mathbb{T}(k, \varnothing) \otimes \mathbf{F}$ *is a complete intersection ring if and only if* $\dim_{\mathbf{F}} (\mathbb{T}(k, \varnothing) \otimes \mathbf{F}) [\mathfrak{m}_{\varnothing}] = 1$.

Apart from the ring theoretic properties of the crystalline deformation ring $R_{\bar{r}}^{k}$ for a fixed k, we are interested in the family $\{R_{\bar{r}}^{k} \otimes \mathbf{F}\}_{k \equiv k_0 \pmod{p-1}}$ as we have mentioned in the introduction. Since there is an injection induced by multiplication by the Hasse invariant $M_{k-(p-1)}(k, Q) \otimes \mathbf{F} \hookrightarrow M(k, Q) \otimes \mathbf{F}$ for all weights k and sets Q of Taylor–Wiles primes, heuristically, the Hecke algebra $\mathbb{T}(k, Q) \otimes \mathbf{F}$ is more "complicated" than $\mathbb{T}(k-(p-1), Q) \otimes \mathbf{F}$. After patching, we expect the same phenomenon for the crystalline deformation rings $R_{\bar{r}}^{k}$. One can ask whether there is a map $R_{\bar{r}}^{k} \otimes \mathbf{F} \to R_{\bar{r}}^{k-(p-1)} \otimes \mathbf{F}$ and moreover whether the map is surjective. If such a surjection exists, it will induce a surjection on the Hecke algebras $\mathbb{T}(k, Q) \otimes \mathbf{F} \twoheadrightarrow \mathbb{T}(k-(p-1), Q) \otimes \mathbf{F}$. We can check this by computing if the ideal of relations of $\mathbb{T}(k, Q) \otimes \mathbf{F}$ is contained in that of $\mathbb{T}(k-(p-1), Q) \otimes \mathbf{F}$. Furthermore, we can measure the "complexity" by using the Hilbert series $H_k(x)$ of $R_{\bar{r}}^{k} \otimes \mathbf{F}$. Recall that the Hilbert series $H(x)$ of a Noetherian local ring $(R, \mathfrak{m})$ is defined to be the formal power series

$$H(x) := \sum_{i=0}^{\infty} \dim(\mathfrak{m}^i/\mathfrak{m}^{i+1}) x^i.$$

We can compute the Hilbert series of $\mathbb{T}(k, Q) \otimes \mathbf{F}$ to approximate $H_k(x)$.

The discussion above mostly applies to $R_{\bar{r}}^{k}[\alpha_p]$.

Proposition 1.3.4.4. *Under assumption 1.3.2.4 (1)–(5), we have the following.*

1. *The ring* $R_{\bar{r}}^{k}[\alpha_p]$ *is Cohen–Macaulay.*

2. *The ring* $R_{\bar{r}}^{k}[\alpha_p]$ *can be Gorenstein but not a complete intersection.*

3. *There is a surjection* $R_{\bar{r}}^{k}[\alpha_p] \otimes \mathbf{F} \twoheadrightarrow R_{\bar{r}}^{k-(p-1)}[\alpha_p] \otimes \mathbf{F}$ *for all weights* $k \geq 2$.

Proof. By construction, the ring $R_{\bar{r}}^{k}[\alpha_p][\![t_1, \ldots, t_h]\!] \otimes \mathbf{F}$ is finite free over $\mathbf{F}[\![d_1, \ldots, d_{\#Q}]\!]$ The first assertion then follows from Proposition 1.2.3.15. We provide an example to assertion

(2). When $p = 5, k = 106$, the Hecke algebra $\widetilde{\mathbb{T}}(106, \varnothing) \otimes \mathbf{F}$ is isomorphic to

$$\mathbf{F}_5[\![x, y, z]\!]/(z^3 + 2yx^3, zy + 4yx^3, zx + 2yx^3, y^2 + 4yx^2 + 3yx + x^3 + 2x^2, x^4),$$

which is not a complete intersection ring. But it is Gorenstein because $\dim \left(\widetilde{\mathbb{T}}(106, \varnothing) \otimes \mathbf{F}\right)[\widetilde{\mathfrak{m}}] = 1$. Assertion (3) is a result from Bao [2023a]. □

We are also interested in the relation between $R_{\bar{r}}^k$ and $R_{\bar{r}}^k[\alpha_p]$. Since $R_{\bar{r}}^k[\alpha_p]$ is in the integral closure of $R_{\bar{r}}^k$ in $R_{\bar{r}}^k[1/p]$. It is natural to ask whether $R_{\bar{r}}^k[\alpha_p]$ is the normalization.

Proposition 1.3.4.5. *The ring $R_{\bar{r}}^k[\alpha_p]$ is the normalization of $R_{\bar{r}}^k$ in $R_{\bar{r}}^k[1/p]$ if and only if $R_{\bar{r}}^k[\alpha_p]$ is normal.*

Proof. The ring $R_{\bar{r}}^k[\alpha_p]$ is reduced because it is a subring of the reduced ring $R_{\bar{r}}^k[1/p]$. A reduced Noetherian ring R is normal if and only if it is integrally closed in its total ring of fractions $\mathrm{Frac}(R)$. If $R_{\bar{r}}^k[\alpha_p]$ is normal, then it is integrally closed in

$$R_{\bar{r}}^k[1/p] = R_{\bar{r}}^k[\alpha_p][1/p] \subseteq \mathrm{Frac}(R_{\bar{r}}^k[\alpha_p]).$$

Hence it is the integral closure of $R_{\bar{r}}^k$ in $R_{\bar{r}}^k[1/p]$. Conversely, suppose that $R_{\bar{r}}^k[\alpha_p]$ is the integral closure of $R_{\bar{r}}^k$ in $R_{\bar{r}}^k[1/p]$. In order to show it is normal, by Serre's criterion, it suffices to check R1 + S2. Since $R_{\bar{r}}^k[\alpha_p]$ is reduced and Cohen-Macaulay, Sk is true all all positive integers k and R0 is true. It remains to show $R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}}$ is a regular local ring for all the prime ideals $\mathfrak{p}$ of $R_{\bar{r}}^k[\alpha_p]$ that are of height one. There are two cases. If $p \notin \mathfrak{p}$, then

$$R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}} = R_{\bar{r}}^k[\alpha_p][1/p]_{\mathfrak{p}}.$$

Kisin showed that $R_{\bar{r}}^k[\alpha_p][1/p] = R_{\bar{r}}^k[1/p]$ is formally smooth, and thus its localizations are regular local. So let's assume $p \in \mathfrak{p}$. We note that $R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}}$ has Krull dimensional one; it is regular local if and only if it is normal, i.e. it is integrally closed in its total ring of fractions. Since localization preserves integral closure, we still have $R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}}$ is integrally closed in $R_{\bar{r}}^k[1/p]_{\mathfrak{p}} = R_{\bar{r}}^k[\alpha_p][1/p]_{\mathfrak{p}}$. Since $p \in \mathfrak{p}$ and we are inverting p, the only prime ideals of $R_{\bar{r}}^k[\alpha_p][1/p]_{\mathfrak{p}}$ are the minimal prime ideals that are contained in $\mathfrak{p}$. Thus this ring is Artinian and it is a product of its localizations at minimal prime ideals which are fields since the ring is reduced) and this is exactly the total ring of fractions of $R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}}$ (it is easy to see that it is contained in the total ring of fractions; but then it is not hard to show we have already inverted every non-zerodivisor in this ring.) The proof is complete. $\square$

From the proof we see that to check $R_{\bar{r}}^k[\alpha_p]$ is the normalization, it is enough to check whether $R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}}$ is regular local for every $\mathfrak{p}$ that contains p. If $p \notin \mathfrak{p}^2$, then this is equivalent to checking whether $R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}} \otimes \mathbf{F}$ is regular.

Remark 1.3.4.6. If we assume a Breuil-Mézard conjecture for $R_{\bar{r}}^k[\alpha_p] \otimes \mathbf{F}$, then the Hilbert–Samuel multiplicity of $R_{\bar{r}}^k[\alpha_p]_{\mathfrak{p}} \otimes \mathbf{F}$ is equal to the Jordan–Hölder multiplicity of one of the Serre weights of $\overline{\rho}$ in the semisimplification of Sym^{k-2}, which is apparently not equal to 1 when k is large. This leads to the discussion in §**??**. One can start to compute the Hilbert–Samuel multiplicity of $R_{\bar{r}}^k[\alpha_p] \otimes \mathbf{F}$ by computing the Hilbert series of $\widetilde{\mathbb{T}}(k, Q) \otimes \mathbf{F}$ and compare this number with that of $R_{\bar{r}}^k \otimes \mathbf{F}$.

Given that $R_{\bar{r}}^k[\alpha_p]$ has many nice properties that we expect $R_{\bar{r}}^k$ to have, we are interested in how different the two rings are from each other. Therefore, we study the cokernel $C^k := R_{\bar{r}}^k[\alpha_p]/R_{\bar{r}}^k$ which can be obtained by patching $C(k, Q) := \widetilde{\mathbb{T}}(k, Q)/\mathbb{T}(k, Q)$. Consider the short exact sequence of finitely generated $\mathcal{O}$-modules

$$0 \to \mathbb{T}(k, Q) \to \widetilde{\mathbb{T}}(k, Q) \to C(k, Q) \to 0.$$

Tensor the sequence with $\mathbf{F}$ and we get the exact sequence

$$0 \to C(k, Q)[\lambda] \to \mathbb{T}(k, Q) \otimes \mathbf{F} \to \widetilde{\mathbb{T}}(k, Q) \otimes \mathbf{F} \to C(k, Q) \otimes \mathbf{F} \to 0.$$

Apply the patching functor and we have

$$0 \to C^k[\lambda] \to R^k_{\bar{r}}[\![t_1, \dots, t_h]\!] \otimes \mathbf{F} \to R^k_{\bar{r}}[\alpha_p][\![t_1, \dots, t_h]\!] \otimes \mathbf{F} \to C^k \otimes \mathbf{F} \to 0.$$

We can prove that $C(k, Q) \otimes \mathbf{F}$ has the desired property and we can compute the rank.

Lemma 1.3.4.7. *Under Assumption 1.3.2.4 (1)–(5), the module $C(k, Q_n) \otimes \mathbf{F}$ is finite free over $\mathbf{F}[\![d_1, \dots, d_{\#Q_n}]\!]/(d_1^{p^n}, \dots, d_{\mathbf{Q}_n}^{p^n})$ The kernel of the surjection*

$$C(k, Q) \otimes \mathbf{F} \twoheadrightarrow C(k - (p-1), Q) \otimes \mathbf{F}$$

has dimension equal to that of

$$W(j, Q_n) := M(j, Q_n) \otimes \mathbf{F}/M(j - (p-1), Q_n) \otimes \mathbf{F}.$$

Proof. Consider the q-expansion map

$$S_k(\Gamma_1(N), L) \to L[\![q]\!]$$

that maps a modular form f over the fraction field F of $\mathcal{O}$ to its q-expansion at ∞. By the q-expansion principal (see for example [Diamond and Im, 1995, Theorem 12.3.4]), this map is injective and the preimage of $\mathcal{O}[\![q]\!] \subset L[\![q]\!]$ is $S_k(\Gamma_1(N), \mathcal{O})$. By [Ribet, 1983, (1.6) and (2.2)], the following pairing is perfect:

$$\begin{aligned} \widetilde{\mathbb{T}} \times S_k(\Gamma_1(N), \mathcal{O}) &\to \mathcal{O} \\ (T, f) &\mapsto a_1(Tf), \end{aligned}$$

where $\widetilde{\mathbb{T}}$ is the $\mathcal{O}$-subalgebra of $\mathrm{End}_F(S_k(\Gamma_1(N)), L)$ generated by all the Hecke operators.

Now consider the anemic q-expansion map

$$S_k(\Gamma_1(N), \mathcal{O}) \to \bigoplus_{p \nmid n} Lq^n$$

that maps a modular form f to its q-expansion away from p. This map is still injective by [Diamond and Shurman, 2005, Theorem 5.7.1] and we have $S_k(\Gamma_1(N), \mathcal{O})$ is a submodule of the preimage $\hat{M}$ of $\bigoplus_{p \nmid n} \mathcal{O}q^n$. We have the pairing

$$\begin{aligned} \mathbb{T} \times \hat{M} &\to \mathcal{O} \\ (T, f) &\mapsto a_1(Tf), \end{aligned}$$

where $\mathbb{T}$ is the $\mathcal{O}$-subalgebra of $\mathrm{End}_F(S_k(\Gamma_1(N)), L)$ generated by Hecke operators away from p. Let f be a modular form such that $a_1(Tf) = 0$ for all $T \in \mathbb{T}$. Then $a_n(f) = a_1(T_n f) = 0$ for all n such that $\gcd(n, p) = 1$. Thus $f = 0$ and we have an injection

$$\hat{M} \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}, \mathcal{O}).$$

Therefore, $\hat{M}$ is a finitely generated $\mathcal{O}$-module and there is some integer $A \gg 0$ such that $A\hat{M} \subseteq S_k(\Gamma_1(N), \mathcal{O})$. Thus we have

$$\mathrm{rank}_{\mathcal{O}}(\hat{M}) = \mathrm{rank}_{\mathcal{O}} S_k(\Gamma_1(N), \mathcal{O}) = \mathrm{rank}_{\mathcal{O}}(\widetilde{\mathbb{T}}) = \mathrm{rank}_{\mathcal{O}}(\mathbb{T}).$$

To show that $\hat{M} \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}, \mathcal{O})$ is an isomorphism, it suffices to prove that the cokernel is torsion free. Let $\varphi : \mathbb{T} \to \mathcal{O}$ be a map such that $n\varphi(T) = a_1(Tf)$ for some $f \in \hat{M}$ and integer n. Then f/n is in $\hat{M}$ by the definition of $\hat{M}$. Thus φ itself is in the image of $\hat{M}$. Hence, we have the isomorphism

$$\hat{M} \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}, \mathcal{O}).$$

Conversely, we want to show the injection

$$\mathbb{T} \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(\hat{M}, \mathcal{O})$$

is also a surjection. It suffices to show

$$\mathbb{T} \otimes \mathbf{F} \to \mathrm{Hom}_{\mathcal{O}}(\hat{M}, \mathcal{O}) \otimes \mathbf{F} = \mathrm{Hom}_{\mathbf{F}}(\hat{M} \otimes \mathbf{F}, \mathbf{F})$$

is an injection. If not, then there is a $T \in \mathbb{T} \setminus \lambda\mathbb{T}$ such that $a_1(T(f)) \in \lambda\mathcal{O}$ for all $f \in \hat{M}$. Then $a_n(Tf) = a_1(TT_n f)$ is in $\lambda\mathcal{O}$. Thus Tf is in $\lambda\hat{M}$, which implies that $\mathbb{T} \otimes \mathbf{F}$ does not act faithfully on $\hat{M} \otimes \mathbf{F}$. But $\hat{M} \otimes \mathbf{F} \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}, \mathcal{O}) \otimes \mathbf{F} = \mathrm{Hom}(\mathbb{T} \otimes \mathbf{F}, \mathbf{F})$ on which $\mathbb{T} \otimes \mathbf{F}$ acts faithfully, a contradiction. Therefore, $\mathbb{T}$ and $\hat{M}$ are dual to each other. We have a short exact sequence

$$0 \to M \to \hat{M} \to Q \to 0$$

where Q_k is the cokernel $\hat{M}/M$. Tensoring with $\mathbf{F}$, we get

$$0 \to Q_k[\lambda] \to M \otimes \mathbf{F} \to \hat{M} \otimes \mathbf{F} \to Q \otimes \mathbf{F} \to 0.$$

Now taking the $\mathbf{F}$-dual we get

$$0 \to (Q \otimes \mathbf{F})^{\vee} \to \mathbb{T} \otimes \mathbf{F} \to \widetilde{\mathbb{T}} \otimes \mathbf{F} \to (Q_k[\lambda])^{\vee} \to 0.$$

Thus we have the identification $C_k \otimes \mathbf{F} = (Q_k[\lambda])^{\vee}$. Note that $Q[\lambda]$ is the kernel of $M \otimes \mathbf{F} \to \hat{M} \otimes \mathbf{F}$, we have

$$Q_k[\lambda] = \{f \in M \otimes \mathbf{F} :\ q\text{−expansion has only } q^{pn} \text{ terms}\} = \ker\theta = \mathrm{Im}\, V.$$

Let j be the largest integer such that $V(M_j \otimes \mathbf{F}) \subseteq M_k$. Then

$$M_j \otimes \mathbf{F} \xrightarrow{V} Q_k[\lambda]$$

is an isomorphism. Since $w(Vf) = pw(f)$ for every mod-p modular form f, the map above is an injection. Suppose that f is a mod-p cusp form such that $Vf \in M_k$. Then $pw(f) = w(Vf) \leq k$ and so $w(f) \leq \lfloor k/p \rfloor$. If $w(f) > j$, then $VM_{w(f)} \subseteq M_k$, contradicting the choice of j. This map then induces an isomorphism

$$W_j := M_j/M_{j-(p-1)} \xrightarrow{V} Q_k[\lambda]/Q_{k-(p-1)}[\lambda].$$

For filtration reason, we see that $Q_k[\lambda]/Q_{k-(p-1)}[\lambda]$ is trivial unless $k = jp$.

Note that all of our discussions above are compatible with the Hecke action; hence, they still hold true after we localize at a maximal ideal of the Hecke algebra. It follows that $(Q[\lambda])_{\mathfrak{m}_{Q_n}}$ is finite free over $\mathbf{F}[\![d_1, \ldots, d_{\#Q_n}]\!]/(d_1^{p^n}, \ldots, d_{\#Q_n}^{p^n})$ because $M(j, Q_n)$ is. Then $C(k, Q_k) \otimes \mathbf{F} \xrightarrow{\sim} (Q_k \otimes \mathbf{F})^\vee$ is an injective module. Since the group algebra of a finite group is a Frobenius algebra, an injective module is also projective and therefore finite free over $\mathbf{F}[\![d_1, \ldots, d_{\#Q_n}]\!]/(d_1^{p^n}, \ldots, d_{\#Q_n}^{p^n})$. □

Since $R_{\bar{r}}^k[\alpha_p][\![t_1, \ldots, t_h]\!] \otimes \mathbf{F}$ is finite free over $\mathbf{F}[\![d_1, \ldots, d_{\#Q}]\!]$, so is the image of $R_{\bar{r}}^k \otimes \mathbf{F}$ in $R_{\bar{r}}^k[\alpha]_p \otimes \mathbf{F}$. If we can show that $C^k[\lambda]$ is finite free over $\mathbf{F}[\![d]\!]$, then we can conclude that $R_{\bar{r}}^k$ is Cohen–Macaulay. Thus it is interesting to see if $C(k, Q_n)[\lambda]$ is finite free over $\mathbf{F}[\![d]\!]/(d^{p^n})$ and if so, what rank it has.

Proposition 1.3.4.8. *Under the assumption so that the minimal level patching works, we always have* $\dim W_n \xrightarrow{\sim} \dim W_{n-(p^2-1)}$ *for all integers* $n \geq p^2 - 1$. *When* $k_0 = 2$, *we have* $\dim W_n = \dim W_2 \neq 0$ *for all* $n \equiv 2, 2p \mod p^2 - 1$ *and* 0 *otherwise.*

Proof. By Lemma 1.2.4.3, it suffices to show the cycles satisfy

$$Z(R_{\overline{r}}^{n} \otimes \mathbf{F}) - Z(R_{\overline{r}}^{n-(p-1)} \otimes \mathbf{F}) = Z(R_{\overline{r}}^{n-(p^2-1)} \otimes \mathbf{F}) - Z(R_{\overline{r}}^{n-(p^2-1)-(p-1)} \otimes \mathbf{F}).$$

By the geometric Breuil–Mézard conjecture, this is equivalent to

$$[\mathrm{Sym}^{n}\mathbf{F}^2] - [\mathrm{Sym}^{n-(p-1)}\mathbf{F}^2] = [\mathrm{Sym}^{n-(p^2-1)}\mathbf{F}^2] - [\mathrm{Sym}^{n-(p^2-1)-(p-1)}\mathbf{F}^2],$$

where $[V]$ means taking the semisimplification of a $\mathrm{GL}_2(\mathbf{F}_p)$-representation V. This follows from the equation from [Reduzzi, 2015, §2.3]

$$[\mathrm{Sym}^{n}\mathbf{F}^2] - [\mathrm{Sym}^{n-(p-1)}\mathbf{F}^2] = [\det]([\mathrm{Sym}^{n-(p+1)}\mathbf{F}^2] - [\mathrm{Sym}^{n-(p-1)-(p+1)}\mathbf{F}^2]).$$

□

Remark 1.3.4.9. The proof works in general. It is just when $k_0 = 2$, we have worked out the structure of W_n.

1.3.5 Implementation of matrix multiplication

The hard part of the implementation is to find an effective way to deal with large matrix multiplication. The rank of $Z^1(\Gamma_Q, \mathrm{Sym}^{k-2}\mathcal{O}^2)$ is

$$\#S_Q \cdot (k-1),$$

where S_Q is a minimal set of free generators of Γ_Q. The cardinality of S_Q can be estimated by the Riemann–Roch theorem:

$$\#S_Q \sim \frac{d}{12}$$

where d is the degree of $X(\Gamma_Q) \to X(1)$ and this is growing at the speed of $\prod_{q \in Q_n} q$ and $q \equiv 1 \pmod{p^n}$. So the size of the matrix is roughly

$$12(k-1) \prod_{q \in Q_n} q.$$

On the other hand, we would like to see the behavior of $\mathbb{T}(k, Q_n)$ when k is large, at least p^3. For example, if $p = 5, n = 1, q = 11$, then we are multiplying matrices of size $16,000$ by $16,000$.

We use NumPy to handle matrix multiplication. This library is fast with handling arrays, including matrix multiplication.

A few (but not all) reasons why NumPy is fast:

1. Underlying parallelization (which is great since from a high performance cluster we can ask for as many cores as we want)

2. Using machine-native datatype

I do not really understand this second bullet-point I put here. But one result of this is that NumPy is only fast when the datatype is $\leq$ float64. The datatype float64 has 1 sign bit, 11 bits exponent, and 52 bits mantissas. So we can only store integers up to 2^{52} using a float64; otherwise, overflow happens. When we multiply two s by s matrices A and B, we need to compute $c_{i,j} = \sum_{l=1}^{n} a_{i,l} b_{l,j}$. For $c_{i,j}$ to be within 2^{52}, we need the size of $a_{i,l}$ and $b_{l,j}$ to be bounded by

$$\sqrt{\frac{2^{52}}{s}} = \frac{2^{26}}{\sqrt{s}}.$$

In practice, we have $s = \#S_Q \cdot (k-1)$. But as k grows, we need higher p-adic precision to compute $\mathbb{T}(k, Q_n) \otimes \mathbf{F}$, which grows linearly dependent on k. This is to say

$$a_{i,l} \sim b_{l,j} \sim p^k$$

and we want this to be bounded by

$$\frac{2^{26}}{\sqrt{\#Q_n(k-1)}}.$$

First year calculus tells us that this is unlikely to happen as k grows larger.

We choose the integer n_0 depending on k such that $p^{n_0} < \frac{2^{26}}{\sqrt{\#Q_n(k-1)}}$. Then we write

$$A = A_0 + A_1 p^{n_0} + \dots \quad \text{and} \quad B = B_0 + B_1 p^{n_0} + \dots.$$

Now

$$A \cdot B = A_0 B_0 + p^{n_0}(A_1 B_0 + A_0 B_1) + \dots.$$

This way we can do matrix multiplication without overflow. This method takes slightly more time in decomposing A into its p-adic expansion. We can use parallelization to carry out multiple matrix multiplication and assemble them in the end.

1.4 Examples

1.4.1 Prototype

This is a prototype of applying the algorithm in the previous section to specific examples. We start with some Schur residual representation $\overline{r} : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathbf{F})$ that takes the form described in §1.2.2.

1. Find a newform f_0 that has the minimal level and minimal weight up to twist such that $\overline{\rho}$ attached to f_0 is isomorphic to $\overline{r}$.

2. Verify the two conditions in Theorem 1.2.3.1 by studying the global residual representation $\overline{\rho}$ attached to f_0 using criteria from §1.2.3.

3. Find a finite set of Hecke operators that generate the local conditions in §1.3.1. We

check, up to weight p^2-1, that the residual representations are all determined by certain Hecke operators by searching in LMFDB LMFDB Collaboration [2022]. It suffices to look for all the eigenforms of the same level as f_0 whose Nebentypus character is congruent to that of f_0. It is important to note that, when we are searching for eigenforms in LMFDB LMFDB Collaboration [2022], only new cuspidal forms are listed.We also need to consider oldforms as well as Eisenstein series.

4. Find a set of Hecke operators that span the tangent space. By §1.3.2, it suffices to find in the initial level, the generators of the tangent space of $\mathbb{T}(k, \varnothing)$ for some $k \geq k_0 p^2$. We are given the Sturm bound $\frac{km}{12} - \frac{m-1}{N(\overline{\rho})}$ where $m := [\mathrm{SL}_2(\mathbf{Z}) : \Gamma]$ so that it suffices to compute the Hecke operators up to this number.

5. Compute the relations by the algorithm in §1.3.3.

After we obtain the presentations of Hecke algebras $\mathbb{T}(k, Q, l)$ and $\widetilde{\mathbb{T}}(k, Q, l)$ for some integer $l \geq prec$ as in Proposition 1.3.3.5, we can do the following verification.

1. Check whether the associated graded algebra of $\mathbb{T}(k, Q_n) \otimes \mathbf{F} \xrightarrow{\sim} \mathbb{T}(k, Q_n, l) \otimes \mathbf{F}$ is free over $\mathbf{F}[d]/d^{p^n}$ by Proposition 1.3.4.1.

2. Calculate $\dim_{\mathbf{F}}(\mathbb{T}(k, \varnothing) \otimes \mathbf{F})[\mathfrak{m}_{\varnothing}]$.

3. Check if there are surjections $\mathbb{T}(k, Q) \otimes \mathbf{F} \to \mathbb{T}(k - (p-1), Q) \otimes \mathbf{F}$.

4. Calculate the Hilbert series of $\mathbb{T}(k, Q) \otimes \mathbf{F}$ and $\widetilde{\mathbb{T}}(k, Q) \otimes \mathbf{F}$.

1.4.2 Example $p = 5$ and $k_0 = 2$

This is the example that we have collected most data of. Here TW1 and TW2 refer to the two conditions in the theorem of Taylor–Wiles–Kisin patching 1.2.3.1.

Modular form f_0	14.2.a.a
Image $\mathrm{P}\overline{\rho}$	$\mathrm{PGL}_2(\mathbf{F}_5) \xrightarrow{\sim} S_5$
Field of $\mathrm{P}\overline{\rho}$	Galois closure of 5.1.4802000.1
TW1	Lemma (1.2.3.3)
TW2	$2, 7 \not\equiv -1 \mod 5$
Taylor Wiles prime	$q = 11$
Localization Operators	$T_3 + 2$ and $U_{11} - 2$
Sturm bound	$m = 24, k = 50$, and bound is 99
Generators of cotangent space	$T_3 + 2, U_{11} - 2, \langle -13 \rangle - 1$

Remark 1.4.2.1 (On the table above).

1. Note that the projective image of $\overline{\rho}|_{G_{\mathbf{Q}_5}}$ is isomorphic to the dihedral group D_8 of 8 elements. The element $\mathrm{P}\overline{\rho}(\mathrm{Frob}_{29})$ has order 3. Among all transitive subgroups of $\mathrm{PGL}_2(\mathbf{F}_5) \xrightarrow{\sim} S_5$, the only one that contains a subgroup isomorphic to D_8 and an element of order 3 has to be S_5 itself.

2. We justify why $q = 11$ is a Taylor–Wiles prime. The characteristic polynomial of Frob_{11} is

$$X^2 + 1 = X^2 - 4 = (X - 2)(X + 2)$$

has two distinct roots. We need to check the Selmer group

$$H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}) = \ker(H^1(G_{\mathbf{Q},\{p,\infty\}\cup Q}, \mathrm{ad}^0\overline{\rho}) \to H^1(G_p, \mathrm{ad}^0\overline{\rho}))$$

is trivial for $Q = \{11\}$. A nontrivial class $[c]$ in the Selmer group gives rise to a surjective ring homomorphism

$$\varphi : \mathbb{T}(k_0, Q) \xrightarrow{\sim} R_Q^{k_0} \twoheadrightarrow \mathbf{F}[x]/(x^2)$$

such that when we compose it with $R_{\overline{r}}^{\text{univ}} \to R_Q^{k_0}$, the image of $R_{\overline{r}}^{\text{univ}}$ under

$$R_{\overline{r}}^{\text{univ}} \to R_Q^{k_0} \twoheadrightarrow \mathbf{F}[x]/(x^2)$$

is $\mathbf{F}$. Since $R_{\overline{r}}^{\text{univ}} \to R_Q^{k_0}$ factors through the crystalline deformation ring $R_{\overline{r}}^{k_0} \xrightarrow{\sim} \mathcal{O}[\![x]\!]$, the variable x is mapped to 0. Note that this x can be taken to be the function α_p within the Fontaine-Laffaille range and the map $R_{\overline{r}}^{k_0} \to R_Q^{k_0} \xrightarrow{\sim} \mathbb{T}(k_0, Q)$ maps α_p to T_p by [Caraiani et al., 2018, Proposition 2.9]. This implies that $\varphi(T_p) = 0$. However, by a direct computation, we see that T_p spans the one-dimensional space $\operatorname{Cot}(\mathbb{T}(k_0, Q))$, a contradiction. Thus the Selmer group $H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \operatorname{ad}^0\overline{\rho})$ is trivial.

We have computed the presentations of $\mathbb{T}(k, \{11\}, prec)$ and $\widetilde{\mathbb{T}}(k, \{11\}, prec)$ for $2 \le k \le 122$ and the presentations of $\mathbb{T}(k, \varnothing, prec)$ and $\widetilde{\mathbb{T}}(k, \varnothing, prec)$ for $2 \le k \le 622$ such that $k \equiv 2 \pmod{p-1}$ and $prec$ determined from Proposition 1.3.3.5.

Fact 1.4.2.2. The following hold true for the data we have collected.

1. The associated graded algebra of $\mathbb{T}(k, \{11\}) \otimes \mathbf{F}$ is finite free over $\mathbf{F}_p[\![d]\!]/(d^5)$.
2. The Hecke algebra $\mathbb{T}(k, \varnothing) \otimes \mathbf{F}$ is Gorenstein if and only if

$$\begin{aligned} k = {} & 10, 14, 18, 22, 34, 38, 42, 46, 58, 62, 66, 70, 82, 86, 90, 94, 106, 110, 114, 118, \\ & 226, 230, 234, 238, 346, 350, 354, 358, 466, 470, 474, 478, 586, 590, 594, 598. \end{aligned}$$

3. There is a surjection from $\mathbb{T}(k, \{11\}) \otimes \mathbf{F}$ to $\mathbb{T}(k - (p-1), \{11\})$ for $6 \le k \le 122$ and $k \equiv 2 \pmod 4$.

Example 1.4.2.3. When $10 \le k \le 30$, the Hecke algebra $\widetilde{\mathbb{T}}(k, \{11\}, l)$ is isomorphic to $\mathbf{Z}_p[\![z, d]\!]/\widetilde{I}(k, l)$ where please email me to see; the formulas do not in this thesis template.

and

$$l = \begin{cases} 5 & 10 \leq k \leq 22 \\ 6 & k = 26 \\ 10 & k = 30 \end{cases}.$$

Using the presentation of $\widetilde{\mathbb{T}}(k, \{11\}, l)$ for $10 \leq k \leq 30$ and the results from [Rozensztajn, 2020, Example 6.2.1], we can compute the presentation of $R_{\bar{r}}^{k}[\alpha_p]$.

Proposition 1.4.2.4. *When $p = 5$, there are isomorphisms*

$$R_{\bar{r}}^{k}[\alpha_p] \xrightarrow{\sim} \begin{cases} \mathbf{Z}_p[\![z, d]\!]/(zd - p) & k = 10, 14, 18, 22 \\ \mathbf{Z}_p[\![z, d]\!]/(z - p^2 d)(z^2 + (u_1(d)d + c_0)z + p^2 u_0(d)) & k = 26 \\ \mathbf{Z}_p[\![z, d]\!]/(z - p^4 d)(z^2 + (v_1(d)d + d_0)z + p v_0(d)) & k = 30 \end{cases}$$

where $u_i(d)$ and $v_i(d)$ in $\mathbf{Z}_p[\![d]\!]$ are some units and c_0 and d_0 are some constants in $p\mathbf{Z}_p$. The variable z is mapped to α_p.

Proof. By our computation, when $2 \leq k \leq 30$, the ring $R_{\bar{r}}^{k}[\alpha_p]$ is a complete intersection. When $10 \leq k \leq 30$, we further have that the cotangent space of $R_{\bar{r}}^{k}[\alpha_p]$ is two dimensional, generated by preimages of the diamond operator and T_5. Thus it is a quotient of the algebra $\mathbf{Z}_5[\![z, d]\!]$ by one element $F_k(z, d)$ such that z is mapped to α_p and d is mapped to the diamond operator. By the Weierstrass preparation theorem, we assume that

$$F_k(z, d) = (z^n + A_{n-1}(d)z^{n-1} + \ldots + A_1(d)z + A_0(d)) \cdot u_k(z, d)$$

where $A_i(d)$ is in the maximal ideal of $\mathbf{Z}_p[\![d]\!]$ and $u_k(z, d)$ is a unit in $\mathbf{Z}_p[\![z, d]\!]$. It is clear that $(F_k(z, d), p^l, (d + 1)^p - 1) \subseteq \widetilde{I}(k, l)$. The other inclusion does not need to be true. For example, when $k = 30$, this is obviously not correct. But we still have the inclusions

$$(F_{30}(z,d), p^{10}, (d+1)^5 - 1) \subseteq \widetilde{I}(30,10) \subseteq (F_{30}(z,d), p^9, (d+1)^5 - 1).$$

To see the second inclusion, we need to show

$$\widetilde{\mathbb{T}}(30,\{11\},10) \twoheadrightarrow \mathbf{Z}_p[\![z,d]\!]/(F_{30}(z,d), p^9, (d+1)^5 - 1).$$

Since

$$\begin{aligned}\mathbf{Z}_p[\![z,d]\!]/(F_{30}(z,d), p^9, (d+1)^5 - 1) &\xrightarrow{\sim} R^{30}_{\overline{r}}[\alpha_p]/(p^9, (d+1)^5 - 1)\\ &\xrightarrow{\sim} \widetilde{\mathbb{T}}(30,\{11\})/(p^9) \xrightarrow{\sim} \widetilde{\mathbb{T}}(30,\{11\}) \otimes \mathbf{Z}/p^9\mathbf{Z},\end{aligned}$$

it suffices to show

$$\widetilde{\mathbb{T}}(30,\{11\},9) \twoheadrightarrow \widetilde{\mathbb{T}}(30,\{11\}) \otimes \mathbf{Z}/p^9\mathbf{Z}.$$

We have computed directly that

$$\widetilde{\mathbb{T}}(30,\{11\},9) \xrightarrow{\sim} \left(\mathbf{Z}/5^{10}\right)^{\oplus 10} \oplus (\mathbf{Z}/5^9)^{\oplus 5}$$

as a $\mathbf{Z}$-module. Thus the claim follows.

When $k = 10$, by the presentation of $\widetilde{\mathbb{T}}(10,\{11\},5)$, we have $u_k(z,d) \equiv 1 \mod (p^5, (1+d)^p - 1)$,

$$A_1(d) \equiv 487d^4 + 2614d^3 + 1736d^2 + 2697d + 2730 \mod (p^5, (1+d)^p - 1)$$

and

$$A_0(d) \equiv 5(319d^4 + 201d^3 + 604d^2 + 156d + 594) \mod (p^5, (1+d)^p - 1).$$

When we specialize d to different values in $\overline{\mathbf{Z}}_p$, $F(d,z)$ defines a quadratic equation in z. By [Berger et al., 2003, Theorem 1.1.1], we see that the solution should satisfy $v(z) = v(T_p) = v(\alpha_p) \leq 2$ because the reduction type of crystalline representations with $v(z) > 2$ is $\mathrm{Ind}_K^{\mathbf{Q}_p} \omega_2^{k-1}$ rather than $\overline{r} = \mathrm{Ind}_K^{\mathbf{Q}_p} \omega_2$ up to an unramified twist. This implies that $v(A_0(d)) \leq 4$. We write

$$A_0(d) = a_0(d) + 5a_1(d) + 5^2 a_2(d) + \dots,$$

where $a_i(d) \in \mathbf{Z}_p[\![d]\!]$ and the nonzero coefficients in $a_i(d)$ are all in $\mathbf{Z}_p^\times$. By comparing the coefficients of powers of d, we see that the lowest degree term of $a_0(d)$ degree $n_0 \geq 5$ if $a_0(d) \neq 0$ and that $a_1(0)$ is always a unit. Now consider the power series in d

$$G(d) = a_0(d) + 5a_1(d) + 5^2 a_2(d) + 5^3 a_3(d) + 5^4 a_4(d).$$

Its Newton polygon has a segment of length n_0 of slope $-1/n_0$ if $a_0(d) \neq 0$. In particular, this implies that $G(d)$ has a root α in $\overline{\mathbf{Z}}_p$. Then

$$A_0(\alpha) = G(\alpha) + 5^5 a_5(\alpha)$$

has valuation at least 5, a contradiction. Therefore, we conclude that $a_0(d) = 0$ and thus

$$A_0(d) = 5u_0(d) = 5(4 + \dots) \in \mathbf{Z}_p[\![d]\!].$$

We let $b(d)$ be the square root of $u_0(d)$ and let $z' = z/b(d)$. Then

$$F_k(d,z)/u_0(d) = z'^2 + (A_1(d)/b(d)) \cdot z' + 5.$$

Now let

$$w = -(z' + A_1(d)/b(d)).$$

Note that $A_1(d)$ is a linear transform of d; the change of variables that we have made are all invertible. Thus

$$R^{10}_{\overline{r}}[\alpha_p] \xrightarrow{\sim} \mathbf{Z}_p[\![z', w]\!]/(z'w - 5).$$

Since $v(z) = v(z')$, we see that this is the annulus $\{z : 0 < v(z) < 1\}$. This argument gives the same result for $R^{14}_{\overline{r}}[\alpha_p], R^{18}_{\overline{r}}[\alpha_p], R^{22}_{\overline{r}}[\alpha_p]$.

When $k = 26$, by the presentation of $\widetilde{\mathbb{T}}(26, \{11\}, 6)$, we have $u_k(z, d) \equiv 1 \mod (p^6, (1 + d)^p - 1)$,

$$A_2(d) \equiv 11927d^4 + 12064d^3 + 12026d^2 + 12867d + 13065 \mod (p^6, (1 + d)^p - 1),$$

$$A_1(d) \equiv 25(334d^4 + 61d^3 + 549d^2 + d + 109) \mod (p^6, (1 + d)^p - 1)$$

and

$$A_0(d) \equiv 5^4(13d^4 + 16d^2 + 13d + 10) \mod (p^6, (1 + d)^p - 1).$$

By [Rozensztajn, 2020, Example 6.2.1], the power series $F_{26}(d, z)$ is reducible in $\mathbf{Z}_p[\![z, d]\!][1/p]$ and it factors into a linear factor and an irreducible quadratic factor. By Gauss' lemma, this factorization holds in $\mathbf{Z}_p[\![z, d]\!]$. Thus we have

$$F_{26}(z, d) = (z + B_0(d))(z^2 + C_1(d)z + C_0(d))$$

for some $B_0(d), C_1(d)$ and $C_0(d)$ in $\mathbf{Z}_p[\![d]\!]$ and the linear factor corresponds to the disk $\{z : v(z) > 2\}$ and the second factor corresponds to the annulus $\{z : 0 < v(z) < 2\}$. By coefficient comparison, we have

$$B_0(d) \equiv -25(317d^4 + 566d^3 + 251d^2 + 572d + 140) \mod (p^6, (1+d)^p - 1),$$

$$C_1(d) \equiv 4002d^4 + 13539d^3 + 5751d^2 + 14192d + 9565 \mod (p^6, (1+d)^p - 1)$$

and

$$C_0(d) \equiv 25(83d^4 + 32d^3 + 240d^2 + 106d + 384) \mod (p^6, (1+d)^p - 1).$$

(I found a unique root $-B_0(d)$ modulo 5 and then I lifted the root by Hensel's lemma.) We write

$$B_0(d) = b_0(d) + 5b_1(d) + 5^2 b_2(d) + \dots,$$

where $b_i(d) \in \mathbf{Z}_p[\![d]\!]$ and the nonzero coefficients in $b_i(d)$ are all in $\mathbf{Z}_p^\times$. If $b_0(d) \neq 0$, then it has lowest degree term of degree $n_0 \geq 5$. Choose a p-adic number $s \in \overline{\mathbf{Z}}_p$ such that $0 < v(s) \ll 1/n_0$. Then

$$v(B_0(s)) = v(b_0(s)) = n_0 v(s) \ll 1,$$

which contradicts the fact that $v(B_0(d)) > 2$. Thus $b_0(d) = 1$. In the same way, we can show that $b_1(d) = 0$. Thus

$$B_0(d) = -25(140 + 572d + 251d^2 + 566d^3 + 317d^4 + \dots).$$

By a similar argument as in the case where $k = 10$, we conclude that $25|C_0(d)$. Now by a suitable change of variable, we have

$$R_{\overline{r}}^{26}[\alpha_p] \xrightarrow{\sim} \mathbf{Z}_p[\![z', d']\!]/((z' - 25d')(z'^2 + (u_1(d')d' + c_0)z' + 25u_0(d'))),$$

where $v(z) = v(z')$, $u_i(d') \in \mathbf{Z}_p[\![d']\!]$ is a unit for $i = 0, 1$ and c_0 is a constant in $p\mathbf{Z}_p$.

When $k = 30$, by the presentation of $\widetilde{\mathbb{T}}(30, \{11\}, 9)$, we have $u_k(z, d) \equiv 1 \mod (p^9, (1+$

$d)^p - 1)$,

$$A_2(d) \equiv 1420662d^4 + 198114d^3 + 330661d^2 + 887347d + 1342055 \mod (p^9, (1+d)^p - 1),$$

$$A_1(d) \equiv 5(927714d^4 + 1024406d^3 + 1742774d^2 + 808961d + 805239) \mod (p^9, (1+d)^p - 1)$$

and

$$A_0(d) \equiv 3125(2518d^4 + 2590d^3 + 451d^2 + 2168d + 800) \mod (p^9, (1+d)^p - 1).$$

By a similar reasoning as in the case where $k = 26$, we have

$$F_{30}(d, z) = (z + B_0(d))(z^2 + C_1(d)z + C_0(d))$$

for some $B_0(d), C_1(d)$ and $C_0(d)$ in $\mathbf{Z}_p[\![d]\!]$ and the linear factor corresponds to the disk $\{z : v(z) > 4\}$ and the second factor corresponds to the annulus $\{z : 0 < v(z) < 1\}$. By comparing the coefficients, we have

$$B_0(d) \equiv -625(1818d^4 + 2506d^3 + 589d^2 + 48d + 925) \mod (p^9, (1+d)^p - 1),$$

$$C_1(d) \equiv 603787d^4 + 1764364d^3 + 698786d^2 + 917347d + 1920180 \mod (p^9, (1+d)^p - 1)$$

and

$$C_0(d) \equiv 5(344339d^4 + 368906d^3 + 122274d^2 + 348961d + 133364) \mod (p^9, (1+d)^p - 1).$$

By using a similar argument as in the case where $k = 26$, we can make a suitable change of variable so that

$$R_{\bar{r}}^{30}[\alpha_p] \xrightarrow{\sim} \mathbf{Z}_p[\![d', z']\!]/(z' - 625d')(z'^2 + (u_1(d')d' + c_0)z' + 5u_0(d'))$$

where $v(z) = v(z')$, $u_i(d') \in \mathbf{Z}_p[\![d']\!]$ is a unit for $i = 0, 1$ and c_0 is a constant in $p\mathbf{Z}_p$. $\square$

Proposition 1.4.2.5. *The proposition above gives examples to the following statements.*

1. *The number of irreducible components of* $\mathrm{Spec}(R_{\bar{r}}^{k} \otimes \mathbf{F})$ *and* $\mathrm{Spec}(R_{\bar{r}}^{k}[\alpha_p] \otimes \mathbf{F})$ *can be different.*

2. *The ring* $R_{\bar{r}}^{k}[\alpha_p]$ *need not be the normalization of* $R_{\bar{r}}^{k}$ *in* $R_{\bar{r}}^{k}[1/p]$.

Proof. For (1), we take the rings $R_{\bar{r}}^{10}$ and $R_{\bar{r}}^{10}[\alpha_p]$. By the geometric Breuil–Mézard conjecture, the space $\mathrm{Spec}(R_{\bar{r}}^{10} \otimes \mathbf{F}_p)$ has only one component which is isomorphic to that of $\mathrm{Spec}(R_{\bar{r}}^{2} \otimes \mathbf{F}_p) = \mathrm{Spec}(\mathbf{F}_p[\![d]\!])$. But it is straightforward from the presentation of $R_{\bar{r}}^{10}[\alpha_p]$ that $\mathrm{Spec}(R_{\bar{r}}^{10}[\alpha_p] \otimes \mathbf{F}_p)$ has two distinct irreducible components. The topology is illustrated in the following picture.

special-fiber.jpeg

For (2), we take the rings $R_{\bar{r}}^{26}$ and $R_{\bar{r}}^{26}[\alpha_p]$. The ring $R_{\bar{r}}^{26}[\alpha_p]$ is computed to be

$$\mathbf{Z}_5[[z, d]]/(z - 25d)(z^2 + (u_1(d)d + c_0)z + 25u_0(d)).$$

Let $\mathfrak{p}$ be image of the prime ideal $(5, z)$ modulo $(z - 25d)(z^2 + (u_1(d)d + c_0)z + 25u_0(d))$. Then

$$(R_{\bar{r}}^{26}[\alpha_p] \otimes \mathbf{F}_p)_{\mathfrak{p}} = \Big(\mathbf{F}_p[\![z, d]\!]/z^2(z + u_1(d)d + c_0)\Big)_{(z)} \xrightarrow{\sim} \Big(\mathbf{F}_p[\![z, d]\!]/z^2\Big)_{(z)}$$

is not regular local. Note also

$$(5,z)^2 + ((z-25d)(z^2 + (u_1(d)d + c_0)z + 25u_0(d))) = (25, 5z, z^2).$$

Thus $5 \in \mathfrak{p} \setminus \mathfrak{p}^2$. It now follows from the discussion after Proposition 1.3.4.5 that $R^{26}_{\overline{r}}[\alpha_p]_{\mathfrak{p}}$ is not regular and so $R^{26}_{\overline{r}}[\alpha_p]$ is not the normalization of $R^{26}_{\overline{r}}$ in its generic fiber. $\square$

Based on the data, we propose conjectures in §1.5.

1.4.3 Future examples

We list here the examples we would like to study in the future. In all these examples, the residual representation $\overline{r}$ is absolutely irreducible and $p = 3$ or 5. We will look for reducible $\overline{r}$ that are Schur in the future.

When $\overline{r}$ is absolutely irreducible, it suffices to consider $2 \leq k_0 \leq (p+3)/2$ because

$$\mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega_2^{k_0-1} = \omega^{k_0-2} \mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega_2^{p+2-k_0}$$

Example $p = 3$ and $k_0 = 2$

By (1.2.2.9), in order for the universal deformation problem of $\overline{r}$ to be unobstructed, the initial weight k_0 has to be 2.

Modular form f_0	20.2.e.a
Image $\mathrm{P}\overline{\rho}$	D_8
Field of $\mathrm{P}\overline{\rho}$	8.0.2916000000.2
TW1	Lemma 1.2.3.3
TW2	$\mathrm{Im}\,(\overline{\rho}\vert_{G_{\mathbf{Q}_2}}) \xrightarrow{\sim} \mathbf{Z}/2$ and $\mathrm{Im}\,(\overline{\rho}\vert_{G_{\mathbf{Q}_5}}) \xrightarrow{\sim} \mathbf{Z}/4$ are reducible
Taylor Wiles prime	$q = 19$
Localization Operators	$T_{29} - i$ and $U_{19} - i$
Sturm bound	$m = 144, k = 26$, and bound is 302
Generators of cotangent space	$T_{29} - i$ and $U_{19} - i$ and a diamond operator

Remark 1.4.3.1 (For the table above).

1. The form f_0 is CM, so the projective image is a dihedral subgroup of $\mathrm{PGL}_2(\mathbf{F}_5) \xrightarrow{\sim} S_5$. Since the order of the projective image of I_3 is cyclic of order $\frac{p+1}{\gcd(k_0-1,p+1)} = 4$ and D_8 is the only dihedral subgroup of S_5 whose order is divisible by 4, the projective image of $\overline{\rho}$ has to be D_8.

2. As a semisimple D_8 representation, $\mathrm{ad}^0\overline{\rho} = \chi_1 \oplus \chi^{\square}$ where χ_1 is the nontrivial character of D_8 that vanishes on $\mathbf{Z}/4 \trianglelefteq D_8$ and $\chi^{\square}$ is the unique two dimensional irreducible character of D_8. Note that the projective image of G_p is also D_8. We have

$$\mathrm{ad}^0\overline{\rho}\vert_{G_p} = \eta \oplus \mathrm{Ind}_{G_K}^{G_{\mathbf{Q}_p}} \omega_2^{p-1},$$

where K is the unique unramified quadratic extension of $\mathbf{Q}_p$ and

$$\eta : G_{\mathbf{Q}_p} \twoheadrightarrow \mathrm{Gal}(K/\mathbf{Q}_p) \xrightarrow{\sim} \{\pm 1\} \subseteq \mathbf{F}^{\times}$$

is the corresponding character. The induced representation is two dimensional irreducible and thus it is $\chi^{\square}$. The character η is trivial when restricted to $C_4 \leq D_8$ and so it is χ_1.

3. We need to check $Q = \{19\}$ satisfies $H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho}) = 0$. By the inflation-restriction sequence, this Selmer group is identified with

$$\mathrm{Hom}_{D_8}(G^{\mathrm{ab}}_{F,Q}/3, \mathrm{ad}^0\overline{\rho}),$$

where F is the number field cut out by the projective image of $\overline{\rho}$. By class field theory, the group $G^{\mathrm{ab}}_{F,\{19\}}/3$ is the Galois group of the maximal abelian 3-elementary extension of F that is unramified away from 19. Since 3 and 19 are coprime, such an extension is tamely ramified at 19 and unramified elsewhere; therefore, it has conductor 19 and the group $G^{\mathrm{ab}}_{F,\{19\}}/3$ can be identified with the 3-elementary part of the ray class group $\mathrm{RCl}(F, 19)/3$. In $\mathrm{RCl}(F, q)/3$ there is always one copy of $\mathbf{Z}/3$ that is a trivial representation of D_8 and it corresponds to the pro-3 part of the cyclotomic extension $\mathbf{Q}(\zeta_q)$ of $\mathbf{Q}$. The character χ_1 corresponds to pro-3 part of the anti-cyclotomic extension ramified at q. In order that there is not such an anti-cyclotomic extension, we want q to be inert in $F^{\mathbf{Z}/4} = \mathbf{Q}(i)$ by the class field theory of $\mathbf{Q}(i)$. Using Magma Bosma et al. [1997], we see that the ray class group $\mathrm{RCl}(F, 19^\infty)/3$ has dimension 2 and $q = 19$ is inert in $\mathbf{Q}(i)$. Thus $\mathrm{RCl}(F, 19^\infty)/3$ is isomorphic to $1 \oplus \chi_i$ for $i = 2$ or 3. Indeed, denote by χ_2 and χ_3 the other two nontrivial irreducible characters of D_8. They correspond to the non-cyclotomic pro-3 part of extensions of $F^{\chi_2} = \mathbf{Q}(\sqrt{15})$ and $F^{\chi_3} = \mathbf{Q}(\sqrt{-15})$, respectively, that are only ramified above q. By checking in Magma Bosma et al. [1997], we conclude that

$$\mathrm{RCl}(F, 19^\infty)/3 = 1 \oplus \chi_3.$$

Example $p = 5$ and $k_0 = 3$

There are two interesting examples but we only need to compute one. I am not sure which is easier at this point.

Modular form	12.3.c.a
Field of $\mathrm{P}\overline{\rho}$	6.0.270000.1
TW1	Lemma 1.2.3.3
TW2	$2, 3 \not\equiv -1 \mod 5$
Taylor–Wiles prime	$q = 11$
Localization primes	$T_7 - 2$ and $U_{11} + 1$ And $\langle 5 \rangle + 1$
Sturm bound	$m = 24, k = 51$, and bound is 102
Generators of cotangent space	$T_7 - 2, U_{11} + 1, \langle d \rangle - 1$ (T_5 if for the full Hecke algebra)

Remark 1.4.3.2 (For the table above).

1. The form f_0 is CM, so the projective image is a dihedral subgroup of $\mathrm{PGL}_2(\mathbf{F}_5) \xrightarrow{\sim} S_5$. Since the order of the projective image of I_5 is cyclic of order $\frac{p+1}{\gcd(k_0-1,p+1)} = 3$ and S_3 is the only dihedral subgroup of S_5 whose order is divisible by 3, the projective image of $\overline{\rho}$ has to be S_3.

2. The representation $\mathrm{ad}^0\overline{\rho}$ is sgn $\oplus\, \chi^{\Delta}$ as an S_3-representation, where sgn is the sign character of S_3 and χ^{Δ} is the two-dimensional irreducible character of S_3. Since the residual representation $\overline{\rho}$ is exceptional, every element in the image is semi-simple. Let $\overline{\rho}(g)$ be a matrix in the image. Suppose that $\overline{\rho}(g)$ has eigenvalues α and β. Then $\mathrm{ad}^0\overline{\rho}(g)$ is also semisimple and has eigenvalues $1, \alpha^{-1}\beta$ and $\beta^{-1}\alpha$. Thus

$$\mathrm{Tr}(\mathrm{ad}^0\overline{\rho}(g)) = 1 + \alpha^{-1}\beta + \beta^{-1}\alpha.$$

   Since $\mathrm{P}\overline{\rho}(g)$ has order $1, 2$ or 3, the eigenvalue $\alpha^{-1}\beta = \pm 1$ or ζ_3. Hence, the trace of identity is 3, the trace of a two-cycle is -1 and trace of a 3-cycle is 0. From this calculation and the character table of S_3, we conclude that $\mathrm{ad}^0\overline{\rho} = \mathrm{sgn} \oplus \chi^{\Delta}$.

3. To find the Taylor–Wiles prime, as in the example 20.2.e.a, we use

$$\mathrm{Hom}_{S_3}(\mathrm{RCl}(F,q)/5, \mathrm{sgn} \oplus \chi^{\Delta})$$

to control $H^1_{\Sigma_Q}(G_{\mathbf{Q}}, \mathrm{ad}^0\overline{\rho})$. There is always a trivial sub-representation of $\mathrm{RCl}(F,q)/5$ that comes from the pro-5 part of $\mathbf{Q}(\zeta_q)/\mathbf{Q}$. The character sgn corresponds to pro-5 part of the anti-cyclotomic extension ramified at q. In order that there is not such an anti-cyclotomic extension, we want q to be inert in F^{sgn}, which is the quadratic imaginary field that f_0 has CM by. Using Magma Bosma et al. [1997], we can directly check that $\mathrm{RCl}(F,11)/5 = 1$ and 11 is a Taylor–Wiles prime.

Example $p = 5$ and $k_0 = 4$

Modular form f_0	One embedding of 13.4.c.b
Image $\mathrm{P}\overline{\rho}$	A_4
Field of $\mathrm{P}\overline{\rho}$	12.0.12745792515625.1
TW1	$\mathrm{P}\overline{\rho}\vert_{G_{\mathbf{Q}(\zeta_5)}}$ has image A_4
TW2	Lemma 1.2.3.4
Taylor Wiles prime	$q = 11$
Localization Operators	$T_2 - (3 + 2\zeta_3)$, $U_{11} + \zeta_3$
Sturm bound	$m = 14, k = 52$, and bound is 59
Generators of cotangent space	$T_2 - (3 + 2\zeta_3)$, $U_{11} + \zeta_3$ and $\langle 79 \rangle - 1$

Remark 1.4.3.3 (For the table above).

1. For those left blank, I have not worked out but I will work out after application.

2. The modular form 13.4.c.b has coefficients in $\mathbf{Q}[\sqrt{-3}, \sqrt{17}]$. There are 4 eigenforms that are conjugate to each other over $\mathbf{Q}$. Let's say they are f_1, f_2, f_3 and f_4. Over $\mathbf{Q}_5$, the Galois orbit over $\mathbf{Q}$ splits into two over $\mathbf{Q}_5$: f_1 and f_2 are conjugate and f_3 and f_4 are conjugate. By checking the a_2-coefficient, we see that they are not congruent to each other nor the two forms labeled 13.4.c.a. Without loss of generality, we pick $f_0 = f_1$. We have $a_2(f_3)$ is a root of $x^2 + x + 2$ in characteristic 5.

3. We verify TW1 by the following reasoning. Since $\overline{r}$ is absolutely irreducible, the global representation $\overline{\rho}$ is, as well. The image of $\mathrm{P}\overline{\rho}$ either contains $\mathrm{PSL}_2(\mathbf{F}_5)$ or is exceptional. If it contains $\mathrm{PSL}_2(\mathbf{F}_5)$, then we are done. So we assume that $\mathrm{Im}\,\mathrm{P}\overline{\rho}$ is exceptional, i.e. dihedral, A_4 or S_4. (In this case, A_5 is not an exceptional image because $p = 5$.) The group $\mathrm{P}\overline{\rho}(G_{\mathbf{Q}(\zeta_5)})$ contains the derived subgroup of $\mathrm{P}\overline{\rho}(G_{\mathbf{Q}})$ and it has index divisible by 4 inside $\mathrm{P}\overline{\rho}(G_{\mathbf{Q}})$. If $\mathrm{P}\overline{\rho}(G_{\mathbf{Q}}) \xrightarrow{\sim} A_4$, then $\mathrm{P}\overline{\rho}(G_{\mathbf{Q}(\zeta_5)})$ is a subgroup that contains V_4 and has index divisible by 4, which forces $\mathrm{P}\overline{\rho}(G_{\mathbf{Q}(\zeta_5)}) = A_4$. Hence, TW1 holds in this case. The same reasoning works for the case $\mathrm{P}\overline{\rho}(G_{\mathbf{Q}}) \xrightarrow{\sim} S_4$. Therefore, the only possible situation that $\overline{\rho}|_{G_{\mathbf{Q}(\zeta_5)}}$ is reducible is when $\mathrm{Im}\,\mathrm{P}\overline{\rho}$ is dihedral D_{2r} of order $2r$. Let $\ell \neq 5, 13$ be a prime number. Suppose that $\overline{\rho}(\mathrm{Frob}_\ell)$ has eigenvalues λ_1 and λ_2. Since we assume $\overline{\rho}$ has exceptional image, $\overline{\rho}(\mathrm{Frob}_\ell)$ is semisimple and thus $\mathrm{P}\overline{\rho}(\mathrm{Frob}_\ell)$ is the ratio $\lambda_1\lambda_2^{-1}$. By calculating the ratios of the eigenvalues of Frobenius elements (up to primes $\ell \leq 2000$), which are roots of

$$x^2 - \left(\frac{a_\ell(f_0)^2}{\chi(\ell)\ell^3} - 2\right)x + 1 = 0,$$

we see that the orders of the ratios are 1 or 2 or 3. So the dihedral group must be S_3 assuming that 2000 is enough for Chebotarev's density theorem. However, since the projective image of $G_{\mathbf{Q}_5}$ is D_4, this is not possible. In conclusion, the TW1 condition is satisfied.

4. On the other hand, our computations strongly suggest that if $\overline{\rho}$ is exceptional, the projective image of $\overline{\rho}$ is A_4. Looking up in LMFDB LMFDB Collaboration [2022], there is a unique number field 12.0.12745792515625.1 whose Galois group is A_4 and is tamely ramified at 5 and 13. By Serre [1986], the projective Galois representation whose image is A_4 can be lifted to an actual Galois representation without introducing more ramification, and by Serre's conjecture should come from a modular form f of level 13. Since the image of $G_{\mathbf{Q}_p}$ is $V_4 \leq A_4$, this implies the local representation at 5 is induced and thus $a_5(f) = 0$. Furthermore, the weight k of f is such that $\omega_2^{(p-1)(k-1)}$ has order 2 because $I_{\mathbf{Q}_p}$ has image $\mathbf{Z}/2 \leq V_4$. This together with the Fontaine–Laffaille bound on k forces $k = 4$. The image of $G_{\mathbf{Q}_{13}}$ is $\mathbf{Z}/3$ and 13 is totally ramified. Thus the Nebentypus character of f has order divisible by 3. With all these conditions combined, we deduce that this f is one embedding of 13.4.c.b. The question is whether it is coming from the Galois orbit of f_1 or f_3. These two forms have the same Nebentypus character (after choosing an embedding of $\zeta_3 \in \overline{\mathbf{Q}}_5$.) By checking their Fourier coefficients at prime number $\ell \leq 2000$, we conclude that f_1 and f_3 differ by a twist of the Legendre symbol $(\cdot/5) = \omega^2$ in characteristic p. Thus they give rise to the same projective image which has to be A_4.

5. Using a similar argument as in the example 12.3.c.a, we conclude that $\mathrm{ad}^0\overline{\rho} = \chi^{\mathrm{Tetra}}$, where χ^{Tetra} is the three dimensional irreducible representation of A_4.

6. The prime $q = 11$ is a Taylor–Wiles prime. The element $\overline{\rho}(\mathrm{Frob}_{11})$ has characteristic polynomial
$$x^2 + (\zeta_3 + 1)x + \zeta_3,$$
which has distinct roots 1 and ζ_3. Since $\overline{\rho}$ has exceptional image, using the inflation–

restriction sequence, we need to verify that

$$\mathrm{Hom}_{A_4}(\mathrm{RCl}(F, 11)/5, \mathrm{ad}^0\overline{\rho}) = 0.$$

Using Magma Bosma et al. [1997], we directly compute that $\mathrm{RCl}(F, 11)/5$ is one-dimensional. This is the trivial representation of A_4, which corresponds to the pro-5 part of the cyclotomic extension $\mathbf{Q}(\zeta_{11})/\mathbf{Q}$. Hence the Selmer group vanishes and $q = 11$ is indeed a Taylor–Wiles prime.

1.5 Conjectures

We formulate conjectures when $k_0 = 2$, based on the data we have collected from §1.4.2.

Let $Sh_k(x)$ be the shift function that is a formal power series in the variable x:

$$Sh_k(x) := x^{\mu(k)} \sum_{i=0}^{\infty} x^i = x^{\mu(k)}(1 - x)^{-1}$$

where the function $\mu(k)$ depends on the p-adic expansion of k as follows. The weight k can be uniquely written in the form $k = 2 + a(p-1) + b(p^2 - 1)$ where a and b are non-negative integers with $0 \leq a \leq p$. Let $b = \sum_{i=0}^{\infty} b_i p^i$ be the p-adic expansion of b with $0 \leq b_i \leq p - 1$. We define the p-adic function $\psi(b)$ in b to be

$$\psi(b) := \sum_{i=0}^{\infty} b_{2i} p^i + 2 \sum_{i=0}^{\infty} b_{2i+1} p^i,$$

and we let $\mu(k)$ be the quantity

$$\mu(k) = \begin{cases} \psi(b) & a = 0 \\ 1 + \psi(b) & a = 2 \\ +\infty & \text{otherwise} \end{cases}.$$

When $\mu(k) = +\infty$, the series $Sh_k(x)$ is understood to be 0.

Conjecture 1.5.0.1. *If* $\overline{r}|_{I_p} \sim \begin{pmatrix} \omega_2 & 0 \\ 0 & \omega_2^p \end{pmatrix}$, *then the Hilbert series of* $R^k \otimes \mathbf{F}$ *is*

$$H_k(x) = \sum_{\substack{2 \leq i \leq k \\ p-1 | i-2}} Sh_i(x).$$

Remark 1.5.0.2. Based on Fact 1.4.2.2(1), we assume that the associated graded algebra $Gr(R^k_{\overline{r}} \otimes \mathbf{F})$ of $R^k_{\overline{r}} \otimes \mathbf{F}$ is finite free over $\mathbf{F}[\![d]\!]$. Using the following proposition, it then suffices to conjecture the Hilbert series of $R^k_{\overline{r}} \otimes \mathbf{F}/(d)$. The Artinian algebra is isomorphic to $\mathbb{T}(k, \varnothing) \otimes \mathbf{F}$ by Remark 1.2.3.14.

Proposition 1.5.0.3. *Let* R *be a graded algebra and* $a \in R$ *a homogeneous element of degree* d *which is not a zero divisor. Then*

$$H_R(x) = \frac{H_{R/a}(x)}{1 - x^d},$$

where $H_R(x)$ *and* $H_{R/a}(x)$ *are the Hilbert series of* R *and* R/a, *respectively.*

Corollary 1.5.0.4 (Bao [2023b])**.** *Assume that Conjecture 1.5.0.1 is true. Then the following holds.*

1. *The sequence* $\{H_k(x)\}_{k=2+n(p-1)}$ *is an increasing sequence in* k, *i.e.*

$$H_k(x) \geq H_{k-(p-1)}(x).$$

2. *The limit of* $H_k(x)$ *as* k *goes to* ∞ *is the Hilbert–Samuel function of* $R_{\overline{r}}^{\mathrm{univ}} \otimes \mathbf{F}_p \xrightarrow{\sim} \mathbf{F}_p[\![x_1, x_2, x_3]\!]$, *i.e.*

$$\lim_{\substack{k\to\infty \\ p-1|k-2}} H_k(x) = \frac{1}{(1-x)^3} = \sum_{i=0}^{\infty} \binom{i+2}{2} x^i.$$

3. *The effectiveness of the limit: Let* n *be a positive number with its unique* p*-adic expansion* $\sum_{i=0}^{\infty}(a_i + 2b_i)p^i$ *such that* $0 \leq a_i + 2b_i < p$ *with* $a_i \in \{0, 1\}$ *and* b_i *a non-negative integer. Set* k *to be the integer*

$$k := 2 + (p^2 - 1)(\sum_{i=0}^{\infty} a_i p^{2i} + \sum_{i=0}^{\infty} b_i p^{2i+1}).$$

Then k *is the smallest integer such that the* n*-th coefficient of* $H_k(x)$ *is equal to* $\binom{n+2}{2}$.

Proof.

1. This follows from directly from the conjectural form of $H_k(x)$.

2. Note that

$$\lim_{\substack{k\to\infty \\ p-1|k-2}} HS(k) = \sum_{\substack{i\geq 2 \\ p-1|i-2}} Sh(i) = (1-T)^{-1} \sum_{\substack{i\geq 2 \\ p-1|i-2}} T^{\mu(i)}.$$

To prove (1), it suffices to show

$$\sum_{\substack{i\geq 2 \\ p-1|i-2}} T^{\mu(i)} = \frac{1}{(1-T)^2} = \sum_{j\geq 0} (j+1)T^j,$$

which is equivalent to

$$\#\{i : \mu(i) = j, i \geq 2, p-1|i-2\} = j+1.$$

By definition of $\mu(i)$, we see that the above is equivalent to

$$\#\{b \in \mathbf{Z} : \psi(b) = j \text{ or } j-1, b \geq 0\} = j+1,$$

Now if we set $A = \sum_{i\geq 0} b_{2i}p^i, B = \sum_{i \geq 0} b_{2i+1}p^i$, then by definition of ψ, we have

$$\#\{b \in \mathbf{Z} : \psi(b) = j, b \geq 0\} = \#\{(A,B) \in \mathbf{Z} \times \mathbf{Z} : A + 2B = j, A, B \geq 0\} = \lfloor j/2 \rfloor + 1.$$

Thus

$$\begin{aligned} \#\{b \in \mathbf{Z} : \psi(b) = j, b \geq 0\} + \#\{b \in \mathbf{Z} : \psi(b) = j-1, b \geq 0\} \\ = \lfloor j/2 \rfloor + 1 + \lfloor (j-1)/2 \rfloor + 1 = j - 1 + 2 = j+1. \end{aligned}$$

3. We have

$$\mu(k) = \psi\left(\sum_{i=0}^{\infty} a_i p^{2i} + \sum_{i=0}^{\infty} b_i p^{2i+1}\right) = \sum_{i=0}^{\infty}(a_i + 2b_i)p^i = m.$$

For $k' > k$, we will show that $\mu(k') > \mu(k)$. We first let

$$k' = 2 + (p^2-1)(\sum_{i=0}^{\infty} a_i' p^{2i} + \sum_{i=0}^{\infty} b_i' p^{2i+1}) = 2 + (p^2-1)(\sum_{i=0}^{\infty}(a_i' + b_i' p)p^{2i})$$

for integers $0 \leq a_i' < p$ and $0 \leq b_i' < p$. Since k and k' are positive integers, the p-adic expansions above all have finitely many terms. Since $k' > k$, there exists a biggest integer i_0 such that $a_{i_0}' + b_{i_0}' p > a_{i_0} + b_{i_0} p$. Then either $b_{i_0}' > b_{i_0}$ or $b_{i_0}' = b_{i_0}$ and

$a'_{i_0} > a_{i_0}$. Now we have

$$\begin{aligned}\mu(k') - \mu(k) &= \psi\left(\sum_{i=0}^{\infty} a'_i p^{2i} + \sum_{i=0}^{\infty} b'_i p^{2i+1}\right) - \psi\left(\sum_{i=0}^{\infty} a_i p^{2i} + \sum_{i=0}^{\infty} b_i p^{2i+1}\right) \\ &= \sum_{i=0}^{i_0}(a'_i + 2b'_i)p^i - \sum_{i=0}^{i_0}(a_i + 2b_i)p^i \\ &= (a'_{i_0} + 2b'_{i_0} - a_{i_0} - 2b_{i_0})p^{i_0} + \sum_{i=0}^{i_0-1}(a'_i + 2b'_i - a_i - 2b_i)p^i.\end{aligned}$$

Since $0 \leq a_i \leq 1$ and $0 \leq a_i + 2b_i < p$, we have

$$a'_{i_0} + 2b'_{i_0} - a_{i_0} - 2b_{i_0} \geq 1$$

and

$$a'_i + 2b'_i - a_i - 2b_i \geq -(p-1).$$

Thus

$$\mu(k') - \mu(k) \geq p^{i_0} - (p-1)\sum_{i=0}^{i_0-1} p^i = p^{i_0} + (1-p)\frac{1-p^{i_0}}{1-p} = 1.$$

In the case when $k' \equiv 2p \mod p^2 - 1$, by the proposition below, we have $\mu(k') \geq \mu(k' + p^2 - 2p - 1)$. Thus $HS_k(x)$ is the smallest integer whose m-th coefficient that is the largest among all weights. But since the limit of $HS_k(x)$ is $(1-x)^{-3}$, the m-th coefficient is equal to $\binom{m+2}{2}$.

□

Proposition 1.5.0.5. *If* $k \equiv 2p \mod (p^2 - 1)$, *then* $\mu(k) \geq \mu(k + p^2 - 1 - 2p)$.

Proof. We have

$$k = 2 + 2(p-1) + b(p^2 - 1)$$

for some positive integer b. Then

$$k + p^2 - 1 - 2p = 2 + (b+1)(p^2 - 1).$$

Suppose that

$$b = (p-1)\sum_{i=0}^{n_0-1} p^i + \sum_{i=n_0}^{N} b_i p^i$$

for some integer N and $0 \leq b_i \leq p-2$. Then $b+1$ has p-adic expansion

$$b + 1 = (b_{n_0} + 1)p^{n_0} + \sum_{i=n_0+1}^{N} b_i p^i.$$

If n_0 is odd, then

$$\begin{aligned} 1 + \psi(b) - \psi(b+1) &= 1 + (p-1)\sum_{i=0}^{(n_0-1)/2} p^i + 2(p-1)\sum_{i=0}^{(n_0-3)/2} p^i - p^{(n_0-1)/2} \\ &= 1 + 3(p-1)\sum_{i=0}^{(n_0-3)/2} p^i \geq 1. \end{aligned}$$

If n_0 is even, then

$$\begin{aligned} 1 + \psi(b) - \psi(b+1) &= 1 + 3(p-1)\sum_{i=0}^{(n_0-2)/2} p^i - p^{n_0/2} \\ &= 1 + 3(p^{n_0/2} - 1) - p^{n_0/2} = 2(p^{n_0/2} - 1) \geq 0. \end{aligned}$$

□

Based on Fact 1.4.2.2(1), we also make the following conjecture.

Conjecture 1.5.0.6. *When $k_0 = 2$, the ring R^k is Gorenstein if and only if*

$$k = k_1 + (p^2 - 1)\left(ap^N - 1\right)$$

for some integers $2p \leq k_1 \leq p^2 - p + 2$ such that $k_1 \equiv k_0 \mod p-1$, $N \geq 0$ and $1 \leq a \leq p$ with the exception that $k = 2$ and $k = p+1$, in which case $R^k_{\bar{r}}$ is formally smooth over $\mathcal{O}$.

1.6 Future plan

The following are things we are working on now and want to explore in the future.

1.6.1 Horizontal Breuil–Mézard conjecture

We are currently computing the $k_0 = 3$ example in Python. We plan to compute all other examples from §1.4.3 to validate and explore variations of conjectures 1.5.0.1 and 1.5.0.6 in different cases. We will also look for examples where $\bar{r}$ is reducible and Schur and carry out the computations.

We are eventually interested in interpreting the conjectural form of $H_k(x)$ on the automorphic side. We hope to find the corresponding invariant from the representation theory of $\mathrm{GL}_2(\mathbf{Q}_p)$.

1.6.2 Components of the crystalline deformation rings

Since we are able to compute the matrices of the T_p operator acting on $M(k, Q)$ up to some p-adic precision, we have access to analyzing the a_p values of the crystalline representations that come from modular forms on the crystalline deformation rings. Combined with Rozensztajn's work Rozensztajn [2020], we can analyze the distribution of the modular points on different components of the crystalline deformation rings. There are many open questions on these components. How many components are there? Are modular points evenly distributed on the components? Are there corresponding automorphic invariant that can be linked to the number of components of $R^k_{\bar{r}}$?

1.6.3 The cokernel C^k

We wonder if $\hat{M}$ is finite free over the Iwasawa algebra as M is from Lemma 1.3.4.7. The freeness of M comes from geometry while $\hat{M}$ is something less straightforward to understand. This is related to understanding how divisible a_p is by p. One idea is to check out Conrad [2007]. But this is all very vague.

REFERENCES

Bodan Arsovski. Reduction modulo p of two-dimensional crystalline representations of $G_{\mathbf{Q}_p}$ of slope less than three. *arXiv preprint arXiv:1503.08309*, 2015.

Bodan Arsovski. Limiting measures of supersingularities, 2021.

Avner Ash and Glenn Stevens. Cohomology of arithmetic groups and congruences between systems of hecke eigenvalues. *Journal für die reine und angewandte Mathematik*, 365: 192–220, 1986a.

Avner Ash and Glenn Stevens. Modular forms in characteristic ℓ and special values of their L-functions. *Duke Mathematical Journal*, 53(3):849–868, 1986b.

Michael F Atiyah. On the krull-schmidt theorem with application to sheaves. *Bulletin de la Société mathématique de France*, 84:307–317, 1956.

Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*. Westview Press, 2016. ISBN 978-0-8133-5018-9.

Chengyang Bao. Locally induced Galois representations with exceptional residual images. *arXiv preprint arXiv:2205.11562*, 2022.

Chengyang Bao. Patching functors for coherent cohomology and applications. in progress, 2023a.

Chengyang Bao. Computing crystalline deformation rings via the Taylor–Wiles–Kisin patching method. in progress, 2023b.

John Bergdall and Brandon Levin. Reductions of some two-dimensional crystalline representations via kisin modules. *International Mathematics Research Notices*, 2022(4):3170–3197, 2022.

Laurent Berger and Christophe Breuil. Sur la réduction des représentations cristallines de dimension 2 en poids moyens, 2005. URL `https://arxiv.org/abs/math/0504388`.

Laurent Berger, Hanfeng Li, and Hui Zhu. Construction of some families of 2-dimensional crystalline representations. *Mathematische Annalen*, 329, 11 2003. doi:10.1007/s00208-004-0529-y.

Shalini Bhattacharya and Eknath Ghate. Reductions of Galois representations for slopes in $(1, 2)$. *Documenta Mathematica*, 20:943–987, 2015.

Shalini Bhattacharya, Eknath Ghate, and Sandra Rozensztajn. Reductions of Galois representations of slope 1. *Journal of Algebra*, 508:98–156, 2018.

Gebhard Böckle. Deformations of galois representations. In *Elliptic curves, Hilbert modular forms and Galois deformations*, pages 21–115. Springer, 2013.

Armand Borel and Jean-Pierre Serre. Corners and arithmetic groups. *Comment. Math. Helv*, 48(1):436–491, 1973.

Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ISSN 0747-7171. doi:10.1006/jsco.1996.0125. URL `http://dx.doi.org/10.1006/jsco.1996.0125`. Computational algebra and number theory (London, 1993).

Raoul Bott, Loring W Tu, et al. *Differential forms in algebraic topology*, volume 82. Springer, 1982.

Christophe Breuil. *Compositio Mathematica*, 138:165–188, 09 2003a. doi:10.1023/a:1026191928449.

Christophe Breuil. Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbf{Q}_p)$: I. *Compositio Mathematica*, 138(2):165–188, 2003b. doi:10.1023/A:1026191928449.

Christophe Breuil. Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbf{Q}_p)$. II. *Journal of the Institute of Mathematics of Jussieu*, 2(1):23–58, 2003c. doi:10.1017/S1474748003000021.

Christophe Breuil. Representations of galois and of GL_2 in characteristic p. *Course at Columbia University*, 2007.

Christophe Breuil. Introduction générale. In Berger Laurent, Breuil Christophe, and Colmez Pierre, editors, *Représentations p-adiques de groupes p-adiques I : représentations galoisiennes et* (φ, Γ)*-modules*, number 319 in Astérisque. Société mathématique de France, 2008. URL `http://www.numdam.org/item/AST_2008__319__1_0/`.

Christophe Breuil and Ariane Mézard. Multiplicités modulaires et représentations de $\mathrm{GL}_2(\mathbf{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ en $\ell = p$. Appendice par Guy Henniart. Sur l'unicité des types pour GL_2. *Duke Mathematical Journal*, 115:205–310, 2002.

Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

Armand Brumer. On the units of algebraic number fields. *Mathematika*, 14(2):121–124, 1967.

Kevin Buzzard. Some notes on principal series representations. URL `https://www.ma.imperial.ac.uk/~buzzard/maths/research/notes/notes_on_classical_principal_series_for_glnqp.pdf`.

Kevin Buzzard. Questions about slopes of modular forms. In Tilouine Jacques, Carayol Henri, Harris Michael, and Vignéras Marie-France, editors, *Formes automorphes (I) - Actes du semestre du centre Émile Borel, printemps 2000*, number 298 in Astérisque.

Société mathématique de France, 2005. URL http://www.numdam.org/item/AST_2005__298__1_0/.

Kevin Buzzard and Toby Gee. Explicit reduction modulo p of certain two-dimensional crystalline representations. *International Mathematics Research Notices*, 2009(12):2303–2317, 2009.

Kevin Buzzard and Toby Gee. Explicit reduction modulo p of certain 2-dimensional crystalline representations, ii. *Bulletin of the London Mathematical Society*, 45(4):779–788, 2013.

Kevin Buzzard, Fred Diamond, and Frazer Jarvis. On serre's conjecture for mod ℓ galois representations over totally real fields. *Duke Mathematical Journal*, 155(1):105–161, 2010.

Frank Calegari and Naser Talebizadeh Sardari. Vanishing Fourier coefficients of Hecke eigenforms. *Mathematische Annalen*, 2021. URL https://doi.org/10.1007/s00208-021-02178-7.

Ana Caraiani and Peter Scholze. On the generic part of the cohomology of non-compact unitary shimura varieties, 2023.

Ana Caraiani and Sug Woo Shin. Recent progress on langlands reciprocity for GL_n: Shimura varieties and beyond, 2023.

Ana Caraiani, Matthew Emerton, Toby Gee, David Geraghty, Vytautas Paškūnas, and Sug Woo Shin. Patching and the p-adic Langlands program for $\mathrm{GL}_2(\mathbb{Q}_p)$. *Compositio Mathematica*, 154(3):503–548, 2018. doi:10.1112/S0010437X17007606.

Henri Carayol. Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. volume 165 of *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture*. Contemporary Mathematics, 1994. doi:https://doi.org/10.1090/conm/165. URL https://api.semanticscholar.org/CorpusID:117513171.

J. W. S. Cassels. *Global Fields.* Algebraic number theory(J. W. S. Cassels and A. Fröhlich, eds). Academic Press Inc., 1967.

Pierre Colmez. Représentations triangulines de dimension 2. *Astérisque*, 319(213-258):83, 2008.

Pierre Colmez. La série principale unitaire de $\mathrm{GL}_2(\mathbf{Q}_p)$. *Astérisque*, 330:213–262, 2010.

Brian Conrad. Arithmetic moduli of generalized elliptic curves. *Journal of the Institute of Mathematics of Jussieu*, 6(2):209–278, 2007.

Brian Conrad. Lifting global representations with local properties. *preprint*, 64, 2011.

KEITH Conrad. Dihedral groups ii. *Internet Online Book*, pages 3–6, 2009.

Charles W Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*, volume 356. American Mathematical Soc., 1966.

Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. *Current developments in mathematics*, 1995(1):1–154, 1995.

Pierre Deligne. Formes modulaires et representations e-adiques. In *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*, pages 139–172. Springer, 1969.

Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. In *Annales scientifiques de l'École Normale Supérieure*, volume 7, pages 507–530, 1974.

Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem, Providence, RI*, pages 39–133, 1995.

Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

Mark Dickinson. On the modularity of certain 2-adic Galois representations. *Duke Mathematical Journal*, 109(2):319 – 382, 2001. doi:10.1215/S0012-7094-01-10923-X. URL `https://doi.org/10.1215/S0012-7094-01-10923-X`.

Bas Edixhoven. The weight in serre's conjectures on modular forms. *Inventiones mathematicae*, 109(1):563–594, 1992.

Bas Edixhoven and Chandrashekhar Khare. Hasse invariant and group cohomology. *arXiv preprint math/0210401*, 2002.

David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

Matthew Emerton. p-adic families of modular forms [after hida, coleman, and mazur]. 2009.

Matthew Emerton. Local-global compatibility in the p-adic langlands programme for $\mathrm{gl}_2(\mathbf{Q})$. *preprint*, 3:4, 2011.

Matthew Emerton and Toby Gee. A geometric perspective on the Breuil-Mézard conjecture. *Journal of the Institute of Mathematics of Jussieu*, 13(1):183–223, 2014. doi:10.1017/S147474801300011X.

Jean-Marc Fontaine and Guy Laffaille. Construction de représentations p-adiques. In *Annales scientifiques de l'École Normale Supérieure*, volume 15, pages 547–608, 1982.

Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I*, pages 41–78, 1995.

William Fulton and Joe Harris. *Representation theory: a first course*, volume 129. Springer Science & Business Media, 2013.

Toby Gee. Modularity lifting theorems–notes for arizona winter school. 2013.

Toby Gee and Mark Kisin. The breuil–mézard conjecture for potentially barsotti–tate representations. In *Forum of Mathematics, Pi*, volume 2, page e1. Cambridge University Press, 2014.

Stephen S Gelbart. *Automorphic forms on adele groups*. Number 83. Princeton University Press, 1975.

Eknath Ghate and Vivek Rai. Reductions of galois representations of slope 3/2. *arXiv preprint arXiv:1901.01728*, 2019.

Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165. Cambridge University Press, 2017.

Fernando Q Gouvêa et al. Deformations of galois representations. *Arithmetic algebraic geometry (Park City, UT, 1999)*, 9:233–406, 2001.

Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Mathematical Journal*, 61(2):445 – 517, 1990. doi:10.1215/S0012-7094-90-06119-8. URL https://doi.org/10.1215/S0012-7094-90-06119-8.

K. Gruenberg. *Profinite groups.* Algebraic number theory(J. W. S. Cassels and A. Fröhlich, eds). Academic Press Inc., 1967.

Klaus Haberland. Perioden von modulformen einer variabler und gruppencohomologie, III. *Mathematische Nachrichten*, 112(1):297–315, 1983.

Kazuyuki Hatada. Eigenvalues of hecke operators on $\mathrm{SL}(2,\mathbf{Z})$. *Mathematische Annalen*, 239: 75–96, 1979. URL https://doi.org/10.1007/BF01420494.

Guy Henniart. Sur l'unicité des types pour GL_2. *Duke Math. J*, 155(2):205–310, 2002.

Taira Honda. Isogeny classes of abelian varieties over finite fields. *Journal of the Mathematical Society of Japan*, 20(1-2):83–95, 1968.

Yong Hu and Fucheng Tan. The Breuil-Mézard conjecture for non-scalar split residual representations. *To appear in Ann. Scient. de l'E.N.S*, 2013. URL https://api.semanticscholar.org/CorpusID:55643816.

Yongquan Hu and Vytautas Paškūnas. On crystabelline deformation rings of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$(with an appendix by Jack Shotton). *Mathematische Annalen*, 373:421–487, 2019.

Loo-keng Hua et al. On the least solution of pell's equation. *Bulletin of the American Mathematical Society*, 48(10):731–735, 1942.

Daniel Huybrechts. *Lectures on K3 Surfaces*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2016. doi:10.1017/CBO9781316594193.

Naomi Jochnowitz. Congruences between systems of eigenvalues of modular forms. *Transactions of the American Mathematical Society*, 270(1):269–285, 1982a. ISSN 00029947. URL http://www.jstor.org/stable/1999772.

Naomi Jochnowitz. A study of the local components of the hecke algebra mod ℓ. *Transactions of the American Mathematical Society*, 270(1):253–267, 1982b.

John W. Jones and David P. Roberts. A database of number fields. *LMS Journal of Computation and Mathematics*, 17(1):595–618, 2014. doi:10.1112/S1461157014000424.

Nicholas M Katz. P-adic properties of modular schemes and modular forms. In *Modular functions of one variable III*, pages 69–190. Springer, 1973.

Nicholas M Katz. A result on modular forms in characteristic p. In *Modular functions of one variable V*, pages 53–61. Springer, 1977.

Nicholas M Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*. Number 108. Princeton University Press, 1985.

Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (i). *Inventiones mathematicae*, 178(3):485–504, 2009a.

Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (ii). *Inventiones mathematicae*, 178(3):505–586, 2009b.

Ian Kiming and Helena A. Verrill. On modular mod ℓ galois representations with exceptional images. *Journal of Number Theory*, 110(2):236–266, 2005. ISSN 0022-314X. doi:https://doi.org/10.1016/j.jnt.2004.05.003. URL https://www.sciencedirect.com/science/article/pii/S0022314X04000952.

Mark Kisin. Modularity for some geometric galois representations-with an appendix by ofer gabber. *L-functions and Galois representations*, pages 438–470, 2007.

Mark Kisin. Potentially semi-stable deformation rings. *Journal of the American Mathematical Society*, 21(2):513–546, 2008. ISSN 08940347, 10886834. URL http://www.jstor.org/stable/20161376.

Mark Kisin. The Fontaine-Mazur conjecture for GL_2. *Journal of the American Mathematical Society*, 22(3):641–690, 2009a. ISSN 08940347, 10886834. URL http://www.jstor.org/stable/40587246.

Mark Kisin. Moduli of finite flat group schemes, and modularity. *Annals of Mathematics*, pages 1085–1180, 2009b.

Mark Kisin. Deformations of $G_{\mathbf{Q}_p}$ and $\mathrm{GL}_2(\mathbf{Q}_p)$ representations. *Asterisque-Societe Mathematique de France*, 2010.

Serge Lang. Elliptic functions. In *Elliptic Functions*, pages 5–21. Springer, 1987.

Serge Lang. *Algebra*. springer, 2002.

D. H. Lehmer. The vanishing of Ramanujan's function $\tau(n)$. *Duke Mathematical Journal*, 14:429–433, 1947.

The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2022. [Online; accessed 15 September 2022].

DAVID LOEFFLER and JARED WEINSTEIN. On the computation of local components of a newform. *Mathematics of Computation*, 81(278):1179–1200, 2012. ISSN 00255718, 10886842. URL http://www.jstor.org/stable/23267992.

Daniel Mamo. A newform theory for mod-p katz modular forms. *The Ramanujan Journal*, 60:861–884, 2023. doi:10.1007/s11139-022-00651-8. URL https://doi.org/10.1007/s11139-022-00651-8.

Barry Mazur. Deforming Galois Representations. In Y. Ihara, K. Ribet, and J-P. Serre, editors, *Galois Groups over* $\mathbb{Q}$, volume 16 of *Mathematical Sciences Research Institute Publications*, pages 385–437. Springer, New York, NY, 1989. URL https://doi.org/10.1007/978-1-4613-9649-9_7.

J.S. Milne. *Arithmetic Duality Theorems*. BookSurge, LLC, second edition, 2006. ISBN 1-4196-4274-X.

J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

Elias Milnor, John Milnor, Milnor John, and John N Mather. *Introduction to algebraic K-theory*. Number 72. Princeton University Press, 1971.

Enno Nagel and Aftab Pande. Reductions of modular galois representations of slope (2, 3). *arXiv preprint arXiv:1801.08820*, 2018.

Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin Heidelberg, 1999.

Frans Oort. Abelian varieties over finite fields. *NATO SECURITY THROUGH SCIENCE SERIES D-INFORMATION AND COMMUNICATION SECURITY*, 16:123, 2008.

Lue Pan. The fontaine-mazur conjecture in the residually reducible case. *Journal of the American Mathematical Society*, 35(4):1031–1169, 2022.

Mihran Papikian. Honda-tate theorem for elliptic curves. 2015.

Vytautas Paškūnas. On the Breuil–Mézard conjecture. *Duke Mathematical Journal*, 164(2), feb 2015. doi:10.1215/00127094-2861604. URL https://doi.org/10.1215%2F00127094-2861604.

Bjorn Poonen. A brief summary of the statements of class field theory.

Davide A Reduzzi. Reduction mod p of cuspidal representations of $\mathrm{GL}_2(\mathbb{F}_{p^n})$ and symmetric powers. *Journal of Algebra*, 324(12):3507–3531, 2010.

Davide A Reduzzi. Weight shiftings for automorphic forms on definite quaternion algebras, and grothendieck ring. *Mathematical Research Letters*, 22(5):1459–1490, 2015.

Kenneth A. Ribet. Galois representations attached to eigenforms with nebentypus. In Jean-Pierre Serre and Don Bernard Zagier, editors, *Modular Functions of one Variable V*, pages 18–52, Berlin, Heidelberg, 1977. Springer Berlin Heidelberg. ISBN 978-3-540-37291-2.

Kenneth A. Ribet. Mod p hecke operators and congruences between modular forms. *Inventiones mathematicae*, 71:193–205, 1983. URL `https://doi.org/10.1007/BF01393341`.

Kenneth A Ribet. On l-adic representations attached to modular forms ii. *Glasgow Mathematical Journal*, 27:185–194, 1985.

Sandra Rozensztajn. An algorithm for computing the reduction of 2-dimensional crystalline representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. *International Journal of Number Theory*, 14(07):1857–1894, 2018.

Sandra Rozensztajn. On the locus of 2-dimensional crystalline representations with a given reduction modulo p. *Algebra & Number Theory*, 14(3):643–700, 2020.

Fabian Sander. Hilbert-Samuel multiplicities of certain deformation rings. *Mathematical Research Letters*, 21, 12 2012. doi:10.4310/MRL.2014.v21.n3.a13.

A.J. Scholl. Motives for modular forms. *Invent Math*, 100:419–430, 1990. URL `https://doi.org/10.1007/BF01231194`.

J-P. Serre. Modular forms of weight one and Galois representations. *OEuvres*, pages 292–367, 1986.

J-P. Serre and R. Livné. Two letters on quaternions and modular forms (mod p). *Israel Journal of Mathematics*, 95:281–299, 1996. doi:10.1007/BF02761043. URL `https://doi.org/10.1007/BF02761043`.

Jean-Pierre Serre. Lettre à Mme Hamer, July a.

Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag New York, b.

Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, Dec 1971. ISSN 1432-1297. doi:10.1007/BF01405086. URL `https://doi.org/10.1007/BF01405086`.

Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 16(1):1–28, 1974.

Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$). 1987.

Jean-Pierre Serre et al. *Linear representations of finite groups*, volume 42. Springer, 1977.

Tetsuji Shioda. The period map of abelian surfaces. *J. Fac. Sci. Univ. Tokyo*, 25:47–59, 1978.

Samir Siksek. The modular approach to diophantine equations. In *Number Theory*, pages 495–527. Springer, 2007.

Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1994.

Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2009.

Y. T. Siu. Every K3 surface is Kähler. *Inventiones mathematicae*, 73:139–150, 1983. URL `https://doi.org/10.1007/BF01393829`.

The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2022.

William A Stein. *Modular forms, a computational approach*, volume 79. American Mathematical Soc., 2007.

Henry Peter Francis Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable III*, pages 1–55. Springer, 1973.

Ole Tange. Gnu parallel 20230722 (''), July 2023. URL `https://doi.org/10.5281/zenodo.8175685`. GNU Parallel is a general parallelizer to run multiple serial command line programs in parallel without changing them.

J. T. Tate. *Global Class Field Theory.* Algebraic number theory(J.W.S. Cassels and A. Fröhlich, eds). Academic Press Inc., 1967.

John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.

John Tate. Relations between K_2 and Galois cohomology. *Inventiones mathematicae*, 36(1): 257–274, 1976.

John Tate. Number theoretic background. In *Proc. Symp. Pure Math*, volume 33, pages 3–26, 1979.

Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Annals of Mathematics*, 141(3):553–572, 1995.

PARI/GP version 2.13.4. The PARI Group, Univ. Bordeaux, 2022. available from http://pari.math.u-bordeaux.fr/.

The Sage Developers. *SageMath, the Sage Mathematics Software System (Version x.y.z)*, 2023. https://www.sagemath.org.

Shen-Ning Tung. On the automorphy of 2-dimensional potentially semistable deformation rings of $G_{\mathbf{Q}_p}$. *Algebra & Number Theory*, 15(9):2173–2194, 2021a.

Shen-Ning Tung. On the modularity of 2-adic potentially semi-stable deformation rings. *Mathematische Zeitschrift*, 298(1-2):107–159, 2021b.

Anthony Várilly-Alvarado. Arithmetic of k3 surfaces. In *Geometry over nonclosed fields*, pages 197–248. Springer, 2017.

Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.

William C Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École Normale Supérieure*, volume 2, pages 521–560, 1969.

William C Waterhouse. Profinite groups are galois groups. *Proceedings of the American Mathematical Society*, 42(2):639–640, 1974.

Jared Weinstein. The principal series of GL_2 over a local field.

Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.

Oscar Zariski and Pierre Samuel. *Commutative algebra: Volume II*, volume 29. Springer Science & Business Media, 2013.