# Modularity of some potentially Barsotti-Tate Galois representations

A thesis presented

by

David Lawrence Savitt

to

The Department of Mathematics

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Mathematics

Harvard University

Cambridge, Massachusetts

May 2001

Thesis advisor
Richard Lawrence Taylor

Author
David Lawrence Savitt

# Modularity of some potentially Barsotti-Tate Galois representations

## Abstract

We prove a portion of a conjecture of Conrad-Diamond-Taylor, which yields proofs of some 2-dimensional cases of the Fontaine-Mazur conjectures. Let $\rho$ be a continuous odd irreducible $l$-adic Galois representation ($l$ an odd prime) satisfying the hypotheses of the Fontaine-Mazur conjecture and such that $\overline{\rho}$ is modular. The notable additional hypotheses we must impose in order to conclude that $\rho$ is modular are that $\rho$ is potentially Barsotti-Tate, that the Weil-Deligne representation associated to $\rho$ is irreducible and tamely ramified, and that $\overline{\rho}$ is conjugate to a representation over $\mathbf{F}_l$ which is reducible with scalar centralizer.

The proof follows techniques of Breuil, Conrad, Diamond, and Taylor, and in particular requires extensive calculation with Breuil's classification of $l$-torsion finite flat group schemes over base schemes with high ramification.

## Contents

# Acknowledgments

This work would not have been possible without the patience of my supervisor, Richard Taylor. At every step of the way, his meticulous advice has been of inestimable value, and his mathematical instruction has provided a wonderful education.

I am also indebted to Brian Conrad, who has been incredibly generous with his time: a tireless resource, Brian has unfailingly been willing to provide a detailed answer to any question, whether on fundamentals of algebraic geometry or minutiae of research. Several conversations with Fred Diamond were of great help to me at key stages of this work.

Joe Harris, Irine Minder, and Donna D'fini have worked tirelessly to make the Harvard math department a phenomenal place to be a graduate student, for which I thank them.

Many of my fellow graduate students have helped make life here a blast; I would particularly like to acknowledge Mira Bernstein (junta!), Spiro Karigiannis, Mark Lucianovic, and Russell Mann.

To my fellow sufferers in the Matsumura seminar—Tomas Klenke, Rob Pollack, and Tom Weston—please take note that the words Artinian and Noetherian are both capitalized everywhere in this document.

I have learned a great deal about number theory from conversations with Pete Clark, Mark Dickinson, Noam Elkies, Adam Logan, Kiran Kedlaya, William Stein, and Marty Weissman.

Ari Benbasat, Jessica Douglas, and Sandy Martinuk have kept me sane by reminding me that there's a world outside of mathematics... and they have been true friends.

Finally, I would like to thank my parents for the loving support they have provided for the past twenty-something years, for encouraging my education and yet never pushing, for always allowing me the freedom to make my own decisions, and for teaching me to make them well.

Throughout this thesis, we let $l$ be an odd prime, and we fix an algebraic closure $\overline{\mathbb{Q}}_l$ of $\mathbb{Q}_l$.

## 1. Introduction

1.1. **Aims, results, and strategies.** In this thesis, we wish to contribute to the effort to answer the following fundamental question of arithmetic algebraic geometry: when can a representation of the absolute Galois group of $\mathbb{Q}$ be found in geometry? We recall the following fundamental conjecture due to Fontaine and Mazur [FM95]:

**Conjecture A:** *Suppose that $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$ is a continuous irreducible representation such that*

(1) *$\rho$ is ramified at only finitely many primes, and*
(2) *the restriction of $\rho$ to a representation of $G_{\mathbb{Q}_l} = \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ is potentially semi-stable.*

*Then there exists a smooth projective variety $V$ defined over $\mathbb{Q}$ such that $\rho$ is a Tate twist of a subquotient of the $l$-adic étale cohomology of $V$.*

The converse to this conjecture is known: any Galois representation arising from geometry in this fashion is indeed ramified at only finitely many primes, and its restriction to $G_{\mathbb{Q}_l}$ is potentially semi-stable. (We will define potential semi-stability in the background section.) The case $n = 1$ in the above conjecture is known, and amounts to class field theory. Recently, R. Taylor [Tay00] proved a number of cases of the conjecture for $n = 2$. Until Taylor's result, all of the known cases of Conjecture A were verifications of the following conjecture, which combines the Fontaine-Mazur conjecture with the expectations of the Langlands program:

**Conjecture B:** *Suppose that* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_l)$ *is a continuous irreducible representation such that*

(1) $\rho$ *is ramified at only finitely many primes,*

(2) *the restriction of* $\rho$ *to a representation of* $G_{\mathbb{Q}_l} = \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ *is potentially semi-stable, and*

(3) $\det \rho(c) = -1$*, where* $c$ *is any choice of complex conjugation.*

*Then some Tate twist of* $\rho$ *is modular; in other words,* $\rho$ *has a Tate twist that is the representation associated to a modular form via the methods of* [Shi71, Del71, DS74]. *It follows that the Fontaine-Mazur conjecture is true for* $\rho$.

In this thesis, we prove the following cases of Conjecture B:

**Theorem 2.4:** *Let* $l$ *be an odd prime,* $K$ *a finite extension of* $\mathbb{Q}_l$ *in* $\overline{\mathbb{Q}}_l$*, and* $k$ *the residue field of* $K$*. Let*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(K)$$

*be an odd continuous representation ramified at only finitely many primes. Assume that its reduction*

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$$

*is absolutely irreducible after restriction to* $\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}\, l})$ *and is modular. Further, suppose that*

(1) $\overline{\rho}\,|_{G_{\mathbb{Q}_l}}$ *is actually a representation to* $\mathrm{GL}_2(\mathbb{F}_l)$*, and as such is reducible with centralizer* $\mathbb{F}_l$*,*

(2) $\rho\,|_{G_{\mathbb{Q}_l}}$ *is potentially Barsotti-Tate, and the associated Weil-Deligne representation* $WD(\rho\,|_{G_{\mathbb{Q}_l}})$ *is irreducible and tamely ramified.*

*Then* $\rho$ *is modular.*

(For the terminology of this result, see section 1.2.) This work carries on the work of Wiles [Wil95] and Taylor-Wiles [TW95] in proving Fermat's Last Theorem, and the continuation of this work by Breuil, Conrad, Diamond, and Taylor [Dia96, CDT99, BCDT] to prove the Shimura-Taniyama conjecture, all of which involved demonstrating special cases of Conjecture B. For example, in [CDT99], Conrad, Diamond, and Taylor are able to prove results similar to theorem 2.4 with conditions (1) and (2) replaced by

- $\overline{\rho}\,|_{G_{\mathbb{Q}_l}}$ is reducible with trivial centralizer, $\rho\,|_{G_{\mathbb{Q}_l}}$ is potentially Barsotti-Tate, and the associated Weil-Deligne representation $WD(\rho\,|_{G_{\mathbb{Q}_l}})$ is reducible and tamely ramified,

as well as a few cases when $WD(\rho\,|_{G_{\mathbb{Q}_l}})$ is irreducible and tamely ramified but the image of $WD(\rho\,|_{G_{\mathbb{Q}_l}})\,|_{I_l}$ has size no greater than $2(l-1)$. These results are achieved by studying deformations which become Barsotti-Tate over extensions of ramification degree dividing $l-1$. With the advent of Breuil modules, the authors of [BCDT] are able to prove results similar to theorem 2.4 for $l = 3$ and a few specific pairs of $\overline{\rho}$ and wildly ramified $WD(\rho\,|_{G_{\mathbb{Q}_3}})$.

The aforementioned authors prove cases of employing a strategy that can be divided roughly into three steps:

(1) Show that $\overline{\rho}$, the mod $l$ reduction of $\rho$, is modular.
(2) Prove results of the form "Under certain hypotheses, the modularity of $\overline{\rho}$ implies the modularity of $\rho$".
(3) Verify these "certain hypotheses" for the cases in question.

For example, Langlands [Lan80] and Tunnell [Tun81] proved results of the form (1), and further results of this form are known for $l = 3$ and $l = 5$. Wiles, Taylor-Wiles, Conrad-Diamond-Taylor, and Skinner-Wiles [SW97] all demonstrated results of the form (2).

The difficulty of step (3) should not be underestimated: for example, it comprises the bulk of the work in [BCDT], and is the most involved step in this work as well. Very roughly, the proof entails showing that particular Galois deformation rings have one-dimensional tangent spaces. The Galois representations under consideration arise from finite flat group schemes, and consequently to understand these deformation rings we must calculate extensively with such group schemes. After providing the necessary background material, will give a detailed description of this work and related potential areas of research.

Finally, in joint work currently in progress with W. Stein, we hope to provide an example of a genus 2 curve whose Jacobian is proved to be modular by theorem 2.4.

1.2. **Background.** The reader should be aware that a great deal of notation required for later sections will be introduced during the following discussion of background material. Further, this material is not background in the sense that we expect most (or many) readers to know it already, but rather that it is the work of others, that it is essential for this to be a moderately self-contained work, and that the expositions of our main results flow more smoothly if this material is treated beforehand (rather than as it arises).

1.2.1. *Mod $l$ Galois representations.* We follow the exposition of Serre [Ser87]. Recall that the Galois group $G_{\mathbb{Q}_l} = \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ fits into an exact sequence

$$0 \longrightarrow I_l \longrightarrow G_{\mathbb{Q}_l} \xrightarrow{v} \hat{\mathbb{Z}} \longrightarrow 0$$

where $I_l$ is the inertia group and $\hat{\mathbb{Z}} \cong \mathrm{Gal}(\overline{\mathbb{F}}_l/\mathbb{F}_l)$. We fix a generator of $\hat{\mathbb{Z}}$ by requiring that $1 \in \hat{\mathbb{Z}}$ map to arithmetic Frobenius $x \mapsto x^l$ in $\mathrm{Gal}(\overline{\mathbb{F}}_l/\mathbb{F}_l)$. Now, the inertia group $I_l$ fits into an exact sequence

$$0 \longrightarrow I_w \longrightarrow I_l \longrightarrow I_t \longrightarrow 0,$$

where $I_w$ is the wild (pro-$l$) inertia and $I_t$ is the tame (prime-to-$l$) inertia. Suppose $s \in G_{\mathbb{Q}_l}$ has image $v(s) = 1$ in $G_{\mathbb{Q}_l}/I_l \cong \hat{\mathbb{Z}}$, so that $s$ is a lift of arithmetic Frobenius; then, if $u \in I_l$ is any element of inertia, one can check that

$$sus^{-1} \in u^l I_w.$$

This amounts to checking that $su = u^l s$ on the fixed field $\mathbb{Q}_l^{\mathrm{tr}}$ of $I_w$, which can be verified directly using the fact that $\mathbb{Q}_l^{\mathrm{tr}}$ is obtained by adjoining to $\mathbb{Q}_l^{\mathrm{ur}}$ (the maximial unramified extension of $\mathbb{Q}_l$, i.e., the fixed field of $I_l$) all of the $n^{\mathrm{th}}$ roots of $l$ for $n$ not divisible by $l$.

Since $I_w$ is pro-$l$ while $\overline{\mathbb{F}}_l^\times$ is prime-to-$l$, every continuous character $\chi : I_l \to \overline{\mathbb{F}}_l^\times$ factors through $I_t$. (Recall that we endow $\overline{\mathbb{F}}_l$ with the discrete topology.) By continuity $\chi$ must have a finite image; the smallest $n$ such that $\chi(I_l) \subset \mathbb{F}_{l^n}$ is called the level of $\chi$. Using the description

$$I_t \cong \lim_{\leftarrow} \mathbb{F}_{l^n}^\times,$$

one sees that every character of level $n$ is a power of the character

$$\omega_n : u \mapsto \frac{u(l^{1/(l^n-1)})}{l^{1/(l^n-1)}} \pmod{l}\,.$$

(We identify $\mathbb{F}_{l^n} \subset \mathbb{Q}_l^{\mathrm{un}}$ via the Teichmüller lifting map.) In particular $\omega = \omega_1$ is the mod $l$ cyclotomic character.

If a character of $I_l$ extends to a character $\chi$ on all of $G_{\mathbb{Q}_l}$, we know that

$$\chi(sus^{-1}u^{-l}) \in \chi(I_w) = 1\,.$$

Since the image of $\chi$ is commutative, this forces $\chi(u)^{l-1} = 1$, and so $\chi\,|_{I_l}$ has level 1. It follows readily that $\chi = \chi_a\omega^i$ for some $a \in \overline{\mathbb{F}}_l^{\times}$ and $i \in \mathbb{Z}/(l-1)\mathbb{Z}$, where $\chi_a$ is the unramified character sending arithmetic Frobenius to $a$. (We will also let $\omega$ denote the extension of $\omega$ to all of $G_{\mathbb{Q}_l}$.)

We now examine two-dimensional representations of $G_{\mathbb{Q}_l}$ over $\overline{\mathbb{F}}_l$. Let $V$ be a two-dimensional vector space over $\overline{\mathbb{F}}_l$, and suppose

$$\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}(V)$$

be a continuous representation. The image $\overline{\rho}(I_w) \subset \mathrm{GL}(V)$ must be unipotent. Letting $V^{ss}$ be the semisimplification of $V$ for the action of $G_{\mathbb{Q}_l}$, it follows that $I_w$ acts trivially on $V^{ss}$, and so the action of $I_l$ on $V^{ss}$ factors through $I_t$. The image of $\overline{\rho}$ is finite and $I_t$ is abelian, so the action of $I_t$ on $V^{ss}$ must decompose as a sum of two characters $\psi$ and $\psi'$; and now the relation $\rho(sus^{-1}) = \rho(u^l)$ tells us that either

$$\psi^l = \psi\,,\ (\psi')^l = \psi'$$

or

$$\psi^l = \psi'\,,\ (\psi')^l = \psi\,.$$

In the former situation, $\psi$ and $\psi'$ are both characters of level 1; in the latter, they have level 2, and in fact there is an integer $m$ not divisible by $l+1$ such that $\psi = \omega_2^m$ and $\psi' = \omega_2^{lm}$.

$V$ **not semisimple.** Since the image of $I_w$ is unipotent and $V$ is not semisimple, it follows that

$$\overline{\rho}(I_w) \subset U \cong \left\{ \begin{pmatrix} 1 & * \\ & \\ 0 & 1 \end{pmatrix} \right\}.$$

Since $I_w$ is normal in $G_{\mathbb{Q}_l}$, we must have

$$\overline{\rho}(G_{\mathbb{Q}_l}) \subset N_{\mathrm{GL}(V)}(U) \cong \left\{ \begin{pmatrix} * & * \\ & \\ 0 & * \end{pmatrix} \right\}.$$

Therefore $\overline{\rho}$ is reducible and the diagonal characters are extensions of $\psi$ and $\psi'$ to all of $G_{\mathbb{Q}_l}$, and so $\psi$ and $\psi'$ are of level 1. It follows that

$$\overline{\rho} \sim \begin{pmatrix} \chi_a \omega^i & * \\ & \\ 0 & \chi_b \omega^j \end{pmatrix}.$$

Suppose $a, b \in \mathbb{F}_l$. It is a good exercise in Galois cohomology to check that unless $(\chi_a \omega^i)/(\chi_b \omega^j)$ is 1 or $\omega$, then the collection of $\mathbb{F}_l$-extensions of $\chi_b \omega^j$ by $\chi_a \omega^i$ is one-dimensional. On the other hand, when $a = b$ and $i = j + 1$, Kummer theory dictates that the group of extensions is two-dimensional, isomorphic to $\mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^l$; the extensions corresponding to $\mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^l \subset \mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^l$ are said to be peu-ramifié, and the others are said to be très-ramifié. (The extensions in case $i = j + 1$ and $a \neq b$ are also said to be peu-ramifié.)

$V$ **semisimple,** $\psi$ **and** $\psi'$ **of level** 1**.** In this case

$$\overline{\rho}\,|_{I_l} \sim \begin{pmatrix} \omega^a & 0 \\ & \\ 0 & \omega^b \end{pmatrix}$$

and the relation $\rho(sus^{-1}) = \rho(u^l)$ tells us that $\overline{\rho}(s)$ commutes with the image of $I_l$. Since only diagonal matrices commute with non-scalar diagonal matrices, it is easy to see that $\overline{\rho} \sim \chi_a \omega^i \oplus \chi_b \omega^j$.

**$V$ semisimple, $\psi$ and $\psi'$ of level 2.** We have

$$\overline{\rho}\,|_{I_l} \sim \begin{pmatrix} \omega_2^m & 0 \\ 0 & \omega_2^{lm} \end{pmatrix}.$$

If $\overline{\rho}$ were reducible, then $G_{\mathbb{Q}_l}$ would act on a subspace of $V$, and this action would have to be an extension of $\omega_2^m$ or $\omega_2^{lm}$ to $G_{\mathbb{Q}_l}$. Since the characters of level 2 do not extend in this fashion, it follows that $\overline{\rho}$ is irreducible.

1.2.2. *Tame $l$-adic representations.* We recall that the Weil group $W_l$ is defined as the subgroup of $G_{\mathbb{Q}_l}$ which fits into the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_l & \longrightarrow & W_l & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I_l & \longrightarrow & G_{\mathbb{Q}_l} & \xrightarrow{v} & \hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

and which has a topology chosen so that the subgroup $I_l$ is open and carries its usual topology, while the quotient $W_l/I_l$ is discrete. Let $K/\mathbb{Q}_l$ be a finite extension and let

$$\rho : G_l \text{ or } W_l \longrightarrow \mathrm{GL}_2(K)$$

be a continuous representation of either $G_l$ or $W_l$. Since the inertia group $I_l$ is compact, it is a standard result (see, e.g., the first section of [Ser89]) that $\rho$ is equivalent to a representation $\tilde{\rho}$ such that

$$\tilde{\rho}\,|_{I_l} : I_l \longrightarrow \mathrm{GL}_2(\mathcal{O}_K)\,,$$

so we may assume without loss of generality that $\rho|_{I_l}$ is a representation over $\mathcal{O}_K$. Suppose now that $\rho$ is tame, that is, suppose that $\rho|_{I_w}$ is trivial. If $\mathcal{O}_K$ has uniformizer $\pi$, then the subgroup

$$U_1 = \ker(\mathrm{GL}_2(\mathcal{O}_K) \longrightarrow \mathrm{GL}_2(\mathcal{O}_K/\pi))$$

is open, and so $H = (\rho|_{I_l})^{-1}(U_1)$ is open in $I_l$. However, $\rho$ is tame, $U_1$ is pro-$l$, and $I_t$ is pro-prime-to-$l$, so $\rho(H) = 1$. It follows that the image $\rho(I_l)$ is finite. Since $\rho|_{I_l}$ factors through the abelian group $I_t$ and has finite image, it decomposes as a sum of two characters of finite order, $\chi_1$ and $\chi_2$. As in the mod $l$ case, the relation $\rho(sus^{-1}) = \rho(u^l)$ forces

$$\chi_1^l = \chi_1\,,\ \chi_2^l = \chi_2$$

or

$$\chi_1^l = \chi_2\,,\ \chi_2^l = \chi_1\,.$$

If $\tilde{\omega}_n$ denotes the Teichmüller lift of the character $\omega_n$ defined in the previous section, so that

$$\tilde{\omega}_n : u \mapsto \frac{u(l^{1/(l^n-1)})}{l^{1/(l^n-1)}}\,,$$

we obtain either

$$\chi_1 = \tilde{\omega}^i\,,\ \chi_2 = \tilde{\omega}^j$$

or

$$\chi_1 = \tilde{\omega}_2^m\,,\ \chi_2 = \tilde{\omega}_2^{lm}\,.$$

(We re-use the shorthand $\tilde{\omega} = \tilde{\omega}_1$, and we may again regard $\tilde{\omega}$ as a character on $G_{\mathbb{Q}_l}$ by taking the Teichmüller lift of the extension to $G_{\mathbb{Q}_l}$ of $\omega$.) By the same argument as in the previous section, the former case occurs when $\rho$ is geometrically reducible, while the latter case occurs when $\rho$ is geometrically irreducible.

1.2.3. *Period rings.* Fontaine (see [Fon94] or [FI93]) has constructed period rings $B_{HT}$, $B_{dR}$, $B_{st}$, and $B_{cris}$ (respectively, the Hodge-Tate, de Rham, semi-stable, and crystalline period rings) in order to prove comparison theorems on cohomology. For each of these rings, he defines a functor on the category of $l$-adic representations of $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}_l/K)$ for any finite extension $K$ of $\mathbb{Q}_l$:

$$D_X(\rho) = (B_X \otimes_{\mathbb{Q}_l} \rho)^{G_K}$$

for each $X \in \{HT, dR, st, cris\}$. Let $K_X$ be the field of invariants $(B_X)^{G_K}$; in other words, $K_X$ is the image under $D_X$ of the trivial representation. If $K_0$ denotes the maximal unramified subfield of $K$, then $K_{HT} = K_{dR} = K$ and $K_{st} = K_{cris} = K_0$. The map

$$\alpha_X : B_X \otimes_{K_X} D_X(\rho) \to B_X \otimes_{\mathbb{Q}_l} \rho$$

is always injective. We say that the representation $\rho$ is *Hodge-Tate*, *de Rham*, *semi-stable*, or *crystalline* if the corresponding map $\alpha_X$ is an isomorphism, which is equivalent to an equality

$$\dim_{K_X} D_X(\rho) = \dim_{\mathbb{Q}_l} \rho.$$

Finally, to say that a representation of $G_K$ is *potentially* semi-stable or crystalline is to say that there is a finite extension $L/K$ such that the restriction to a representation of $G_L$ is, respectively, semi-stable or crystalline. These properties fit into the following hierarchy:

$$\text{pot. crystalline} \implies \text{pot. semi-stable} \implies \text{de Rham} \implies \text{Hodge-Tate}.$$

Geometrically, the $l$-adic étale cohomology of a variety possessing a semi-stable model over the ring of integers $\mathcal{O}_K$ is always a semi-stable representation. Crystalline representations should be thought of as coming from varieties having smooth models.

The advantage of working with representations having these properties is that the period rings $B_X$ have structure which carries over to $D_X(\rho)$; then, via the isomorphism $\alpha_X$, the structure on $D_X(\rho)$ yields information about $\rho$. Moreover, the $D_X(\rho)$ are essentially linear-algebraic objects, and are therefore easier to compute with than the Galois representations $\rho$. For example, $B_{HT}$ is graded, so for any two-dimensional Hodge-Tate representation $\rho$, the two-dimensional vector space $D_{HT}(\rho)$ is also graded. Hence we can assign to $\rho$ a pair of integers called the Hodge-Tate weights of $\rho$: the degrees of the two (possibly equal) nonzero graded pieces of $D_{HT}(\rho)$. If $\rho$ is potentially semi-stable, and consequently Hodge-Tate, its Hodge-Tate weights $(r, s)$ with $s \geq r$ have the following significance: in Conjecture B, one would expect the modular form giving rise to $\rho$ to have weight $s - r + 1$. (In Conjecture B, representations with lesser Hodge-Tate number equal to 0 are themselves expected to be modular. Giving $\rho$ a Tate twist by $n$ translates both Hodge-Tate numbers of $\rho$ by $n$, and so indeed we see that any semi-stable representation should be a Tate twist of a modular one.)

**Example 1:** (characters of $G_{\mathbb{Q}_l}$ over $\mathbb{Z}_l$; see section 8 of [FM95]) Let $\epsilon$ be the cyclotomic character of $G_{\mathbb{Q}_l}$, so that the mod $l$ reductions of both $\epsilon$ and $\tilde{\omega}$ are equal to $\omega$. Their ratio

$$\epsilon/\tilde{\omega} = \chi_0 : G_{\mathbb{Q}_l} \to 1 + l\mathbb{Z}_l.$$

Let $\chi_a$ denote the unramified character of $G_{\mathbb{Q}_l}$ taking arithmetic Frobenius to $a \in \mathbb{Z}_l^\times$. Then the characters of $G_{\mathbb{Q}_l}$ over $\mathbb{Z}_l$ are of the form

$$\chi_a \cdot \chi_0^r \cdot \tilde{\omega}^i$$

with $r \in \mathbb{Z}_l$ and $i \in \mathbb{Z}/(l-1)\mathbb{Z}$. This character is potentially semi-stable if and only if it is Hodge-Tate if and only if $r \in \mathbb{Z}$, in which case it has Hodge-Tate weight $r$. Moreover, the representation is crystalline if and only if $i \equiv r \pmod{l-1}$, i.e. if and only if it is of the form $\chi_a \epsilon^r$.

**Example 2:** in section 4 of [Tat67], Tate shows that the $2d$-dimensional Galois representation on the Tate module of an abelian scheme of dimension $d$ has Hodge-Tate weights 0 and 1, each with multiplicity $d$.

1.2.4. *Galois types.* The ring $B_{st}$ carries a monodromy operator $N$ and a Frobenius-semilinear endomorphism $\phi$; if $\rho$ is semi-stable and the monodromy operator $N$ vanishes on $D_{st}(\rho)$, then $\rho$ is crystalline.

Let $\rho$ be a $d$-dimensional potentially semi-stable representation of $G_{\mathbb{Q}_l}$ over $K \subset \overline{\mathbb{Q}}_l$. Following section B.1 of Appendix B of [CDT99] and section 2.2.1 of [BM00] as references, we use the extra structure provided by potential semi-stability to construct a new representation $WD(\rho) : W_l \to \mathrm{GL}_d(\overline{\mathbb{Q}}_l)$, where $W_l$ is the Weil subgroup of $G_{\mathbb{Q}_l}$ (whose definition was recalled in section 1.2.2). Let $E/\mathbb{Q}_l$ be a finite Galois extension over which $\rho$ becomes semi-stable, so that

$$D_{st,E}(\rho) = (B_{st} \otimes_{\mathbb{Q}_l} \rho\,|_{G_E})^{G_E}$$

is free of rank $d$ over $E_0 \otimes_{\mathbb{Q}_l} K$. Since $\rho$ was a representation of the whole of $G_{\mathbb{Q}_l}$, the space $D_{st,E}$ still carries an action of $\mathrm{Gal}(E/\mathbb{Q}_l)$, which is linear with respect to

$K$ but semilinear with respect to $E_0$. Moreover, the action of $\mathrm{Gal}(E/\mathbb{Q}_l)$ commutes with the Frobenius $\phi$, which is also linear in $K$ and semilinear in $E_0$.

We may therefore define a *linear* action of $W_l$ on $D_{st,E}$ as follows. First, if $g \in I_l$, we let $g$ act as $g\,|_E \in \mathrm{Gal}(E/\mathbb{Q}_l)$. We extend this action to all of $W_l$ by letting $g \in W_l$ act as $g\,|_E \cdot \phi^{-v(g)}$. Finally, we extend this action linearly to

$$WD(\rho) = D_{st,E}(\rho) \otimes_{E_0 \otimes_{\mathbb{Q}_l} K} \overline{\mathbb{Q}}_l\,,$$

a $d$-dimensional representation over $\overline{\mathbb{Q}}_l$, which together with a monodromy operator is the Weil-Deligne representation attached to $\rho$. One proves (Lemme 2.2.1.1 of [BM00]) that this definition is independent of our choice of $E$ and of our embedding $E_0 \hookrightarrow \overline{\mathbb{Q}}_l$. If $\sigma \in G_K$, then ${}^{\sigma}WD(\rho) \sim WD(\rho)$, but $WD(\rho)$ may not be defined over $K$.

We make several observations regarding $WD(\rho)$. First, since the image of $WD(\rho)$ is finitely generated by the action of $\mathrm{Gal}(E/\mathbb{Q}_l)$ and $\phi$, we see that $WD(\rho)$ must have field of definition which is finite over $\mathbb{Q}_l$; in fact, any common extension of $E_0$ and $K$ will do. Second, by construction the inertia subgroup $I_E$ of $G_E$ is in the kernel of $WD(\rho)$, and so $WD(\rho)$ is a continuous representation. Finally, the $WD$-functor is compatible with tensor products and exterior products. This is not obvious; for a proof, see [Fon94].

**Example 1:** (following appendix B.2 of [CDT99]) If $\epsilon$ is the cyclotomic character $G_{\mathbb{Q}_l} \to \overline{\mathbb{Q}}_l$, then $WD(\epsilon)$ is the unramified character sending arithmetic Frobenius to $l$. The fact that $WD(\epsilon)$ is unramified can be seen from the fact that $\epsilon$ is crystalline; verifying the action of arithmetic Frobenius amounts to checking that $\phi$ acts as $1/l$,

which comes down to showing the existence of $t \in B_{cris}$ on which $G_{\mathbb{Q}_l}$ acts via $\epsilon$ and such that $\phi(t) = lt$.

**Example 2:** (again following appendix B.2 of [CDT99]) If $\rho$ has finite image, then $WD(\rho) \cong \rho|_{W_l} \otimes \overline{\mathbb{Q}}_l$. This can be seen by taking $E$ to be any splitting field for $\rho$.

The isomorphism class of the representation

$$\tau(\rho) = WD(\rho)\,|_{I_l}$$

is called the *l-type* or *Galois type* of $\rho$. We have seen that if $\rho$ becomes semi-stable over $E$ then $\tau\,|_{I_E}$ is trivial. The converse is also true, which we argue as follows: suppose $\tau\,|_{I_E}$ is trivial and $\rho$ becomes semi-stable over $E'/E$, and suppose $E'/E$ is Galois and has inertial index $f$. Now, $I_E$ acts trivially on $D_{st,E'}(\rho)$, so by a descent argument

$$\dim_K D_{st,E}(\rho) = \frac{1}{f} \dim_K D_{st,E'}(\rho)\,.$$

Since $[E'_0 : E_0] = f$, it follows that

$$\dim_{E_0 \otimes K} D_{st,E}(\rho) = \dim_{E'_0 \otimes K} D_{st,E'}(\rho) = d\,.$$

Since the left-hand side is at most $d$, we see equality must hold, the map $\alpha_{st,E}$ must be surjective, and by definition $\rho$ is semistable over $E$.

We record the following facts in the case $d = 2$: if $\rho$ is potentially semi-stable and $\tau(\rho)$ is not scalar, then the monodromy operator $N$ must vanish and so $\rho$ is potentially crystalline. Furthermore, C. Breuil [Bre99a] has proved that $\rho$ is potentially crystalline with Hodge-Tate weights $(0, 1)$ if and only if $\rho$ is *potentially*

*Barsotti-Tate*, i.e., some restriction $\rho|_{G_K}$ is the representation on the Tate module of an $l$-divisible group $\Gamma$ over the ring of integers $\mathcal{O}_K$.

1.2.5. *The Barsotti-Tate case.* We directly follow Appendix B.3 of [CDT99]. When $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_d(K)$ is potentially Barsotti-Tate, we provide an alternate description of $WD(\rho)$. Suppose $\rho$ becomes Barsotti-Tate over a finite Galois extension $E$ of $\mathbb{Q}_l$, so that $\rho|_{G_E}$ arises from an $l$-divisible group $\Gamma$ over $\mathcal{O}_E$. Write $\mathcal{O}$ for the integers of $K$, and $\mathbf{k}$ for the residue field of $E$.

By Tate's full faithfulness theorem (Theorem 4 of [Tat67]), $\Gamma$ has an action of $\mathrm{Gal}(E/\mathbb{Q}_l)$ over the action of $\mathrm{Gal}(E/\mathbb{Q}_l)$ on Spec $(\mathcal{O}_E)$. This reduces to an action on the closed fibre $\Gamma \times \mathbf{k}$. Let $\phi$ be the Frobenius endomorphism of the closed fibre of $\Gamma$; then we produce an action of $W_l$ on $\Gamma_{/\mathbf{k}}$ by letting $g$ act via $g|_E \circ \phi^{-v(g)}$.

This above action of $W_l$ is a right-action. It therefore translates into a left-action on the contravariant Dieudonné module $D(\Gamma_{/\mathbf{k}})$. $D$ is a free $W(\mathbf{k})$-module of rank $d[K : \mathbb{Q}_l]$. Let $F$ denote the Frobenius element of the Dieudonné ring.

Next, we define an action of $W_l$ on

$$D'(\Gamma_{/\mathbf{k}}) = \mathrm{Hom}_{W(\mathbf{k})}(D(\Gamma_{/\mathbf{k}}), W(\mathbf{k}))\,.$$

We set

$$\phi'(f) = \sigma \circ f \circ F^{-1}$$

on $D'(\Gamma_{/\mathbf{k}})[1/l]$, where $\sigma$ is Frobenius on $W(\mathbf{k})$, and for $g \in \mathrm{Gal}(E/\mathbb{Q}_l)$ we set

$$g(f) = \overline{g} \circ f \circ g^{-1}$$

where $\overline{g}$ is the map $g$ induces on $W(\mathbf{k})$ and $g^{-1}$ is the semilinear action on $D(\Gamma_{/\mathbf{k}})$ coming from the semilinear action on $\Gamma$. Finally, as usual, we let $W_l$ act on $D'(\Gamma_{/\mathbf{k}})$ by letting $g$ act as $g|_E \circ (\phi')^{-v(g)}$.

Finally, we note that the action of $\mathcal{O}$ on $\Gamma$ propagates through all of the above constructions, and we have (proposition B.3.1 in [CDT99]):

$$WD(\rho) \cong D'(\Gamma_{/\mathbf{k}}) \otimes_{W(\mathbf{k})\otimes_{\mathbb{Z}_l}\mathcal{O}} \overline{\mathbb{Q}}_l \,.$$

Our main use for this result will be to translate knowledge about $WD(\rho)$ into facts about $D(\Gamma_{/\mathbf{k}})$.

1.2.6. *Deformation problems.* Let $\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbf{k})$ be a representation over a finite field $\mathbf{k}$ of characteristic $l$, and assume that the only matrices which commute with the image of $\overline{\rho}$ are scalar matrices. Fix a positive integer $k$ and a Galois type $\tau$. We are interested in lifts $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_l)$ of $\overline{\rho}$ with the following properties, which can be thought of as properties coming from modular forms:

(1) $\rho$ is potentially semi-stable with Hodge-Tate weights $(0, k-1)$,

(2) $\tau(\rho)$ is isomorphic to $\tau$, and

(3) $\det(\rho) = \epsilon^{k-1}\chi$, where $\epsilon$ denotes the $l$-adic cyclotomic character on $G_{\mathbb{Q}_l}$ and $\chi$ is a character of finite order prime to $l$.

We want to define a deformation ring $R(\overline{\rho}, k, \tau)$ parametrizing representations of the above type. However, the immediate difficulty is that the above conditions are not a deformation condition in any traditional sense. (For example, conditions (1) and (2) are not meaningful for deformations to Artinian $\mathbb{Z}_l$-algebras.) We get around this problem by taking a "Zariski closure", as follows. Let $R_{\mathcal{O}}^{univ}$ denote the universal deformation ring parametrizing deformations of $\rho$ over $\mathcal{O}$-algebras for $\mathcal{O}$ the integers of an $l$-adic local field containing both the Witt vectors $W(\mathbf{k})$ and a field of rationality of $\tau$, and let $\rho^{univ}$ be the universal deformation. (See [Maz95] for deformation theory details.) We say that a prime $\mathfrak{p}$ of $R_{\mathcal{O}}^{univ}$ has type $(k, \tau)$ if

there is a local field $K \supset \mathcal{O}$ and a map of $\mathcal{O}$-algebras

$$f_{\mathfrak{p}} : R^{univ}_{\mathcal{O}} \to K \quad \text{with} \quad \mathfrak{p} = \ker(f_{\mathfrak{p}})$$

such that the pushforward of $\rho^{univ}$ by $f_{\mathfrak{p}}$ satisfies the three desired conditions above. Since $\mathcal{O}$ contains a field of rationality of $\tau$, if $\sigma \in G_K$ we have ${}^{\sigma}\tau \sim \tau$, and so the definition of type $(k, \tau)$ is independent of the choice of $f_{\mathfrak{p}}$. We next define

$$R(\overline{\rho}, k, \tau)_{\mathcal{O}} = R^{univ}_{\mathcal{O}} / \bigcap_{\mathfrak{p} \text{ type } (k,\tau)} \mathfrak{p} \, .$$

When $W(\mathbf{k})$ contains a field of rationality of $\tau$, we will often write $R(\overline{\rho}, k, \tau)$ for $R(\overline{\rho}, k, \tau)_{W(\mathbf{k})}$; we remark in particular that this is always the case for $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, which is rational over $\mathbb{Q}_l$.

These deformation rings are of particular interest because [CDT99] and [BCDT] use the methods of [Wil95] and [TW95] to prove results of roughly the following form (for a precise statement, see theorem 2.1) : if $\rho$ is a potentially semi-stable $l$-adic representation of $G_{\mathbb{Q}}$ of Galois type $\tau$ and Hodge-Tate weights $(0, 1)$ and such that $\overline{\rho}$ is modular, and if there is a surjection $\mathcal{O}[[X]] \twoheadrightarrow R(\overline{\rho}, 2, \tau)_{\mathcal{O}}$, then $\rho$ is modular. In this case, we say that $\tau$ is *weakly acceptable* for $\overline{\rho}$. If $\tau$ is weakly acceptable for $\overline{\rho}$ and $R(\overline{\rho}, 2, \tau)_{\mathcal{O}} \neq (0)$, we say that $\tau$ is acceptable for $\overline{\rho}$. We remark (Appendix A of [CDT99]) that

$$R(\overline{\rho}, k, \tau)_{\mathcal{O}'} \cong \mathcal{O}' \otimes_{\mathcal{O}} R(\overline{\rho}, k, \tau)_{\mathcal{O}} \, ,$$

so when $\tau$ is defined over the fraction field of $W(\mathbf{k})$ the acceptability and weak acceptability of $\tau$ for $\overline{\rho}$ depend only on $R(\overline{\rho}, k, \tau)$.

### 1.3. **Open questions and progress.**

1.3.1. *Conjectures of Conrad, Diamond, and Taylor, and our approach.* Let $\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbf{k})$. In [CDT99], Conrad, Diamond, and Taylor make the following conjectures regarding weak acceptability of tamely ramified $l$-types $\tau$:

**Conjecture:** ([CDT99], Conjecture 1.2.2) *Suppose that $\tau = \tilde{\omega}^i \oplus \tilde{\omega}^j$. Then $R(\overline{\rho}, 2, \tau)$ is nonzero if and only if $\overline{\rho}\,|_{I_l} \otimes_{\mathbf{k}} \overline{\mathbf{k}}$ has one of the following forms:*

- $\begin{pmatrix} \omega^{1+i} & * \\ 0 & \omega^j \end{pmatrix}$ *and in case $j \equiv i \pmod{l-1}$, $*$ is peu-ramifié,*
- $\begin{pmatrix} \omega^{1+j} & * \\ 0 & \omega^i \end{pmatrix}$ *and in case $j \equiv i \pmod{l-1}$, $*$ is peu-ramifié,*
- $\omega_2^{1+\{j-i\}+(l+1)i} \oplus \omega_2^{l-\{j-i\}+(l+1)j}$, *where $\{a\}$ denotes the unique integer in the range from $0$ to $l-2$ congruent to $a$ modulo $l-1$.*

*In the first two of these cases, $R(\overline{\rho}, 2, \tau)_{\mathcal{O}} \cong \mathcal{O}[[X]]$, and so $\tau$ is acceptable for $\overline{\rho}$. In the last case, if $j \equiv i \pmod{l-1}$, then $R(\overline{\rho}, 2, \tau)_{\mathcal{O}} \cong \mathcal{O}[[X]]$ and so $\tau$ is acceptable for $\overline{\rho}$.*

**Conjecture:** ([CDT99], Conjecture 1.2.3) *Suppose that $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, where $m \in \mathbb{Z}/(l^2-1)\mathbb{Z}$ and $m = i + (l+1)j$ with $i = 1, \ldots, l$ and $j \in \mathbb{Z}/(l-1)\mathbb{Z}$. Then $R(\overline{\rho}, 2, \tau)$ is nonzero if and only if $\overline{\rho}\,|_{I_l} \otimes_{\mathbf{k}} \overline{\mathbf{k}}$ has one of the following forms:*

- $\begin{pmatrix} \omega^{i+j} & * \\ 0 & \omega^{1+j} \end{pmatrix}$ *and in case $i = 2$, $*$ is peu-ramifié,*
- $\begin{pmatrix} \omega^{1+j} & * \\ 0 & \omega^{i+j} \end{pmatrix}$ *and in case $i = l-1$, $*$ is peu-ramifié,*
- $\omega_2^{1+m} \oplus \omega_2^{l(1+m)}$,
- $\omega_2^{l+m} \oplus \omega_2^{1+lm}$.

*In all of these cases $R(\overline{\rho}, 2, \tau)_{\mathcal{O}} \cong \mathcal{O}[[X]]$, and so $\tau$ is acceptable for $\overline{\rho}$.*

We are interested in proving these conjectures. Because of significant work of Breuil and Mézard on the former of these two conjectures, in this thesis we will consider the latter. Our objective is to obtain modularity results, for which we require proofs of weak acceptability, and not the stronger assertion of acceptability; that is, we wish to prove that certain rings $R(\overline{\rho}, 2, \tau)$ have 1-dimensional tangent spaces, but we will not concern ourselves with giving precise descriptions of rings $R(\overline{\rho}, 2, \tau)$.

Our methods are akin to the computations carried out by Conrad and Diamond in [BCDT] for $l = 3$ and wildly ramified $\tau$. The idea is to replace $R(\overline{\rho}, 2, \tau)$ with a deformation ring $R'$ which surjects onto $R(\overline{\rho}, 2, \tau)$ but whose tangent space can be found more easily, and then to tighten $R'$ until its tangent space is as small as needed. Since $\tau$ is non-scalar and we have taken $k = 2$, we are considering deformations $\rho$ which are potentially Barsotti-Tate. The work of C. Breuil [Bre98, Bre99c] gives an equivalence of categories between the category of $l$-torsion finite flat groups schemes over $\mathcal{O}_K$, and a certain category of linear-algebraic objects which have become known as Breuil modules; specifically, it is now tractable to perform computations involving finite flat group schemes over rings with arbitrary ramification index. (The ramification index of $K/\mathbb{Q}_l$ is $e = l^2 - 1$ for the calculations we will perform.) Computations with finite flat groups schemes are well-suited to finding tangent spaces of deformation rings, and we would therefore prefer to work with deformations $\rho$ having constraints involving finite flat group schemes instead of constraints involving $l$-divisible groups.

To accomplish the shift to working with finite flat group schemes instead of $l$-divisible groups, suppose $\rho|_{G_K}$ is Barsotti-Tate, so that $\rho|_{G_K}$ is the representation

on the Tate module of an $l$-divisible group $\mathcal{G}$ over $\mathcal{O}_K$. Then the $l^n$-torsion $\mathcal{G}[l^n]$ of $\mathcal{G}$ is a finite flat group scheme over $\mathcal{O}_K$ whose generic fibre, via the equivalence between finite flat group schemes over $K$ and representations of $G_K$, corresponds to a Galois representation filtered by $\overline{\rho}\,|_{G_K}$; moreover, due to the restriction of $\rho$ from $G_{\mathbb{Q}_l}$ to $G_K$, the integral group scheme $\mathcal{G}[l^n]$ obtains descent data. Hence, instead of working with potentially Barsotti-Tate deformations, we may concern ourselves with the larger collection of deformations $\rho$ such that the Artinian quotients of $\rho\,|_{G_K}$ have finite flat group scheme (integral) models with the above properties: namely, a filtration of the geometric points by $\overline{\rho}\,|_{G_K}$, plus descent data.

Using the fact that $\mathcal{G}$ arises from a representation $\rho$ with Galois type $\tau$ and satisfying the determinant condition, one may use our explicit description of $WD(\rho)$ in the Barsotti-Tate case to compute relations which hold on th Dieudonné module of the generic fibre of $\mathcal{G}$. We may therefore require that these relations hold on the the Dieudonné modules of our finite flat group scheme models, reducing the size of the tangent space of $R'$ to be as small as needed while still maintaining a surjection $R' \twoheadrightarrow R(\overline{\rho}, 2, \tau)$

The task is therefore to identify suitable integral models for $\overline{\rho}\,|_{G_{\mathbb{Q}_l}}$ plus descent data which satisfy the desired Dieudonné module relations, and to compute the dimension of the tangent space of the deformation ring $R'$ using the corresponding Breuil modules. To show that the dimension of this tangent space is at most 1 requires computations which are long and complicated, but which we successfully complete in certain cases: namely, when $\overline{\rho}$ is a non-semisimple (and therefore reducible) representation over $\mathbb{F}_l$.

The reason we restrict to this special case is that to perform the desired computations when the residual representations is over $\mathbf{F}_{l^n}$, as opposed to representations over $\mathbb{F}_l$, one should probably work with Breuil modules *with coefficients*, i.e., with a theory of Breuil modules suited for working specifically with $\mathbf{F}_{l^n}$-vector-space schemes. Such a theory has been developed in [BCDT] for the simpler situation when $\mathbf{F}_{l^n}$ and the residue field of $K$ are linearly disjoint, which unfortunately is not the case in the computations we would need to do. This is a project we hope to attempt in the future. It is, of course, possible to have irreducible $\overline{\rho}$ over $\mathbb{F}_l$; however, since in this situation the characters of $\overline{\rho}\,|_{I_l}$ are of level 2, it is more natural to consider $\overline{\rho}$ over $\mathbb{F}_{l^2}$, and so we postpone consideration of this case as well.

1.3.2. *Conjectures of Breuil and Mézard.* Breuil and Mézard [BM00] have proposed an extension of the conjectures of Conrad, Diamond, and Taylor. A result of Henniart associates to each Galois type $\tau$ a unique $\overline{\mathbb{Q}}_l$-representation $\sigma(\tau)$ of $\mathrm{GL}_2(\mathbf{Z}_l)$. (We remark that the existence of $\sigma(\tau)$ is well-known; Henniart's contribution, in an appendix to [BM00], is the uniqueness.) Breuil and Mézard have a recipe for using $\sigma(\tau)$ to compute an "automorphic multiplicity"

$$\mu_{aut}(\overline{\rho}, k, \tau)$$

for $2 \leq k \leq l-1$. They conjecture ([BM00], 2.3.1.1) that when $\tau$ is tame, $\mu_{aut}(\overline{\rho}, k, \tau)$ is the same the "Galois multiplicity"

$$\mu_{Gal}(\overline{\rho}, k, \tau),$$

defined as the Samuel multiplicity of $R(\overline{\rho}, k, \tau)$. Breuil and Mézard provide a varient of this conjecture when $\tau$ has wild ramification. (Recall that the Samuel multiplicity

of a Noetherian local ring $(A, \mathfrak{m})$ is equal to $(\dim A)!$ times the leading coefficient of the polynomial (for $n$ sufficiently large) $\text{length}_A(A/\mathfrak{m}^n)$.)

Additional conjectures ([BM00], 2.2.2.3) regarding the structure of $R(\overline{\rho}, k, \tau)$ would imply that $\mu_{Gal}(\overline{\rho}, k, \tau) = 1$ if and only if $R(\overline{\rho}, k, \tau)_{\mathcal{O}} \cong \mathcal{O}[[X]]$, and so the conjectures of Breuil and Mézard generalize the conjectures of Conrad, Diamond, and Taylor. We also remark that in the terminology of [BCDT], $\tau$ *admits* $\overline{\rho}$ if and only if $\mu_{aut}(\overline{\rho}, 2, \tau) \geq 1$, while $\tau$ *simply admits* $\overline{\rho}$ if and only if $\mu_{aut}(\overline{\rho}, 2, \tau) = 1$. Thus, the conjectures of Breuil and Mézard also subsume Conjecture 1.3.1 of [BCDT]: that $\tau$ simply admits $\overline{\rho}$ if and only if $\tau$ is acceptable for $\overline{\rho}$.

Breuil and Mézard provide a proof of their conjecture in case $\tau$ is scalar and $k$ is even. (Notice that the conjectures from [CDT99] are a portion of the $k = 2$, $\tau$ non-scalar case of the Breuil-Mézard conjectures.) Breuil and Mézard use methods which are somewhat different from those of [BCDT], computing with Fontaine's weakly admissible filtered modules (the category of which is equivalent to the category of semi-stable representations [CF00]) as well as with Breuil's strongly divisible modules [Bre99b]. Moreover, they indicate that their methods should yield a proof of Conjecture 1.2.2 of [CDT99].

## 2. Main Results

We begin by recalling the following result, due to Wiles and Breuil-Conrad-Diamond-Taylor (Theorem 1.4.1 of [BCDT]):

**Theorem 2.1.** *Let $l$ be an odd prime, $K$ a finite extension of $\mathbb{Q}_l$ in $\overline{\mathbb{Q}}_l$, and $k$ the residue field of $K$. Let*

$$\rho : G_{\mathbb{Q}} \to \text{GL}_2(K)$$

*be an odd continuous representation ramified at only finitely many primes. Assume that its reduction*

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$$

*absolutely irreducible after restriction to* $\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}l})$*, and is modular. Further, suppose that*

- $\overline{\rho}\,|_{G_{\mathbb{Q}_l}}$ *has centralizer* $k$*,*
- $\rho\,|_{G_{\mathbb{Q}_l}}$ *is potentially Barsotti-Tate with* $l$*-type* $\tau$*,*
- $\tau$ *admits* $\overline{\rho}$*,*
- *and* $\tau$ *is weakly acceptable for* $\overline{\rho}$*.*

*Then* $\rho$ *is modular.*

We wish to prove the following special case of Conjecture 1.2.3 of [CDT99]:

**Theorem 2.2.** *Suppose that* $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$*, where* $m \in \mathbb{Z}/(l^2-1)\mathbb{Z}$ *and* $m = i+(l+1)j$ *with* $i = 1, \ldots, l$ *and* $j \in \mathbb{Z}/(l-1)\mathbb{Z}$*. Suppose also that* $\overline{\rho}\,|_{G_{\mathbb{Q}_l}} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbb{F}_l)$*, has centralizer* $\mathbb{F}_l$*, and is reducible. Then* $R(\overline{\rho}, 2, \tau) \neq (0)$ *only if* $\overline{\rho}\,|_{I_l}$ *is one of the following forms:*

- $\overline{\rho}|_{I_l} = \begin{pmatrix} \omega^{i+j} & * \\ 0 & \omega^{1+j} \end{pmatrix}$ *and if* $i = 2$*,* $*$ *is peu-ramifié,*
- $\overline{\rho}|_{I_l} = \begin{pmatrix} \omega^{1+j} & * \\ 0 & \omega^{i+j} \end{pmatrix}$ *and if* $i = l-1$*,* $*$ *is peu-ramifié.*

*In each of these cases,* $\tau$ *is weakly acceptable for* $\overline{\rho}$*.*

**Remark 2.3.** We have seen in section 1.2.1 that such $\overline{\rho}$ must be of the form $\begin{pmatrix} \omega^c\chi_a & * \\ 0 & \omega^d\chi_b \end{pmatrix}$ for some $c, d \in \mathbb{Z}/(l-1)\mathbb{Z}$ and $a, b \in \mathbb{F}_l^\times$. Since the result we wish

to establish considers only those $\overline{\rho}$ with trivial centralizer, we may assume that $* \neq 0$ and that $(a, c) \neq (b, d)$.

Combining 2.1 and 2.2, we obtain the following theorem:

**Theorem 2.4.** *Let $l$ be an odd prime, $K$ a finite extension of $\mathbb{Q}_l$ in $\overline{\mathbb{Q}}_l$, and $k$ the residue field of $K$. Let*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(K)$$

*be an odd continuous representation ramified at only finitely many primes. Assume that its reduction*

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$$

*is absolutely irreducible after restriction to $\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}l})$ and is modular. Further, suppose that*

- *$\overline{\rho}\,|_{G_{\mathbb{Q}_l}}$ is equivalent to a representation to $\mathrm{GL}_2(\mathbb{F}_l)$ which is reducible with centralizer $\mathbb{F}_l$,*
- *$\rho\,|_{G_{\mathbb{Q}_l}}$ is potentially Barsotti-Tate, and the associated Weil-Deligne representation $WD(\rho\,|_{G_{\mathbb{Q}_l}})$ is irreducible and tamely ramified.*

*Then $\rho$ is modular.*

*Proof.* If $\rho$ satisfies the given hypotheses, then by the results in section 1.2.2, the fact that $WD(\rho\,|_{G_{\mathbb{Q}_l}})$ is irreducible and tamely ramified implies that the $l$-type of $\rho$ is $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$ for some $m$ not divisible by $l+1$. The hypotheses on $\rho$ guarantee that $\overline{\rho}$ satisfies the conditions of Theorem 2.2, and the very existence of $\rho$ implies that $R(\overline{\rho}, 2, \tau) \neq (0)$. Hence $\tau$ is weakly acceptable for $\overline{\rho}$, and $\overline{\rho}$ is of one of the forms specified by Theorem 2.2. Once we see that our $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$ admits each of the two possibilities for $\overline{\rho}$, then by Theorem 2.1 we obtain that $\rho$ is modular.

To verify the admittance statement, one first checks that (in the notation of [CDT99] and [BCDT]) $\sigma_\tau \cong \Theta(\chi)$ where $\chi : \mathbb{F}_{l^2}^\times \to \overline{\mathbb{Q}}_l$ takes $c \mapsto c^{-m}$. (The reason for an exponent of $-m$ instead of an exponent of $m$ is the choice of normalization for the local Langlands correspondence in [CDT99]: namely, in Lemma 4.2.4(3) of [CDT99], we note that since $\eta_{l,2} = \tilde{\omega}_2^{-1}$, the character $\tilde{\omega}_2$ corresponds to $c \mapsto c^{-1}$.) Since $m = i+(l+1)j$ with $i \in \{1, \ldots, l\}$ and $j \in \mathbb{Z}/(l-1)\mathbb{Z}$, we may similarly write $-m = (l+1-i)+(l+1)(-1-j)$. By Lemma 3.1.1 of [CDT99], $\sigma_\tau \otimes \overline{\mathbb{F}}_l$ contains as Jordan-Hölder subquotients (again, in the notation of [BCDT]) the representation $\sigma_{l-1-i,-j}$ (if $i \neq l$) and $\sigma_{i-2,l-i-j}$ (if $i \neq 1$). From the defintions in section 1.3 of [BCDT], $\sigma_{l-1-i,-j}$ admits $\begin{pmatrix} \omega^{1+j} & * \\ 0 & \omega^{i+j} \end{pmatrix}$ with $*$ peu-ramifié if $i = l-1$, while $\sigma_{i-2,l-i-j}$ admits $\begin{pmatrix} \omega^{i+j} & * \\ 0 & \omega^{1+j} \end{pmatrix}$ with $*$ peu-ramifié if $i = 2$, as desired. □

**Remark 2.5.** A full proof of Conrad, Diamond, and Taylor's Conjecture 1.2.3 of [CDT99] (see section 1.3.1) would allow one to remove from theorem 2.4 the hypotheses that $\overline{\rho}$ is a representation over $\mathbb{F}_l$ (instead of $\overline{\mathbb{F}}_l$) and that $\overline{\rho}$ is reducible.

The remainder of this thesis is concerned with the proof of Theorem 2.2.

## 3. Deformation Theory

For the rest of this thesis, we fix $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, and the following notation. Let $\mathbb{Q}_{l^2}$ be the copy in $\overline{\mathbb{Q}}_l$ of the field of fractions of the Witt vectors $W(\mathbb{F}_{l^2})$, and $\pi$ is a choice of $(-l)^{\frac{1}{l^2-1}}$. Let $F = \mathbb{Q}_l(\pi)$, $F' = \mathbb{Q}_{l^2}(\pi)$. We are interested in the field $F$ because $\tau|_{I_F}$ is trivial, and so potentially semi-stable Galois representations with $l$-type $\tau$ become semi-stable over $F$. However, since $F/\mathbb{Q}_l$ is not Galois, we must typically work with its Galois closure $F'$.

We will regard an element $\zeta \in \mathbb{F}_{l^2}$ as an element in $W(\mathbb{F}_{l^2})$ (and hence in $\mathbb{Q}_{l^2}$) via the Teichmuller lifting map. Let $g_\zeta$ denote the element of $\mathrm{Gal}(F'/\mathbb{Q}_l)$ fixing $\mathbb{Q}_{l^2}$ and sending $\pi$ to $\zeta\pi$. Let $\varphi$ denote the element of $\mathrm{Gal}(F'/\mathbb{Q}_l)$ fixing $\pi$ and extending the nontrivial automorphism of $\mathbb{Q}_{l^2}$.

For any subfield $K$ of $\overline{\mathbb{Q}}_l$, we will let $K^{un}$ denote its maximal unramified extension. Finally, henceforth $\rho$ and $\overline{\rho}$ will denote representations of $G_{\mathbb{Q}_l}$ (so that we can avoid having to repeat the cumbersome $\rho\,|_{G_{\mathbb{Q}_l}}$.)

3.1. **Dieudonné module calculations.** Suppose $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(K)$ is a potentially Barsotti-Tate representation with $l$-type $\tau$ and with determinant

$$\det(\rho) = \epsilon \cdot \mathrm{Teich}(\omega^{-1} \det(\overline{\rho}))\,,$$

where Teich denotes the Teichmüller lift.

We now specialize the discussion of section 1.2.5 to our current situation. We know $\tau\,|_{I_{F'}}$ is trivial, and so $\rho$ becomes Barsotti-Tate when restricted to $G_{F'}$. Consequently, we obtain an $l$-divisible group $\Gamma$ over $\mathcal{O}_{F'}$ such that the Tate module of the generic fibre of $\Gamma$ is $\rho\,|_{G_{F'}}$. The field residue field of $E$ is $\mathbf{k} = \mathbb{F}_{l^2}$, the Witt vectors $W(\mathbf{k}) = \mathbb{Z}_{l^2}$, $\sigma$ is the Frobenius automorphism of $\mathbb{Z}_{l^2}$, the map $\overline{g}_\zeta$ is the identity for each $\zeta$, and the map $\overline{\varphi} = \sigma$.

We saw in section 1.2.5 (Proposition B.3.1 of [CDT99]) that

$$WD(\rho) \cong D'(\Gamma_{/\mathbb{F}_{l^2}}) \otimes_{\mathbb{Z}_{l^2} \otimes_{\mathbb{Z}_l} \mathcal{O}_K} \overline{\mathbb{Q}}_l,$$

where $g \in W_l$ acts on the right-hand side via $g\,|_{F'} \circ (\phi')^{-v(g)}$. In particular, $I_l$ acts via $I_l \twoheadrightarrow \mathrm{Gal}(F'/\mathbb{Q}_{l^2})$, and since $v(I_l) = 0$, no untwisting is needed.

Since $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$, there exist basis elements $\mathbf{v}, \mathbf{w}$ of $D'(\Gamma_{/\mathbb{F}_{l^2}}) \otimes_{\mathbb{Z}_{l^2} \otimes \mathbb{Z}_l} \mathcal{O}_K \ \overline{\mathbb{Q}}_l$ so that for $g \in I_l$,

$$g(\mathbf{v}) = \tilde{\omega}_2^m(g)\mathbf{v}$$

and

$$g(\mathbf{w}) = \tilde{\omega}_2^{lm}(g)\mathbf{w}.$$

For $\zeta \in \mathbb{F}_{l^2}$, by definition we have

$$\tilde{\omega}_2^m(g_\zeta) = (g_\zeta(\pi)/\pi)^m = \zeta^m\,,$$

and similarly $\tilde{\omega}_2^{lm}(g_\zeta) = \zeta^{lm}$. Thus $g_\zeta(\mathbf{v}) = \zeta^m\mathbf{v}$ and $g_\zeta(\mathbf{w}) = \zeta^{lm}\mathbf{w}$ . Similarly, we find $g_\zeta^l(\mathbf{v}) = \zeta^{lm}\mathbf{v}$ and $g_\zeta^l(\mathbf{w}) = \zeta^m\mathbf{w}$, from which we conclude that $g_\zeta + g_\zeta^l$ acts on $D'(\Gamma_{/\mathbb{F}_{l^2}}) \otimes_{\mathbb{Z}_{l^2} \otimes \mathbb{Z}_l} \mathcal{O}_K \ \overline{\mathbb{Q}}_l$ by scalar multiplication by $\zeta^m + \zeta^{lm}$, whereas $g_\zeta^{l+1}$ acts by scalar multiplication by $\zeta^{(l+1)m}$. (The action is linear, and not semilinear, since the image of $I_l \to \mathrm{Gal}(F'/\mathbb{Q}_{l^2})$ acts trivially on the coefficients $\mathbb{Z}_{l^2}$.)

We now wish to use the action $g_\zeta(f) = \overline{g}_\zeta \circ f \circ g_\zeta^{-1} = f \circ g_\zeta^{-1}$ on $D'(\Gamma_{/\mathbb{F}_{l^2}})$ to draw conclusions regarding the action of $g_\zeta$ on $D(\Gamma_{/\mathbb{F}_{l^2}})$.

Since $D'(\Gamma_{/\mathbb{F}_{l^2}})$ is a free module, the actions of $g_\zeta$ and $g_\zeta^l$ must sum and multiply on $D'(\Gamma_{/\mathbb{F}_{l^2}})$ to scalar multiplication by $\zeta^m + \zeta^{lm}$ and $\zeta^{(l+1)m}$ respectively. If $f \in D'(\Gamma_{/\mathbb{F}_{l^2}})$, we know

$$g_\zeta(f(x)) = f(g_\zeta^{-1}x)$$

with $x \in D(\Gamma_{/\mathbb{F}_{l^2}})$. It follows that

$$f((g_\zeta^{-1} + g_\zeta^{-l})x) = (g_\zeta + g_\zeta^l)f(x) = (\zeta^m + \zeta^{lm})f(x) = f((\zeta^m + \zeta^{lm})x).$$

By freeness, for any nonzero $x \in D(\Gamma_{/\mathbb{F}_{l^2}})$ we can find $f \in D'(\Gamma_{/\mathbb{F}_{l^2}})$ which does not vanish on $x$, so we conclude that $g_\zeta^{-1} + g_\zeta^{-l}$ acts as scalar multiplication by

$\zeta^m + \zeta^{lm}$ on $D(\Gamma_{/\mathbb{F}_{l^2}})$. Replacing $\zeta$ by $\zeta^{-1}$, we have found that

$$g_\zeta + g_\zeta^l \text{ acts as scalar multiplication by } \zeta^{-m} + \zeta^{-lm} \text{ on } D(\Gamma_{/\mathbb{F}_{l^2}}).$$

Similarly $g_\zeta^{l+1}$ acts as scalar multiplication by $\zeta^{-(l+1)m}$ on $D(\Gamma_{/\mathbb{F}_{l^2}})$.

We next wish to see what the determinant condition tells us about $D(\Gamma_{/\mathbb{F}_{l^2}})$. Recalling the two examples described in section 1.2.4, if $\chi_l$ denotes the 1-dimensional unramified character of $W_l$ sending arithmetic Frobenius to $l$, and if

$$\chi = \text{Teich}(\omega^{-1} \det(\overline{\rho})) \,|_{W_{\mathbb{Q}_l}} \otimes_K \overline{\mathbb{Q}}_l,$$

then since $WD$ is compatible with tensor products,

$$WD(\det(\rho)) = \chi_l \chi \,.$$

Let $s$ be any lift of $\varphi$ to $W_l$, so $s$ is a lift of arithmetic Frobenius but fixes $F$. Since $WD$ is compatible with the formation of exterior products, we know $\det(WD(\rho)) = WD(\det(\rho))$, and in particular $\det(WD(\rho)(s)) = lT$, where $T = \text{Teich}(\omega^{-1} \det(\overline{\rho}))(s) = \text{Teich}(\det(\overline{\rho}))(s)$. (We have $\omega(s) = 1$ since $s$ fixes $F$.) Note that $T$ depends only on $\overline{\rho}$, not on $\rho$ or the choice of $s$.

We claim that $\text{Trace}(WD(\rho)(s)) = 0$. Since

$$WD(\rho)\,|_{I_l} = \begin{pmatrix} \tilde{\omega}_2^m & 0 \\ 0 & \tilde{\omega}_2^{lm} \end{pmatrix}$$

and since for any $u \in I_l$ we have the relation $WD(\rho)(sus^{-1}) = WD(\rho)(u^l)$, it follows immediately that $WD(\rho)(s)$ must act via a matrix

$$\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}.$$

Therefore, we have shown that $WD(\rho)(s)$ satisfies the characteristic polynomial $X^2 + lT = 0$. By our characterization of $WD(\rho)$ in terms of $D'(\Gamma_{/\mathbb{F}_{l^2}})$, and since the latter is free, the action of $s$ on the latter must satisfy this same characteristic polynomial.

To understand the consequences for $D(\Gamma_{/\mathbb{F}_{l^2}})$, note that if $f \in D'(\Gamma_{/\mathbb{F}_{l^2}})[1/l]$ then

$$s(f)(x) = \varphi \circ (\phi')^{-1}(f)(x) = (\sigma(\sigma^{-1} \circ f \circ F) \circ \varphi)(x) = f(F \circ \varphi(x))$$

for $x \in D(\Gamma)$. Then

$$s^2(f)(x) = f(F^2 \circ [\varphi]^2(x)) = f(F^2(x)).$$

Since $s^2 + lT = 0$ on $D'(\Gamma_{/\mathbb{F}_{l^2}})$, we learn that

$$f((F^2 + lT)x) = 0$$

for all $x$ and $f$, and consequently $F^2 + lT = 0$ on $D(\Gamma_{/\mathbb{F}_{l^2}})$. Applying $V$ to both sides of this equation we see $F(FV) + lTV = lF + lTV = 0$, and since $D(\Gamma_{/\mathbb{F}_{l^2}})$ is free we obtain the relation

$$F + TV = 0$$

on $D(\Gamma_{/\mathbb{F}_{l^2}})$.

3.2. **Deformation problems.** Fix $\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbb{F}_l)$ a reducible Galois representation with centralizer $\mathbb{F}_l$, let $V$ denote the standard $\mathbb{F}_l$-vector space on which $G_{\mathbb{Q}_l}$ acts via $\overline{\rho}$, and let $T = \mathrm{Teich}(\det(\overline{\rho}))(\mathrm{Frob}_1)$.

We adopt the notation of section 4 of [BCDT] for group schemes: the pair $(\mathcal{G}, \{[g]\})$ consists of a group scheme $\mathcal{G}$ over $\mathcal{O}_{F'}$ and descent data $\{[g]\}_{g \in \mathrm{Gal}(F'/\mathbb{Q}_l)}$ from $F'$ to $\mathbb{Q}_l$. This is descent data in the sense of section 4 of [BCDT]: these

are maps $\mathcal{G} \to {}^g\mathcal{G}$ satisfying the usual compatibility conditions. This descent data does not necessarily descend $\mathcal{G}$, as $\mathcal{O}_{F'}/\mathbb{Z}_l$ is ramified; however, the base change of this descent data to the generic fibre is the standard sort of descent data, and we denote the descended group scheme by $(\mathcal{G}, \{[g]\})_{\mathbb{Q}_l}$.

We let $\mathcal{S}(\overline{\rho})$ denote the full category of the category of finite length discrete $\mathbb{Z}_l$-modules with $\mathbb{Z}_l$-linear action of $G_{\mathbb{Q}_l}$ consisting of objects which admit a finite filtration so that each graded piece is isomorphic to $V$. Let $\mathcal{S}$ be the full subcategory of $\mathcal{S}(\overline{\rho})$ consisting of objects $X$ for which there exists a finite flat $\mathcal{O}_{F'}$-group scheme $(\mathcal{G}, \{[g]\})$ with descent data to $\mathbb{Q}_l$ such that $X \cong (\mathcal{G}, \{[g]\})_{\mathbb{Q}_l}(\overline{\mathbb{Q}}_l)$ as $\mathbb{Z}_l[G_{\mathbb{Q}_l}]$-modules and such that $[\zeta]+[\zeta]^l-(\zeta^{-m}+\zeta^{-lm})$ and $[\zeta]^{l+1}-\zeta^{-(l+1)m}$ and $F+TV$ all annihilate the Dieudonné module $D(\mathcal{G} \times \mathbb{F}_{l^2})$.

From [BCDT], Lemma 4.1.3 it follows that $\mathcal{S}$ is closed under finite products, subobjects, and quotients. Following section 4.3 of [BCDT], define the set-valued functor $\mathcal{D}^{\mathcal{S}}_{V,\mathbb{Z}_l}$ on the category of complete Noetherian local $\mathbb{Z}_l$-algebras with finite residue field by letting $\mathcal{D}^{\mathcal{S}}_{V,\mathbb{Z}_l}(R)$ be the set of conjugacy classes of continuous representations such that $\rho \mod \mathfrak{m}_R$ is conjugate to $\overline{\rho}$ and such that for each open ideal $\mathfrak{a} \subset R$ the action $\rho$ makes $(R/\mathfrak{a})^2$ into an object of $\mathcal{S}$.

By a theorem of Ramakrishna [Ram93], if $\mathcal{D}^{\mathcal{S}}_{V,\mathbb{Z}_l}(\mathbb{F}_l)$ is nonempty, then the functor $\mathcal{D}^{\mathcal{S}}_{V,\mathbb{Z}_l}$ is representable; in this case, let $R^{\mathcal{S}}_{V,\mathbb{Z}_l}$ denote the resulting deformation ring. We have:

**Proposition 3.1.** *If $\mathcal{D}^{\mathcal{S}}_{V,\mathbb{Z}_l}(\mathbb{F}_l)$ is nonempty, then there is a surjection*

$$R^{\mathcal{S}}_{V,\mathbb{Z}_l} \twoheadrightarrow R(\overline{\rho}, 2, \tau)\,.$$

*Proof.* Let $R_V^{univ}$ denote the universal deformation ring for $\overline{\rho}$, and let

$$\mathcal{I} = \ker(R_V^{univ} \twoheadrightarrow R_{V,\mathbb{Z}_l}^{\mathcal{S}}).$$

It suffices to show

$$\mathcal{I} \subset \ker(R_V^{univ} \twoheadrightarrow R(\overline{\rho}, 2, \tau)) = \bigcap_{\mathfrak{p} \text{ type } \tau} \mathfrak{p} = \bigcap_{i \geq 1, \mathfrak{p} \text{ type } \tau} (\mathfrak{p}, l^i).$$

In other words, we need to show that each map $R_V^{univ} \twoheadrightarrow R_V^{univ}/(\mathfrak{p}, l^i)$ factors through $R_V^{univ} \twoheadrightarrow R_{V,\mathbb{Z}_l}^{\mathcal{S}}$. Let $\tilde{\rho}$ denote the representation arising from $R_V^{univ} \twoheadrightarrow R_V^{univ}/(\mathfrak{p}, l^i)$. Since $\mathfrak{p}$ has type $\tau$, there is an extension $K/\mathbb{Q}_l$ and an exact sequence $0 \to \mathfrak{p} \to R_V^{univ} \to K$ so that the resulting $\rho : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(K)$ is of type $\tau$. The results of section 3.1 produce an $l$-divisible group $\Gamma/\mathcal{O}_{F'}$ satisfying the desired relations on the Dieudonné module of its closed fibre and whose generic fibre representation is $\rho|_{G_{F'}}$. The $l^i$-torsion $\Gamma[l^i]$ is the desired finite flat group scheme with descent data which shows that the conjugacy class of $\tilde{\rho}$ is indeed in $\mathcal{D}_{V,\mathbb{Z}_l}^{\mathcal{S}}(R_V^{univ}/(\mathfrak{p}, l^i))$. □

**Corollary 3.2.** *If $\mathcal{D}_{V,\mathbb{Z}_l}^{\mathcal{S}}(\mathbb{F}_l)$ is nonempty, then the dimension of the tangent space of $R(\overline{\rho}, 2, \tau)$ is at most the dimension of the tangent space of $R_{V,\mathbb{Z}_l}^{\mathcal{S}}$.*

The rest of this article will be concerned with the proof of the following theorem:

**Theorem 3.3.** *If $R(\overline{\rho}, 2, \tau) \neq (0)$, then $\mathcal{D}_{V,\mathbb{Z}_l}^{\mathcal{S}}(\mathbb{F}_l)$ is nonempty. In this case, $\overline{\rho}|_{I_l}$ is of one of the two desired forms, and up to isomorphism there is exactly one finite flat group scheme $(\mathcal{G}, \{[g]\})$ over $\mathcal{O}_{F'}$ with descent data to $\mathbb{Q}_l$ such that $(\mathcal{G}, \{[g]\})_{\mathbb{Q}_l} \cong \overline{\rho}$ and such that $D(\mathcal{G} \times \mathbb{F}_{l^2})$ satisfies the relations described in section 3.1. Moreover, the space of extensions of $(\mathcal{G}, \{[g]\})$ by $(\mathcal{G}, \{[g]\})$ whose Dieudonné modules still satisfy the desired relations is 1-dimensional.*

This theorem evidently implies that if $R(\overline{\rho}, 2, \tau) \neq (0)$ then $R^{\mathcal{S}}_{V,\mathbb{Z}_l}$ exists and has a 1-dimensional tangent space, which completes the proof of Theorem 2.2.

3.3. **Strategy of the calculation.** If $R(\overline{\rho}, 2, \tau) \neq (0)$, then there exists a prime $\mathfrak{p}$ of type $\tau$. Hence there is a lift $\rho$ of $\overline{\rho}$ which arises from an $l$-divisible group $\Gamma$ over $\mathcal{O}_{F'}$ with descent data to $\mathbb{Q}_l$ and satisfying the desired relations on its Dieudonné module. Then the $l$-torsion $\Gamma[l]$ is filtered by models for $\overline{\rho}$ with descent data, so we see that $\mathcal{D}^{\mathcal{S}}_{V,\mathbb{Z}_l}(\mathbb{F}_l)$ is nonempty.

It remains: to determine all (reducible) $\overline{\rho}$ for which there exists a group scheme $(\mathcal{G}, \{[g]\})$ over $\mathcal{O}_{F'}$ with descent data to $\mathbb{Q}_l$ such that $(\mathcal{G}, \{[g]\})_{\mathbb{Q}_l} \cong \overline{\rho}$ and satisfying the necessary Dieudonné module relations; to show that when such a group scheme exists, there is exactly one of them; and, in this case, to compute the extensions described in Theorem 3.3.

Note that since $\overline{\rho}$ is reducible, any model for $\overline{\rho}|_{G_{F'}}$ is an extension of rank 1 group schemes, and by a scheme-theoretic closure argument (see Lemma 4.1.3 of [BCDT] or, for a classic reference, see [Ray74]), our descent data extends to descent data on the extension (i.e. on the subobject and quotient). We will use the theory of Breuil modules to classify such $\mathcal{O}_{F'}$-group schemes with descent data. (Any desired $\mathcal{G}$ is a model for $\overline{\rho}\,|_{G_{F'}}$, so $\mathcal{G}$ is killed by $l$, and therefore the theory of Breuil modules applies). Our analysis will proceed as follows. We compute all of the rank 1 Breuil modules corresponding to models of the relevant characters; we also take a moment to identify explicitly the group schemes corresponding to these rank 1 Breuil modules with descent data. We next classify all of their rank 2 extensions, and the descent data from $F'$ to $\mathbb{Q}_l$ which can be placed on these

extensions. Finally, we remove models from consideration based on our conditions on Dieudonné modules.

Once done with this, we will indeed see that the only $\overline{\rho}$ for which such group schemes exist are the desired ones, and that for each $\overline{\rho}$ the group schemes are unique (up to isomorphism). We then proceed with calculating the extensions of these group schemes by themselves, which completes the proof.

## 4. Review of Breuil Modules with Descent Data

We remind the reader that the prime $l$ is odd. Let $K/\mathbb{Q}_l$ be a finite extension, and suppose $K$ has integers $\mathcal{O}$, ramification index $e$, and residue field $\mathbf{k}$. Fix a uniformizer $\pi$ of $\mathcal{O}$. A Breuil module $(\mathcal{M}, \mathcal{M}_1, \phi_1)$ for $K$ consists of the following data:

- a finite-rank free $\mathbf{k}[u]/u^{el}$-module $\mathcal{M}$,
- a submodule $\mathcal{M}_1 \subset \mathcal{M}$ such that $\mathcal{M}_1 \supset u^e\mathcal{M}$, and
- an additive map $\phi_1 : \mathcal{M}_1 \to \mathcal{M}$ such that $\phi_1(hv) = h^l\phi_1(v)$ for any $h \in \mathbf{k}[u]/u^{el}$ and $v \in \mathcal{M}_1$, and such that the $\mathbf{k}[u]/u^{el}$-span of $\phi_1(\mathcal{M}_1)$ is all of $\mathcal{M}$.

Morphisms of Breuil modules preserve $\mathcal{M}_1$ and commute with $\phi_1$.

C. Breuil [Bre00, Bre98] has proved the following remarkable theorem:

**Theorem 4.1.** *There is an (additive) contravariant equivalence of categories, depending heavily on the choice of uniformizer $\pi$, between the category of Breuil modules for $K$ and the category of finite flat group schemes over $\mathcal{O}$ which are killed by $l$. The rank of the Breuil module is the same as the rank of the corresponding group scheme.*

The Breuil module functor has numerous useful properties: for example, a short exact sequence of group schemes corresponds to a short exact sequence of Breuil modules, and a sequence of Breuil modules is short-exact if and only if the sequence of underlying $\mathbf{k}[u]/u^{el}$-modules is short-exact. ([BCDT], Lemma 5.1.1.) This will allow us directly to compute Exts of Breuil modules.

**Example:** ([BCDT], Example 5.2) It is an informative exercise to check that the rank 1 Breuil modules are of the form:

$$\mathcal{M} = (\mathbf{k}[u]/u^{el})\mathbf{e}\,,$$

$$\mathcal{M}_1 = (\mathbf{k}[u]/u^{el})u^r\mathbf{e}\,,$$

$$\phi_1(u^r\mathbf{e}) = a\mathbf{e}$$

with $0 \leq r \leq e$ and $a \in \mathbf{k}^\times$. We will denote this module as $\mathcal{M}(r,a)$. We recommend that the reader verify that a homomorphism $\mathcal{M}(r,a) \to \mathcal{M}(r_1,a_1)$ exists if and only if $r_1 \geq r$, $r_1 \equiv r \pmod{l-1}$, and $a/a_1 \in (\mathbf{k}^\times)^{l-1}$, and is always given by $\mathbf{e} \mapsto bu^{l(r_1-r)/(l-1)}\mathbf{e}_1$ where $b^{l-1} = a/a_1$.

There is a very useful compatibility between Breuil theory and contravariant Dieudonné theory. Let

$$u^e - lG_\pi(u)$$

be the minimal polynomial of $\pi$ over $W(\mathbf{k})$, and let $c_\pi = -G_\pi(u)^l \in \mathbf{k}[u]/u^{el}$. On any Breuil module, define $\phi : \mathcal{M} \to \mathcal{M}$ via

$$\phi(v) = \frac{1}{c_\pi}\phi_1(u^e v).$$

Note that $u^e v \in \mathcal{M}_1$ by definition. Then ([BCDT], Theorem 5.1.3(3)) if $\mathcal{M}_\pi$ is the Breuil module corresponding to the group scheme $\mathcal{G}$ (with $\pi$ as our fixed

uniformizer), there is a canonical $\mathbf{k}$-linear isomorphism

$$D(\mathcal{G}) \otimes_{\mathbf{k},\mathrm{Frob}_l} \mathbf{k} \cong \mathcal{M}_\pi / u\mathcal{M}_\pi$$

under which $F \otimes \mathrm{Frob}_l$ corresponds to $\phi$ and $V \otimes \mathrm{Frob}_l^{-1}$ corresponds to the composition

$$\mathcal{M}/u\mathcal{M} \xrightarrow{\phi_1^{-1}} \mathcal{M}_1/u\mathcal{M}_1 \to \mathcal{M}/u\mathcal{M}\,.$$

Finally, a group scheme with descent data $(\mathcal{G}, \{[g]\})$ corresponds to a Breuil module with descent data. In the case where $K'/K$ a is tamely ramified Galois extension and the uniformizer $\pi$ of $K'$ satisfies $\pi^e \in K$, the description of descent data is fairly simple. (In the wild case, it is decidedly not.) The following description is essentially a transcription from an unpublished preprint of B. Conrad [Con]:

**Theorem 4.2.** *If $K'/K$ is tamely ramified and $\pi^e \in K$, then giving descent data on $(\mathcal{M}, \mathcal{M}_1, \phi_1)$ is equivalent to giving, for each $g \in \mathrm{Gal}(K'/K)$, an additive bijections $[g] : \mathcal{M} \mapsto \mathcal{M}$ satisfying:*

- *each $[g]$ preserves $\mathcal{M}_1$ and commutes with $\phi_1$,*
- *$[1]$ is the identity and $[g][h] = [gh]$, and*
- *$g(au^i v) = g(a)(zu)^i g(v)$, where $g(\pi) = z\pi$ and $a \in \mathbf{k}'$ is regarded as being in $K'$ via the Teichmüller lift.*

An extension of Breuil modules with descent data means the obvious thing: namely, we want the extension to have descent data which restricts and projects, respectively, to the given descent data on the specified submodule and quotient.

For any further facts about Breuil modules which may be necessary, the reader can refer to section 5 of [BCDT]. We now begin the computations needed for the proof of theorem 3.3.

## 5. Rank 1 Modules

We describe the rank 1 Breuil modules corresponding to group schemes over $\mathcal{O}_{F'}$ using $\pi$ as our uniformizer, and we find those which can obtain descent data from $F'$ to $\mathbb{Q}_l$. Since the ramification index $e(F') = l^2 - 1$ and the residue field of $F'$ is $\mathbb{F}_{l^2}$, these are rank 1 modules over $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ with a filtered $\phi_1$-module structure. As explained in the previous section, we find that all of these rank 1 Breuil modules are isomorphic to (at least) one of the form $\mathcal{M}(r, a)$, that is, of the form

$$\mathcal{M} = \langle \mathbf{e} \rangle, \quad \mathcal{M}_1 = \langle u^r \mathbf{e} \rangle, \quad \phi_1(u^r \mathbf{e}) = a\mathbf{e}$$

with $0 \leq r \leq l^2 - 1$ and $a \in \mathbb{F}_{l^2}^\times$. Moreover, $\mathcal{M}(r, a) \cong \mathcal{M}(r, a')$ if and only if $a/a' \in (\mathbb{F}_{l^2}^\times)^{l-1}$.

Before applying descent data to these Breuil modules, we recall the Galois theory of $F'/\mathbb{Q}_l$: we have fixed $g_\zeta \in \mathrm{Gal}(F'/\mathbb{Q}_{l^2})$ sending $\pi \to \zeta\pi$, and $\varphi$ is the extension of $\mathrm{Gal}(\mathbb{Q}_{l^2}/\mathbb{Q}_l)$ fixing $\pi$. Then $\mathrm{Gal}(F'/\mathbb{Q}_l)$ is generated by $\varphi$ and the $g_\zeta$, subject to the relations $g_\zeta^{l^2-1} = 1$ and $\varphi g_\zeta \varphi = g_\zeta^l$ for all $\zeta \in \mathbb{F}_{l^2}$. Since $\pi$ is a choice of $(-l)^{1/(l^2-1)}$, in the notation of section 4 we have $G_\pi = -1$, $c_\pi = 1$, and $\phi(v) = \phi_1(u^e v)$ for $v \in \mathcal{M}$.

Since $F'/\mathbb{Q}_l$ is tamely ramified and $\pi^e = -l \in \mathbb{Q}_l$, we conclude from our description in the previous section that to give descent data from $F'/\mathbb{Q}_l$ on a Breuil module for $F'$ is to give an additive bijection $[\zeta] : \mathcal{M} \to \mathcal{M}$ for each $g_\zeta \in \mathrm{Gal}(F'/\mathbb{Q}_{l^2})$ and an additive bijection $[\varphi] : \mathcal{M} \to \mathcal{M}$, all sending $\mathcal{M}_1 \to \mathcal{M}_1$ and satisfying the following compatibilities:

(1) $[\zeta_1] \circ [\zeta_2] = [\zeta_1\zeta_2]$,

(2) $[\zeta] \circ \phi_1 = \phi_1 \circ [\zeta]$ and $[\varphi] \circ \phi_1 = \phi_1 \circ [\varphi]$ on $\mathcal{M}_1$,

(3) $[\zeta](au^i m) = a(\zeta u)^i[\zeta](m)$ for $a \in \mathbb{F}_{l^2}$ and $m \in \mathcal{M}$,

(4) $[\varphi](au^i m) = a^l u^i[\varphi](m)$ for $a \in \mathbb{F}_{l^2}$ and $m \in \mathcal{M}$, and

(5) $[\varphi][\zeta][\varphi] = [\zeta]^l$.

(Here, we have made the observation that $\zeta$ acts trivially on $\mathbb{F}_{l^2}$, while $\varphi$ acts as Frobenius.) The following theorem gives a complete list of these desired Breuil modules with descent data:

**Proposition 5.1.** *In the category of Breuil modules corresponding to group schemes over $\mathcal{O}_{F'}$ and with $\pi$ as our choice of uniformizer, a rank 1 Breuil module $\mathcal{M}(r,a)$ can obtain descent data from $F'$ to $\mathbb{Q}_l$ if and only if $r$ is divisible by $l-1$ and $a \in (\mathbb{F}_{l^2}^\times)^2$. Furthermore, any such Breuil module with descent data is isomorphic to exactly one of the following form: $\mathcal{M} = \mathcal{M}(r,a')$ with $a' \in \mathbb{F}_l^\times$, and descent data given by choosing an element $c \in \mathbb{Z}/(l-1)\mathbb{Z}$ and setting $[\varphi](\mathbf{e}) = \mathbf{e}$ and*

$$[\zeta](\mathbf{e}) = \zeta^{(l+1)c - lr'}\mathbf{e}$$

*with $r = (l-1)r'$.*

*Proof.* First, we compute the allowable actions of the subgroup $\langle[\zeta]\rangle$. To do this, it is enough to select a system of $A_\zeta \in (\mathbb{F}_{l^2}[u]/u^{l(l^2-1)})^\times$, set $[\zeta](\mathbf{e}) = A_\zeta\mathbf{e}$ (extending to all of $\mathcal{M}$ via property (3) above), and to decide which systems of $A_\zeta$ satisfy the above relations.

To begin with, by the above property (2) of descent data, we require $\phi_1 \circ [\zeta](u^r\mathbf{e}) = [\zeta] \circ \phi_1(u^r\mathbf{e})$. Evaluating the left-hand side yields

$$\phi_1 \circ [\zeta](u^r\mathbf{e}) = \phi_1(A_\zeta\zeta^r u^r\mathbf{e}) = (A_\zeta\zeta^r)^l a\mathbf{e},$$

whereas evaluating the right-hand side yields

$$[\zeta] \circ \phi_1(u^r \mathbf{e}) = [\zeta](a\mathbf{e}) = A_\zeta a \mathbf{e}.$$

Hence

$$A_\zeta^{l-1} = \zeta^{-lr},$$

from which we conclude that $A_\zeta \in \mathbb{F}_{l^2}^\times$. (Note that we automatically have $[\zeta]^{l^2-1} = [1]$. If our Breuil modules had $\overline{\mathbb{F}}_l$-coefficients, then above we would only have been able to conclude $A_\zeta \in \overline{\mathbb{F}}_l^\times$, and we would now use the relation $[\zeta]^{l^2-1} = [1]$ to prove that $A_\zeta$ is actually in $\mathbb{F}_{l^2}$.)

For the moment choosing $\zeta$ to be a generator for $\mathbb{F}_{l^2}^\times$, an examination of the equation $A_\zeta^{l-1} = \zeta^{-lr}$ reveals that we need $r$ divisible by $l-1$ if we are to have $A_\zeta \in \mathbb{F}_{l^2}^\times$. Write $r = (l-1)r'$. For any $\zeta$ we then obtain

$$A_\zeta \in \zeta^{-lr'} \mathbb{F}_l^\times.$$

Since the map $\zeta \mapsto A_\zeta$ must be multiplicative, it follows easily that $A_\zeta$ has the form $\zeta^{(l+1)c-lr'}$ for some $c$.

Now we must study the compatibility of this action with potential actions of $[\varphi]$. Suppose $[\varphi](\mathbf{e}) = A_\varphi \mathbf{e}$. We must have $[\varphi] \circ \phi_1(u^r \mathbf{e}) = \phi_1 \circ [\varphi](u^r \mathbf{e})$. This time the left-hand side evaluates to $a^l A_\varphi \mathbf{e}$, while the right-hand side evaluates to $a A_\varphi^l \mathbf{e}$, and so

$$A_\varphi^{l-1} = a^{l-1}.$$

It follows that $A_\varphi$ is a scalar, and in fact that it is contained in $a\mathbb{F}_l^\times$. Moreover,

$$\begin{aligned}[\varphi][\zeta][\varphi](\mathbf{e}) &= [\varphi][\zeta](A_\varphi \mathbf{e}) \\ &= [\varphi](A_\varphi \zeta^{(l+1)c-lr'}\mathbf{e}) \\ &= A_\varphi^{l+1}(\zeta^{(l+1)c-lr'})^l \mathbf{e}\,,\end{aligned}$$

and this equals $[\zeta]^l(\mathbf{e})$ precisely when $A_\varphi^{l+1} = 1$. From this, we obtain that $A_\varphi$ is a square in $\mathbb{F}_{l^2}^\times$, and since $A_\varphi \in a\mathbb{F}_l^\times$ it follows that $a$ is also a square. One checks with ease that if $a$ is in fact a square, then $A_\varphi = \pm a^{(l-1)/2}$ are the only remaining possibilities, and in fact that both of these choices yield valid descent data.

Replacing $\mathbf{e}$ as basis vector by $b\mathbf{e}$ replaces $a$ by $b^{l-1}a$, and since $[\varphi](b\mathbf{e}) = b^{l-1}A_\varphi(b\mathbf{e})$ it also replaces $A_\varphi$ by $b^{l-1}A_\varphi$. To prove the proposition, it therefore remains to check that there is exactly one $a' \in \mathbb{F}_l^\times$ such that $a'/a \in (\mathbb{F}_{l^2}^\times)^{l-1}$ and $A_\varphi a' = a$. Uniqueness is evident from the latter equality. Since $A_\varphi$ is in both $(\mathbb{F}_{l^2}^\times)^{l-1}$ and $a\mathbb{F}_l$, existence follows.

□

For the remainder of this document, we fix the notation $r = (l-1)r'$ and $s = (l-1)s'$. Moreover, $\mathcal{M}(r,a,c)$ will always denote the Breuil module $\mathcal{M}(r,a)$ with $a \in \mathbb{F}_l^\times$ and carrying the descent data $[\zeta](\mathbf{e}) = \zeta^{(l+1)c-lr'}\mathbf{e}$, $[\varphi](\mathbf{e}) = \mathbf{e}$. Define $\mathcal{M}(s,b,d)$ analogously. We will always let $\mathbf{e}$ and $\acute{\mathbf{e}}$ denote the standard basis elements of $\mathcal{M}(s,b,d)$ and $\mathcal{M}(r,a,c)$ respectively.

## 6. Identification of Rank 1 Breuil Modules

We now sketch an argument which identifies the Breuil modules with descent data from the preceeding section, in the following sense: given $\mathcal{M}(r,a,c)$, this

corresponds to a finite flat group scheme $\mathcal{G}(r,a,c)$ over $\mathcal{O}_{F'}$ with descent data, and we wish to determine the finite flat group scheme $\mathcal{G}_{\mathbb{Q}_l}(r,a,c)$ over $\mathbb{Q}_l$ to which the generic fibre $\mathcal{G}_{/F'}(r,a,c)$ descends. Equivalently, we will compute the character $\chi(r,a,c) : G_{\mathbb{Q}_l} \to \mathbb{F}_l^\times$ obtained as the Galois representation on $\mathcal{G}_{\mathbb{Q}_l}(r,a,c)(\overline{\mathbb{Q}}_l)$.

To begin, we note:

**Lemma 6.1.** *There exists a non-zero homomorphism from $\mathcal{M}(r,a,c)$ to $\mathcal{M}(s,b,d)$ if and only if $r \leq s$, $a = b$, and $c = d$.*

*Proof.* Ignoring descent data for the moment, the descent-dataless analogue of this lemma (e.g. part 2 of Lemma 5.2.1 in [BCDT]) states that we have a non-zero map from $\mathcal{M}(r,a)$ to $\mathcal{M}(s,b)$ if and only if $r \leq s$ and $a = b$, and moreover all such maps are of the form $\mathbf{\acute{e}} \mapsto \alpha u^{l(s'-r')}\mathbf{e}$ for $\alpha \in \mathbb{F}_l^\times$. These maps are compatible with descent data exactly when

$$\zeta^{(l+1)d-ls'}\alpha(\zeta u)^{l(s'-r')}\mathbf{e} = \alpha u^{l(s'-r')}\zeta^{(l+1)c-lr'}\mathbf{e},$$

i.e. if and only if $c = d$. □

**Corollary 6.2.** *$\chi(r,a,c)$ is independent of $r$.*

*Proof.* The non-zero map $\mathcal{M}(0,a,c) \to \mathcal{M}(r,a,c)$ corresponds to a non-zero map $\mathcal{G}(r,a,c) \to \mathcal{G}(0,a,c)$ compatible with descent data, so we get a non-zero map $\mathcal{G}_{\mathbb{Q}_l}(r,a,c) \to \mathcal{G}_{\mathbb{Q}_l}(0,a,c)$. This amounts to a non-zero map of Galois modules of order $l$, so is therefore an isomorphism, and we find $\chi(r,a,c) = \chi(0,a,c)$. □

**Theorem 6.3.** *$\chi(r,a,c) = \omega^{1-c}\chi_a$.*

*Proof.* By the above considerations, it suffices to verify the theorem for $r = l^2 - 1$, i.e. for $\mathcal{M}(l^2-1, a)$ for which $[\zeta]$ acts on $\mathcal{M}/u$ via multiplication by $\zeta^{(l+1)c-l(l+1)} = \zeta^{(l+1)(c-1)}$.

Using part 2 of Theorem 5.6.1 of [BCDT], we compute that $D([\zeta])$ is the multiplication-by-$\zeta^{(l+1)(c-1)}$ endomorphism of the Dieudonné module $D(\mathcal{G}(l^2-1, a, c) \times_{F'} \mathbb{F}_{l^2})$. Since $\zeta^{(l+1)(c-1)} \in \mathbb{F}_l$, there is an integer $n$ such that $D([\zeta]) = \mathrm{Id} + \cdots + \mathrm{Id}$ (where there are $n$ Id's in the sum). As the Dieudonné functor is additive, it follows that the corresponding action of $[\zeta]$ on $\mathcal{G}(l^2-1, a, c) \times_{F'} \mathbb{F}_{l^2}$ is also multiplication by $n$. By 3.1.2 of [Bre00], the affine algebra of $\mathcal{G}(l^2-1, a, c)$ is $\mathcal{O}_{F'}[X]/(X^l - aX)$, where again $a \in \mathbb{F}_l$ is identified with its Teichmuller lift. We see without difficulty that the multiplication-by-$n$ endomorphism on $\mathbb{F}_{l^2}[X]/(X^l - aX)$ is exactly $X \mapsto \zeta^{(l+1)(c-1)}X$. The action of $[\zeta]$ on $\mathcal{G}(l^2-1, a, c)$ fits in the commutative diagram

$$\begin{array}{ccc} \mathcal{G}(l^2-1,a,c) & \xrightarrow{[\zeta]} & \mathcal{G}(l^2-1,a,c) \\ \downarrow & & \downarrow \\ \mathrm{Spec}\ \mathcal{O}_{F'} & \xrightarrow[\zeta]{} & \mathrm{Spec}\ \mathcal{O}_{F'} \end{array}$$

and on the closed fibre sends $X \mapsto \zeta^{(l+1)(c-1)}X$; it follows that if $\psi$ is the homomorphism from $\mathcal{O}_{F'}[X]/(X^l - aX)$ to itself sending $X$ to $\zeta^{(l+1)(c-1)}X$ and $f \in F'$ to $\zeta(f)$ (with $\zeta$ in this context being the element of the Galois group), then $(\mathrm{Spec}\ \psi)^{-1}[\zeta]$ is an $\mathcal{O}_{F'}$-group scheme endomorphism of $\mathcal{G}(l^2-1, a, c)$ which is trivial on the closed fibre, hence is easily seen to be the identity. (For example, one may use Breuil modules to compute directly that $\mathrm{End}\ \mathcal{G}(l^2-1, a, c) \cong \mathbb{Z}/l\mathbb{Z}$ and hence injects into the endomorphisms of the closed fibre.)

Similarly, we find that $D([\varphi])$ coincides with $(1/a)F$ on $D(\mathcal{G}(l^2-1,a,c)\times_{F'}\mathbb{F}_{l^2})$. On $\mathbb{F}_{l^2}[X]/(X^l-aX)$, this translates into $[\varphi](X)=(1/a)X^l=(1/a)(aX)=X$ and $[\varphi](f)=f^l$ if $f\in\mathbb{F}_{l^2}$; just as for $[\zeta]$, we can compute that $[\varphi]:F'[X]/(X^l-aX)\to F'[X]/(X^l-aX)$ is the map which fixes $X$ and sends $f\in F'$ to $\varphi(f)$.

Having completely identified the descent data on $\mathcal{G}(l^2-1,a,c)$, we will now show that the affine algebra of $\mathcal{G}_{\mathbb{Q}_l}(l^2-1,a,c)$ is $\mathbb{Q}_l[X]/(X^l-a(-l)^{1-c}X)$. To achieve this, we simply base change this algebra from $\mathbb{Q}_l$ to $F'$ and check that the resulting descent data coincides with the descent data we have already computed. Noting that we have an isomorphism $F'[X]/(X^l-a(-l)^{1-c}X)\to F'[X]/(X^l-aX)$ sending $X\mapsto\pi^{(l+1)(1-c)}X$, we are asking, for each $g\in\mathrm{Gal}(F'/\mathbb{Q}_l)$, for the commutativity of the diagram:

$$\begin{array}{ccc} F'[X]/(X^l-a(-l)^{1-c}X) & \longrightarrow & F'[X]/(X^l-aX) \\ {\scriptstyle X\mapsto X}\downarrow & & \downarrow{\scriptstyle [g]} \\ F'[X]/(X^l-a(-l)^{1-c}X) & \longrightarrow & F'[X]/(X^l-aX) \end{array}$$

where the horizontal maps are $F'$-linear sending $X\mapsto\pi^{(l+1)(1-c)}X$, and the vertical maps are $g$-semilinear. For $g=\zeta$, mapping first horizontally and then vertically we find

$$X\mapsto\pi^{(l+1)(1-c)}X\mapsto(\zeta\pi)^{(l+1)(1-c)}\zeta^{(l+1)(c-1)}X=\pi^{(l+1)(1-c)}X$$

as desired, and for $\varphi$ the verification is even easier.

Finally, one can check without difficulty that the representation on the $\overline{\mathbb{Q}}_l$-points of $\mathbb{Q}_l[X]/(X^l-a(-l)^{1-c}X)$ is indeed $\omega^{1-c}\chi_a$.

□

## 7. Rank 2 Extensions of Rank 1 Modules

In this section, we classify the extensions with descent data of the rank 1 modules in the previous section by one another. The extensions without descent data are classified in Lemma 5.2.2 of [BCDT], which specializes to our situation as follows:

**Lemma 7.1.** *In the category of Breuil modules corresponding to finite flat $l$-torsion group schemes over $\mathcal{O}_{F'}$ with choice of uniformizer $\pi$, we have an isomorphism*

$$\mathrm{Ext}^1(\mathcal{M}(r,a),\mathcal{M}(s,b)) \cong \{h \in u^{\max(0,r+s-(l^2-1))}\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}\}/\{u^s t - (b/a)u^r t^l\}$$

*given by associating to each $h \in u^{\max(0,r+s-(l^2-1))}\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ the $\phi_1$-module*

$$\mathcal{M} = \langle \mathbf{e}, \mathbf{e}' \rangle,\ \mathcal{M}_1 = \langle u^s \mathbf{e}, u^r \mathbf{e}' + h\mathbf{e} \rangle,$$

*with*

$$\phi_1(u^s \mathbf{e}) = b\mathbf{e},\ \phi_1(u^r \mathbf{e}' + h\mathbf{e}) = a\mathbf{e}'.$$

*Moreover, the transformation $\mathbf{e}' \mapsto \mathbf{e}' - (b/a)t^l\mathbf{e}$ gives the equivalence between the extension classes associated to $h$ and to $h + (u^s t - (b/a)u^r t^l)$.*

We now wish to impose descent data on the above extensions, extending the descent data on both sides of the extension; that is, the descent data must act as usual on the subobject $\mathcal{M}(s'(l-1), b, d)$ and must reduce modulo $\mathcal{M}(s'(l-1), b, d)$ to the usual descent data on $\mathcal{M}(r'(l-1), a, c)$. In particular, the subgroup $\langle [\zeta] \rangle$ must act on

$$\mathcal{M} = \langle \mathbf{e}, \mathbf{e}' \rangle,\ \mathcal{M}_1 = \langle u^{s'(l-1)} \mathbf{e}, u^{r'(l-1)} \mathbf{e}' + h\mathbf{e} \rangle$$

via descent data of the form

$$[\zeta](\mathbf{e}) = \zeta^{(l+1)d - ls'} \mathbf{e},\ [\zeta](\mathbf{e}') = \zeta^{(l+1)c - lr'} \mathbf{e}' + A_\zeta \mathbf{e}.$$

We wish to show that $A_\zeta$ may be taken to be 0 by an appropriate change of variables $\mathbf{e}' \mapsto \mathbf{e}' - (b/a)t^l\mathbf{e}$, to determine for which choices of $h$, $r'$, $s'$, $a$, $b$, $c$, and $d$ this is actually valid descent data, and to exhaust whatever degrees of freedom in $\mathbf{e}'$ may be remaining by finding a canonical choice for $h$.

We begin, as we did in the one-dimensional case, with an analysis of the fact that descent data must commute with $\phi_1$. This amounts to checking the relations imposed by applying these maps to $u^{r'(l-1)}\mathbf{e}' + h\mathbf{e}$. First,

$$[\zeta] \circ \phi_1(u^{r'(l-1)}\mathbf{e}' + h\mathbf{e}) = [\zeta](a\mathbf{e}') = a\zeta^{(l+1)c-lr'}\mathbf{e}' + aA_\zeta\mathbf{e}.$$

To compute $\phi_1 \circ [\zeta](u^{r'(l-1)}\mathbf{e}' + h\mathbf{e})$, let $h'$ be the the polynomial with $h'(u) = h(\zeta u)$, and we compute

$$\begin{aligned}
[\zeta](u^{r'(l-1)}\mathbf{e}' + h\mathbf{e}) &= (\zeta u)^{r'(l-1)}(\zeta^{(l+1)c-lr'}\mathbf{e}' + A_\zeta\mathbf{e}) + h'\zeta^{(l+1)d-ls'}\mathbf{e} \\
&= \zeta^{r'(l-1)+(l+1)c-lr'}(u^{r'(l-1)}\mathbf{e}' + h\mathbf{e}) \\
&\quad + (h'\zeta^{(l+1)d-ls'} - h\zeta^{(l+1)c-r'} + \zeta^{r'(l-1)}A_\zeta u^{r'(l-1)})\mathbf{e}.
\end{aligned}$$

The latter must be an element of $\mathcal{M}_1$, from which we conclude

$$u^{s'(l-1)} \mid h'\zeta^{(l+1)d-ls'} - h\zeta^{(l+1)c-r'} + \zeta^{r'(l-1)}A_\zeta u^{r'(l-1)}.$$

Writing the right-hand side as $u^{s'(l-1)}\Delta_\zeta$, we compute

$$\phi_1 \circ [\zeta](u^{r'(l-1)}\mathbf{e}' + h\mathbf{e}) = a\zeta^{l(r'(l-1)+(l+1)c-lr')}\mathbf{e}' + b\Delta_\zeta^l\mathbf{e} = a\zeta^{(l+1)c-lr'}\mathbf{e}' + b\Delta_\zeta^l\mathbf{e}.$$

Matching up coordinates with our calculation for $[\zeta] \circ \phi_1(u^{r'(l-1)}\mathbf{e}' + h\mathbf{e})$, we obtain the equality

$$b\Delta_\zeta^l = aA_\zeta.$$

We continue with an analysis of $A_\zeta$ and the effect on $A_\zeta$ of changing $\mathbf{e}'$.

**Lemma 7.2.** *There exists a polynomial $f(u) \in \mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ such that, for each $\zeta$, $A_\zeta = \zeta^{(l+1)d-ls'} f(\zeta u) - \zeta^{(l+1)c-lr'} f(u)$.*

*Proof.* Observe that

$$\begin{aligned}[\zeta_2][\zeta_1]\mathbf{e}' &= [\zeta_2](\zeta_1^{(l+1)c-lr'}\mathbf{e}' + A_{\zeta_1}\mathbf{e}) \\ &= \zeta_1^{(l+1)c-lr'}(\zeta_2^{(l+1)c-lr'}\mathbf{e}' + A_{\zeta_2}\mathbf{e}) + A'_{\zeta_1}\zeta_2^{(l+1)d-ls'}\mathbf{e}\end{aligned}$$

where $A'_{\zeta_1}$ is the polynomial in $u$ given by $A'_{\zeta_1}(u) = A_{\zeta_1}(\zeta_2 u)$. Matching coefficients with $[\zeta_1\zeta_2]\mathbf{e}'$, we see that

$$A_{\zeta_1\zeta_2} = \zeta_1^{(l+1)c-lr'} A_{\zeta_2} + \zeta_2^{(l+1)d-ls'} A'_{\zeta_1}\,.$$

Dividing both sides by $(\zeta_1\zeta_2)^{(l+1)c-lr'}$, this transforms to

$$\frac{A_{\zeta_1\zeta_2}}{(\zeta_1\zeta_2)^{(l+1)c-lr'}} = \frac{A_{\zeta_2}}{\zeta_2^{(l+1)c-lr'}} + \zeta_2^{(l+1)(d-c)-l(s'-r')}\frac{A'_{\zeta_1}}{\zeta_1^{(l+1)c-lr'}}$$

from which we see that the map $\zeta \mapsto A_\zeta/\zeta^{(l+1)c-lr'}$ is a cocycle in the group cohomology $H^1(\mathbb{F}_{l^2}^\times, \mathbb{F}_{l^2}[u]/u^{l(l^2-1)})$, where $\mathbb{F}_{l^2}^\times$ acts on $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ via $\zeta \cdot f(u) = \zeta^{(l+1)(d-c)-l(s'-r')} f(\zeta u)$. Since this cohomology group is trivial (as $\mathbb{F}_{l^2}^\times$ has order $l^2-1$ and $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ is $l$-torsion), we see that $\zeta \mapsto A_\zeta/\zeta^{(l+1)c-lr'}$ is actually a coboundary, and any polynomial $f(u)$ of which our cocycle is a coboundary will satisfy the conditions of the lemma. □

We remark that if $A_\zeta = 0$ for $\zeta$ a primitive root in $\mathbb{F}_{l^2}$, then $A_\zeta = 0$ for all $\zeta \in \mathbb{F}_{l^2}$, so we may use the equation $A_\zeta = 0$ unambiguously to denote either.

**Lemma 7.3.** *Transforming $\mathbf{e}' \mapsto \mathbf{e}' - (b/a)t(u)^l\mathbf{e}$ transforms $A_\zeta$ by*

$$A_\zeta \mapsto A_\zeta - (b/a)\left(\zeta^{(l+1)d-ls'} t(\zeta u)^l - \zeta^{(l+1)c-lr'} t(u)^l\right)\,.$$

*Proof.* This is a straightforward calculation. □

Observe that one can combine these two lemmas with the equation $b\Delta_\zeta^l = aA_\zeta$, which implies that $A_\zeta$ is in fact an $l^{\text{th}}$ power, to see immediately that there is a $t \in \mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ so that the transformation of $\mathbf{e}'$ corresponding to $t$ transforms $A_\zeta$ to 0. We could then perform an analysis of the resulting possibilities for $h$. However, another approach (studying $h$ first) seems to be somewhat easier.

**Lemma 7.4.** *Unless $s \geq r$ and $b/a = \pm 1$, we can transform $\mathbf{e}'$ so that $h(u)$ has degree less than $s$. If $s \geq r$ and $b/a = \pm 1$, let $\eta$ be any choice of $(l-1)^{st}$ root of $b/a$; then we can transform $\mathbf{e}'$ so that $h(u)$ has degree less than $s$ except possibly for a term of degree $ls' - r'$ with coefficient in $\eta\mathbb{F}_l$.*

*Proof.* Recall that by altering our choice of $\mathbf{e}'$, we may transform $h \mapsto h + (u^s t - (b/a)u^r t^l)$, so it suffices to show that the terms of degree $s$ and greater in $u^s t - (b/a)u^r t^l$ can be arbitrary (save that when $s \geq r$ and $b/a = \pm 1$, we can only claim that the coefficient of $u^{ls'-r}$ can be made to represent any additive coset of $\eta\mathbb{F}_l$ in $\mathbb{F}_{l^2}$). Write $t = t_0 + t_1 u + t_2 u^2 + \cdots + t_{l(l^2-1)-1} u^{l(l^2-1)-1}$, so

$$u^s t = t_0 u^s + t_1 u^{s+1} + t_2 u^{s+2} + \cdots$$

while

$$\frac{b}{a} u^r t^l = \frac{b}{a}(t_0^l u^r + t_1^l u^{r+l} + t_2^l u^{r+2l} + \cdots).$$

Hence we wish to know that for arbitrary $\{a_i \in \mathbb{F}_{l^2}\}_{0 \leq i < l(l^2-1)-s}$ we can simultaneously solve the system of equations

$$\begin{cases} t_i = a_i & \text{if } 0 \leq i < l(l^2-1) \text{ and } i \not\equiv r-s \pmod{l}, \\ t_i - \frac{b}{a} t^l_{\frac{i-r+s}{l}} = a_i & \text{if } 0 \leq i < l(l^2-1) \text{ and } i \equiv r-s \pmod{l}. \end{cases}$$

(with $t_k$ understood to be 0 for $k < 0$) save for the aforementioned exception. Notice that if $i > s' - r'$ then $i > (i - r + s)/l > s' - r'$, and similarly that if $i < s' - r'$ then $i < (i - r + s)/l < s' - r'$.

We will now prove by induction on $N$ that the subset of equations involving only those $i$ with $|i - (s' - r')| \leq N$ can be solved simultaneously. If $s' - r' \geq 0$ we need to take $N = 0$ as our base case. Note that $i = s' - r'$ corresponds to the potentially exceptional term of degree $ls' - r'$. For this base case to be true, we must be able to solve the equation

$$t_{s'-r'} - \frac{b}{a} t^l_{s'-r'} = a_{s'-r'}$$

whenever $b/a \neq \pm 1$, and see that the set of elements $t_{s'-r'} - \frac{b}{a} t^l_{s'-r'}$ are coset representatives for $\eta \mathbb{F}_l$ when $b/a = \pm 1$. We argue as follows: to solve

$$t_{s'-r'} - \frac{b}{a} t^l_{s'-r'} = a_{s'-r'}\,,$$

raise this equation to the $l^{\text{th}}$ power to find

$$t^l_{s'-r'} - \frac{b}{a} t_{s'-r'} = a^l_{s'-r'}\,.$$

Multiplying this latter equation by $b/a$ and adding to the original equation, we find

$$t_{s'-r'} \left(1 - \left(\frac{b}{a}\right)^2\right) = a_{s'-r'} + \frac{b}{a} a^l_{s'-r'}\,.$$

When $b/a \neq \pm 1$, this equation may be solved for $t_{s'-r'}$. When $b/a = \pm 1$, we uncover the requirement that

$$\frac{b}{a} a^l_{s'-r'} + a_{s'-r'} = 0\,.$$

When $b/a = 1$, this implies that $a_{s'-r'} \in \mathbb{F}_{l^2}$ has trace 0; when $b/a = -1$, this implies $a_{s'-r'} \in \mathbb{F}_l$. Since the kernel of $t_{s'-r'} \mapsto t_{s'-r'} - \frac{b}{a} t^l_{s'-r'}$ has size at most $l$,

we see that the desired $t_{s'-r'}$ does exist for each such $a_{s'-r'}$ we have just described. Finally, we note that the traceless elements of $\mathbb{F}_{l^2}$ are a complete set of coset representatives for $\mathbb{F}_{l^2}/\mathbb{F}_l$, while the elements of $\mathbb{F}_l$ are a complete set of coset representatives for $\mathbb{F}_{l^2}/\{\mathrm{Tr}=0\}$; since the $(l-1)^{\mathrm{st}}$ roots of $-1$ are exactly the traceless elements of $\mathbb{F}_{l^2}$, this completes the base case of our induction when $s \geq r$.

If $s'-r'<0$, we take $N=r'-s'$ as our base case, and taking $t_0=a_0$ the assertion is evidently true.

To step from $N-1$ to $N>\max\{0,r'-s'\}$, observe that the equations for $t_{s'-r'+N}$ and $t_{s'-r'-N}$ are independent of one another and depend only on $t$'s which have already been determined; moreover, they are linear in the variables for which we are trying to solve, so have solutions in $\mathbb{F}_{l^2}$. Taking $N$ large enough shows that all of the equations can be solved simultaneously, as desired. □

We now assume that $h$ has been transformed as in the above lemma, and we return to considering the equation $b\Delta_\zeta^l = aA_\zeta$, i.e.

$$A_\zeta = \frac{b}{a}\left(\frac{h'\zeta^{(l+1)d-ls'} - h\zeta^{(l+1)c-r'} + \zeta^{r'(l-1)}u^{r'(l-1)}A_\zeta}{u^{s'(l-1)}}\right)^l.$$

**Case 1.** Suppose $r'>s'$, so $\deg(h)<s$. Then $u^{s'(l-1)}$ divides $h'\zeta^{(l+1)d-ls'} - h\zeta^{(l+1)c-r'}$, which is a polynomial of degree less than $s'(l-1)$, and so the latter is 0. Hence

$$A_\zeta = \frac{b}{a}\left(u^{(r'-s')(l-1)}\zeta^{r'(l-1)}A_\zeta\right)^l,$$

and by considering the nonzero term of smallest degree in this equation we can conclude $A_\zeta = 0$.

Next, we turn to the cases when $s' \geq r'$. The polynomial $h$ may now have a term $h_{ls'-r'}u^{ls'-r'}$, in which case we find that $h'\zeta^{(l+1)d-ls'} - h\zeta^{(l+1)c-r'}$ has a term

$$h_{ls'-r'}\zeta^{-r'}\left(\zeta^{(l+1)d} - \zeta^{(l+1)c}\right)u^{ls'-r'} = Hu^{ls'-r'};$$

unless $a = \pm b$ and $c \neq d$, this extra term vanishes.

The equation $aA_\zeta = b\Delta_\zeta^l$ tells us

$$A_\zeta = \frac{b}{a}\left(\frac{(\text{polynomial of degree } < s) + Hu^{ls'-r'} + \zeta^r u^r A_\zeta}{u^s}\right)^l,$$

so the polynomial of degree less than $s$ must precisely cancel the terms of $\zeta^r u^r A_\zeta$ of degree less than $s$. Writing $A_\zeta = a_0 + a_1 u + a_2 u^2 + \cdots$, this leaves the equality

$$A_\zeta = \frac{b}{a}\left(\frac{Hu^{ls'-r'} + \zeta^r u^r (u^{s-r}a_{s-r} + \cdots)}{u^s}\right)^l,$$

the right-hand side of which, written out explicitly, is

$$\frac{b}{a}H^l u^{l(s'-r')} + \zeta^{rl}\frac{b}{a}(a_{s-r}^l + a_{s-r+1}^l u^l + a_{s-r+2}^l u^{2l} + \cdots + a_{s-r+(l^2-2)}^l u^{(l^2-2)l}).$$

(Remember that $u^{(l^2-1)l} = 0$ in our coefficient ring.) Since the right-hand side is a polynomial in $u^l$, looking at the left-hand side we find $a_i = 0$ unless $i$ is divisible by $l$. Feeding this conclusion back into the right-hand side, we conclude on the left-hand side that $a_{il} = 0$ unless $i \equiv (r-s) \pmod{l}$, i.e. $a_i = 0$ unless $i \equiv (r-s)l \pmod{l^2}$. So on the right-hand side, out of $a_{s-r}, \ldots, a_{s-r+l^2-2}$ only $a_{l(s'-r')}$ may be nonzero. Therefore $A_\zeta = a_{l(s'-r')}u^{l(s'-r')}$, and we have the relation

$$a_{l(s'-r')} = \frac{b}{a}H^l + \zeta^{r'(l-1)l}\frac{b}{a}a_{l(s'-r')}^l\,.$$

**Case 2:** $s \geq r$, $a \neq \pm b$. In this case $h_{ls'-r'} = 0$, so $H = 0$, and if $a_{l(s'-r')}$ is nonzero we see from the above relation that $\frac{b}{a} \in \mathbb{F}_l$ must be an $(l-1)^{\text{st}}$ power in $\mathbb{F}_{l^2}$. This contradicts the assertion that $a \neq \pm b$, so in this case $A_\zeta = 0$.

**Case 3:** $s \geq r$, $a = \pm b$, and $c = d$. Here $H = 0$ even though $h_{ls'-r'}$ may not be. However, we see easily from 7.2 that the coefficient of $u^{l(s'-r')}$ in $A_\zeta$ is 0, and hence $A_\zeta = 0$. We remark that the change of variables $\mathbf{e}' \mapsto \mathbf{e}' + (b/a)t^l_{s'-r'}u^{l(s'-r')}\mathbf{e}$ leaves the equation $A_\zeta = 0$ unchanged.

**Case 4:** $s \geq r$, $a = \pm b$, and $c \neq d$. Since $c \neq d$, we may choose $t_{s'-r'}$ to satisfy

$$a_{l(s'-r')} + \frac{b}{a}\zeta^{-lr'}t^l_{s'-r'}(\zeta^{(l+1)c} - \zeta^{(l+1)d}) = 0$$

and so by 7.3 we can transform $\mathbf{e}' \mapsto \mathbf{e}' + (b/a)t^l_{s'-r'}u^{l(s'-r')}\mathbf{e}$ in order to force $A_\zeta = 0$. Notice that this transform does not affect our supposition that $h$ has no terms other than those of degree $ls' - r'$ and of degree less than $s$. However, now that $a_{l(s'-r')} = 0$, we also must have $H = 0$, and since $c \neq d$ this can only happen if $h_{ls'-r'} = 0$. Thus, in this case we may alter $\mathbf{e}'$ to make $A_\zeta = 0$ and $\deg(h) < s$.

To summarize, we have proved that $A_\zeta$ may always be taken to be 0, in a fashion according to the following proposition:

**Proposition 7.5.** *(1) Unless $s \geq r$, $a = \pm b$, and $c = d$, we may simultaneously take $\deg(h) < s$ and $A_\zeta = 0$. Specifically, except for the cases when $s \geq r$ and $a = \pm b$, the condition $\deg(h) < s$ forces $A_\zeta = 0$, while if $s \geq r$, $a = \pm b$, and $c \neq d$, then by altering $\mathbf{e}'$ we can make $A_\zeta = 0$.*

*(2) If $s \geq r$, $a = \pm b$, and $c = d$, by altering $\mathbf{e}'$ we may suppose that $A_\zeta = 0$, that the only term of $h$ of degree at least $s$ is a term of degree $ls' - r'$ and moreover that the coefficient of $u^{ls'-r'}$ in $h$ lies in $\eta\mathbb{F}_l$, where $\eta^{l-1} = b/a$.*

Taking $A_\zeta = 0$ and $h$ of small degree, as described above, the condition that $\phi_1$ commutes with $\zeta$ is equivalent to the equality

$$h'\zeta^{(l+1)d-ls'} = h\zeta^{(l+1)c-r'}.$$

Examining this equation term-by-term, if $h = \sum h_n u^n$ we get

$$h_n \zeta^n \zeta^{(l+1)d-ls'} = h_n \zeta^{(l+1)c-r'}.$$

It follows that $h_n = 0$ unless

$$n + (l+1)d - ls' \equiv (l+1)c - r' \pmod{l^2-1}.$$

If $\deg(h) < s \leq l^2 - 1$ it follows that at most one $h_n$ is nonzero, and since $u^{\max(0,r+s-(l^2-1))} | h$ we find that $h_n$ may be nonzero only if $n$ satisfies the following conditions: $\max(0, r+s-(l^2-1)) \leq n < s$ and $n \equiv (l+1)(c-d) + ls' - r' \pmod{l^2-1}$. On the other hand, in the case where $\deg(h) = ls' - r' \geq s$, at most two $h_n$ are non-zero: either $n$ is as in the preceeding sentence, or $n = ls' - r'$.

Now we will complete our analysis of descent data on these Breuil modules by attempting to impose a compatible action of $\varphi$. If such a compatible action exists, we know that it must have the form

$$[\varphi]\mathbf{e} = \mathbf{e} \text{ and } [\varphi]\mathbf{e}' = \mathbf{e}' + A_\varphi \mathbf{e}$$

for some $A_\varphi \in \mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$. Using the relation $[\varphi][\zeta][\varphi] = [\zeta^l]$ we obtain

$$\begin{aligned}
[\varphi][\zeta][\varphi]\mathbf{e}' &= [\varphi][\zeta](\mathbf{e}' + A_\varphi \mathbf{e}) \\
&= [\varphi](\zeta^{(l+1)c-lr'}\mathbf{e}' + A'_\varphi \zeta^{(l+1)d-ls'}\mathbf{e}) \\
&= (\zeta^l)^{(l+1)c-lr'}\mathbf{e}' + (\zeta^l)^{(l+1)c-lr'} A_\varphi \mathbf{e} + (\zeta^l)^{(l+1)d-ls'} A''_\varphi \mathbf{e} \\
&= [\zeta^l]\mathbf{e}' + ((\zeta^l)^{(l+1)c-lr'} A_\varphi + (\zeta^l)^{(l+1)d-ls'} A''_\varphi)\mathbf{e}
\end{aligned}$$

where if $A_\varphi = \sum a_j u^j$, then $A'_\varphi = \sum a_j (\zeta u)^j$ and $A''_\varphi = \sum a_j^l (\zeta^l)^j u^j$. Matching coefficients, we therefore require

$$a_j + (\zeta^l)^{j+(l+1)(d-c)-l(s'-r')} a_j^l = 0$$

for all $j$ and $\zeta$. It follows that if $a_j \neq 0$, then the above coefficient of $a_j^l$ must be the same for all $\zeta$, and so $j \equiv (l+1)(c-d) + l(s'-r') \pmod{l^2-1}$. Moreover, in this situation, $a_j + a_j^l = 0$.

Turning now to the conditions imposed by $\phi_1[\varphi] = [\varphi]\phi_1$, without difficulty one computes (by applying this relation to the element $u^r\mathbf{e}' + h\mathbf{e}$ of $\mathcal{M}_1$) that

$$A_\varphi = \frac{b}{a}\left(\frac{(h^{(l)} - h) + u^r A_\varphi}{u^s}\right)^l$$

where $h^{(l)}$ denotes the polyonmial whose coefficients are the $l^{\text{th}}$ powers of those of $h$. Our aim will be to show that we may take $A_\varphi = 0$, and hence $h \in \mathbb{F}_l[u]/u^{l(l^2-1)}$.

If $r > s$, then $h = h_n u^n$ with $n < s$, and since $u^s$ divides $h^{(l)} - h$ we need $h_n \in \mathbb{F}_l$. Then an examination of the lowest nonzero term of the equation $A_\varphi = (b/a)(u^{r-s}A_\varphi)^l$ proves that $A_\varphi = 0$.

Suppose now that $s \geq r$. Recalling that we have written $A_\varphi = \sum a_j u^j$, we learn that

$$a_0 + a_1 u + a_2 u^2 + \cdots = \frac{b}{a}(a_{s-r} + a_{s-r+1}u + \cdots)^l + \frac{b}{a}(h_{ls'-r'}^l - h_{ls'-r'})^l u^{l(s'-r')}.$$

Now we employ the same argument that we used in the discussion preceeding Case 2, earlier in this section. Comparing the two sides tells us that $a_j = 0$ unless $l|j$; feeding this into the right-hand side, we find that the coefficient of $u^j$ on the right-hand side is 0 unless $j = l(kl + r - s)$ for some $k$. Finally, feeding this through the equation again, since $l^3 > l(l^2-1)$ we learn that at most $a_{l(s'-r')}$ may be nonzero, in which case it satisfies

$$a_{l(s'-r')}^l = (a/b)a_{l(s'-r')} - (h_{ls'-r'}^l - h_{ls'-r'})^l\,.$$

If $a/b \neq \pm 1$, then $h_{ls'-r'} = 0$, and we conclude from the above equation that if $a_{l(s'-r')} \neq 0$ then $a/b \in \mathbb{F}_l$ is an $(l-1)^{\text{st}}$ power in $\mathbb{F}_{l^2}$. This contradicts the assumption that $a/b \neq \pm 1$, so in this case $A_\varphi = 0$.

If $a/b = 1$, then from our use of proposition 7.5 we are already assuming that $h_{ls'-r'} \in \mathbb{F}_l$, so $a^l_{l(s'-r')} = a_{l(s'-r')}$. Recall, however, that we already saw $a_j^l + a_j = 0$ for any $a_j$, so in this case we also have $A_\varphi = 0$.

Finally, suppose that $a/b = -1$ and $a_{l(s'-r')}$ is nonzero. We must have $l(s'-r') \equiv (l+1)(c-d) + l(s'-r') \pmod{l^2-1}$, in other words, that $c = d$. This latter observation is crucial, because by the remark at the end of Case 3 above, we still the latitude to alter $\mathbf{e}'$ to eliminate $A_\varphi$. To achieve this, continue to let $\eta$ denote an $(l-1)$st root of $-1 = a/b$. If $t = C\eta u^{s'-r'}$ with $C \in \mathbb{F}_l$ then $u^s t - (b/a)u^r t^l = 0$, and the basis change $\mathbf{e}' \mapsto \tilde{\mathbf{e}}' = \mathbf{e}' - (b/a)t^l \mathbf{e} = \mathbf{e}' - C\eta u^{l(s'-r')}\mathbf{e}$ fixes $h$ and preserves $A_\zeta = 0$. Moreover,

$$\begin{aligned}
[\varphi]\tilde{\mathbf{e}}' &= [\varphi](\mathbf{e}' - C\eta u^{l(s'-r')}\mathbf{e}) \\
&= \mathbf{e}' + a_{l(s'-r')}u^{l(s'-r')}\mathbf{e} + C\eta u^{l(s'-r')}\mathbf{e} \\
&= \tilde{\mathbf{e}}' + (a_{l(s'-r')} + 2C\eta)u^{l(s'-r')}\mathbf{e}
\end{aligned}$$

and since $l \neq 2$ we can choose $C$ so that $[\varphi]\tilde{\mathbf{e}}' = \tilde{\mathbf{e}}'$, as desired. Better yet, now that $a_{ls'-r'} = 0$ we find $h_{ls'-r'} \in \mathbb{F}_l$; but since $h_{ls'-r'} \in \eta\mathbb{F}_l$ as well, we must have $h_{ls'-r'} = 0$.

This completes the proof that the basis for our Breuil module may be chosen so that $A_\varphi = 0$, and we have also seen that the only remaining case in which $h_{ls'-r'} \neq 0$ is when $s \geq r$ and $(a,c) = (b,d)$. Note that this may only happen when

both diagonal characters of the (descended) generic fibre representation attached to this Breuil module are equal.

We have shown the following theorem:

**Theorem 7.6.** *Let $(\mathcal{M}, \mathcal{M}_1, \phi_1) \in \mathrm{Ext}^1(\mathcal{M}(r,a,c), \mathcal{M}(s,b,d))$ be a Breuil module with descent data from $F'$ to $\mathbb{Q}_l$ extending the descent data on $\mathcal{M}(r,a,c)$ and $\mathcal{M}(s,b,d)$.*

*(1) Unless $(a,c) = (b,d)$ and $s \geq r$, either $(\mathcal{M}, \mathcal{M}_1, \phi_1)$ is isomorphic to the direct sum $\mathcal{M}(r,a,c) \oplus \mathcal{M}(s,b,d)$ with the direct sum descent data, or it is isomorphic to a Breuil module of the form*

$$\mathcal{M} = \langle \mathbf{e}, \mathbf{e}' \rangle, \ \mathcal{M}_1 = \langle u^s \mathbf{e}, u^r \mathbf{e}' + h_n u^n \mathbf{e} \rangle$$

*and*

$$\phi_1(u^s \mathbf{e}) = b\mathbf{e}, \ \phi_1(u^r \mathbf{e}' + h_n u^n \mathbf{e}) = a\mathbf{e}'$$

*for $h_n \in \mathbb{F}_l^\times$ with*

$$\max(0, r+s-(l^2-1)) \leq n < s \text{ and } n \equiv (l+1)(c-d) + ls' - r' \pmod{l^2-1},$$

*with descent data given by*

$$[\zeta](\mathbf{e}) = \zeta^{(l+1)d - ls'} \mathbf{e}, \ [\zeta](\mathbf{e}') = \zeta^{(l+1)c - lr'} \mathbf{e}'$$

*and*

$$[\varphi](\mathbf{e}) = \mathbf{e}, \ [\varphi](\mathbf{e}') = \mathbf{e}'.$$

*We will denote this Breuil module by $\mathcal{M}(r,a,c;s,b,d;n,h_n)$. (This notation is somewhat redundant, since $r$, $s$, $c$, and $d$ determine $n$.)*

*(2) If* $(a,c)=(b,d)$ *and* $s\geq r$*, then* $(\mathcal{M},\mathcal{M}_1,\phi_1)$ *is isomorphic to a Breuil module of the form*

$$\mathcal{M}=\langle \mathbf{e},\mathbf{e}'\rangle,\ \mathcal{M}_1=\langle u^s\mathbf{e},u^r\mathbf{e}'+(h_nu^n+h_{ls'-r'}u^{ls'-r'})\mathbf{e}\rangle$$

*and*

$$\phi_1(u^s\mathbf{e})=b\mathbf{e},\ \phi_1(u^r\mathbf{e}'+(h_nu^n+h_{ls'-r'}u^{ls'-r'}\mathbf{e})=a\mathbf{e}'$$

*for* $h_n,h_{ls'-r'}\in\mathbb{F}_l$ *with*

$$\max(0,r+s-(l^2-1))\leq n<s \text{ and } n\equiv(l+1)(c-d)+ls'-r' \pmod{l^2-1},$$

*and with descent data given by*

$$[\zeta](\mathbf{e})=\zeta^{(l+1)d-ls'}\mathbf{e},\ [\zeta](\mathbf{e}')=\zeta^{(l+1)c-lr'}\mathbf{e}'$$

*and*

$$[\varphi](\mathbf{e})=\mathbf{e},\ [\varphi](\mathbf{e}')=\mathbf{e}'.$$

*(The* $h_n$ *term is not present if no* $n$ *satisfying the given conditions exists.)*

**Corollary 7.7.** *If* $(a,c)\neq(b,d)$ *or* $r>s$*, then* $\mathrm{Ext}^1(\mathcal{M}(r,a,c),\mathcal{M}(s,b,d))$ *is either* 0- *or* 1*-dimensional, the latter occuring when there exists* $n$ *satisfying the given congruence and inequality. If* $(a,c)=(b,d)$ *and* $s\geq r$*, then* $\mathrm{Ext}^1(\mathcal{M}(r,a,c),\mathcal{M}(s,b,d))$ *is either* 1- *or* 2*-dimensional, and the latter may occur only when* $s'=l$ *or* $l+1$ *and* $r'=0$ *or* $1$*.*

*Proof.* The only statement which requires verification is that when $s\geq r$ and $c=d$, then $n$ exists only when $s'=l$ or $l+1$ and $r'=0$ or 1. But in this case $n\equiv ls'-r'$ (mod $l^2-1$), and since we need $0\leq n<s$ we require $ls'-r'\geq l^2-1$, which forces

$s' = l$ and $r' = 0, 1$ or $s' = l+1$. We also need $r+s-(l^2-1) \leq n = ls'-r'-(l^2-1)$, forcing $lr' \leq s'$, which means $r' = 0, 1$ even in the $s' = l+1$ case.

□

**Remark 7.8.** For the nonsplit Breuil modules $\mathcal{M}(r, a, c; s, b, c; n, h_n)$ above, the descent data is strongly diagonal in the sense that it acts diagonally on our bases both for $\mathcal{M}$ and for $\mathcal{M}_1$. Indeed, an easy calculation reveals that $[\zeta](u^r\mathbf{e}'+h_nu^n\mathbf{e}) = \zeta^{(l+1)c-r'}(u^r\mathbf{e}' + h_nu^n\mathbf{e})$.

**Remark 7.9.** If the equation $u^st - u^rt^l = h_nu^n$ could be solved for $t$, then a seemingly nonsplit Breuil module in the $(a, c) \neq (b, d)$ or $r > s$ case of above theorem would be a direct sum. However, this does not occur, even after an unramified base extension. Indeed, since $n < s$ one sees that for this to occur, it is necessary that $r < s$; then the equality $u^st =$ (terms of degree at least $s$ in $u^rt^l$) forces $t$ to be a monomial of degree $s' - r'$. But then $n = s + (s' - r') > s$, a contradiction.

**Remark 7.10.** On the other hand, in the $(a, c) = (b, d)$, $s > r$ case, we *can* eliminate the $h_{ls'-r'}$ term after an unramified base extension (specifically, one must extend the coefficient field by adjoining a root of $t - t^l = h_{ls'-r'}$ to $\mathbb{F}_{l^2}$, so we need an extension of degree $l$). Observe that the arguments of this section (e.g., lemma 7.3) show that the form of the descent data is unchanged after this change of basis. (However, as before, we cannot affect any $h_nu^n$ term. Indeed, $u^st - u^rt^l$ cannot have a term of degree $u^n$: this would require $r \equiv n \pmod{l}$, but by Corollary 7.7 we have $n = ls' - r' - (l^2 - 1)$, contradiction.)

Henceforth we may restrict ourselves to the nonsplit situation above, since we have assumed that $\overline{\rho}$ has centralizer $\mathbb{F}_l$; in particular $s \neq 0$ and $r \neq l^2-1$, so that an

$n$ satisfying the given inequality and congruence can exist. We also need not concern ourselves with the case $(a, c) = (b, d)$, since in that case both diagonal characters of $\overline{\rho}$ are equal, and so $\overline{\rho}$ would again have nontrivial centralizer. Moreover, we will always take $h_n = 1$: if $h_n \neq 1$, the resulting group scheme is isomorphic to the group scheme with identical parameters save $h_n = 1$ — they are simply anisomorphic as extension classes, which will be of no concern. Therefore, we will need to consider only Breuil modules of the form $\mathcal{M}(r, a, c; s, b, d; n, 1)$.

We now turn to the question of which of these group schemes satisfy the necessary relations on their Dieudonné modules: namely, that $[\zeta] + [\zeta]^l$ acts as $\zeta^{-m} + \zeta^{-lm}$, that $[\zeta]^{l+1}$ acts as $\zeta^{-(l+1)m}$, and that $F + TV = F + abV$ acts at 0. It is easy to see, using the compatibility between Dieudonné theory and Breuil theory described in section 4, that the Dieudonné module of the closed fibre of $\mathcal{M}(r, a, c; s, b, d; n, 1)$ has a basis $\mathbf{v}, \mathbf{w}$ on which $[\zeta]$ acts in the following manner:

$$[\zeta](\mathbf{v}) = \zeta^{(l+1)c-lr'}\mathbf{v} \text{ and } [\zeta](\mathbf{w}) = \zeta^{(l+1)d-ls'}\mathbf{w}$$

and so

$$[\zeta]^l(\mathbf{v}) = \zeta^{(l+1)c-r'}\mathbf{v} \text{ and } [\zeta]^l(\mathbf{w}) = \zeta^{(l+1)d-s'}\mathbf{w}.$$

It follows that if $[\zeta]$ satisfies the desired relations, then either

$$\zeta^{(l+1)c-lr'} = \zeta^{-m} \text{ and } \zeta^{(l+1)c-r'} = \zeta^{-lm}$$

or

$$\zeta^{(l+1)c-lr'} = \zeta^{-lm} \text{ and } \zeta^{(l+1)c-r'} = \zeta^{-m},$$

and a similar relationship holds between $d$, $s'$, and $m$. Recalling that $m = i+(l+1)j$, the first possibility yields congruences

$$(l+1)c - lr' \equiv -m \pmod{l^2-1} \text{ and } (l+1)c - r' \equiv -lm \pmod{l^2-1}.$$

Solving for $r'$, we obtain $r' \equiv -i \pmod{l+1}$. Since $1 \leq i \leq l$ and $0 \leq r' \leq l+1$, we conclude $r' = l+1-i$. This allows us to solve that $c \equiv 1-i-j \pmod{l-1}$ (which completely determines $c$, since it is an element of $\mathbb{Z}/(l-1)\mathbb{Z}$). Applying a similar analysis to the second of the possible sets of relations among $c$, $r'$, and $m$, we find that between the two cases,

$$(r', c) = (i, -j) \text{ or } (l+1-i, 1-i-j).$$

By an identical calculation,

$$(s', d) = (i, -j) \text{ or } (l+1-i, 1-i-j).$$

However, if $r' = s'$ and $c = d$, we would require

$$n \equiv (l+1)(c-d) + ls' - r' \equiv (l-1)s' = s \pmod{l^2-1}.$$

Since we require $0 \leq n < s$ and since $s < l^2 - 1$ (as $i \neq l+1$), this situation is impossible. We have therefore proved that the only possibilities for finite flat group scheme models with descent data for $\overline{\rho}|_{G_{F'}}$ which satisfy our Dieudonné module relations are those of the form

$$\mathcal{M}((l-1)(l+1-i), a, 1-i-j; (l-1)i, b, -j; 0, 1)$$

and

$$\mathcal{M}((l-1)i, a, -j; (l-1)(l+1-i), b, 1-i-j; 0, 1).$$

By Theorem 6.3 (and recalling the contravariance of the Breuil module functor) the residual representations $\overline{\rho}$ which give rise to these group schemes are exactly of the form

- $\overline{\rho} = \begin{pmatrix} \omega^{i+j}\chi_a & * \\ 0 & \omega^{1+j}\chi_b \end{pmatrix}$ and
- $\overline{\rho} = \begin{pmatrix} \omega^{1+j}\chi_a & * \\ 0 & \omega^{i+j}\chi_b \end{pmatrix}$.

Notice that unless $i = 1$ or $i = l$, each different possibility for $\overline{\rho}$ yields at most one finite flat group scheme in our list. When $i = 1$ and $i = l$, it is still possible that $\mathcal{M}(l(l-1), a, -j; (l-1), b, -j; 0, 1)$ and $\mathcal{M}((l-1), a, -j; l(l-1), b, -j; 0, 1)$ are both models for the same $\overline{\rho}$; however, we will see in the next section that the former arises from a residual representation of $G_{\mathbb{Q}_l}$ which is either split or is nonsplit but does not have centralizer $\mathbb{F}_l$, and since we have assumed that $\overline{\rho}$ has centralizer $\mathbb{F}_l$ this group scheme cannot arise from our $\overline{\rho}$. Therefore it is again the case that our $\overline{\rho}$ gives rise to at most one finite flat group scheme model. We will also prove in the next section that if $\overline{\rho} = \begin{pmatrix} \omega^{i+j}\chi_a & * \\ 0 & \omega^{1+j}\chi_b \end{pmatrix}$ gives rise to one of the finite flat group scheme models with descent data in the above list and if $i = 2$, then $*$ is peu-ramifié. Similarly if $\overline{\rho} = \begin{pmatrix} \omega^{1+j}\chi_a & * \\ 0 & \omega^{i+j}\chi_b \end{pmatrix}$ and if $i = l - 1$, then $*$ is peu-ramifié. Once done, all of these results together will have completed the proof of

**Proposition 7.11.** *If $\tau = \tilde{\omega}_2^m \oplus \tilde{\omega}_2^{lm}$ and $\overline{\rho} : G_{\mathbb{Q}_l} \to \mathrm{GL}_2(\mathbb{F}_l)$ has centralizer $\mathbb{F}_l$ and is reducible, and if $R(\overline{\rho}, 2, \tau) \neq 0$, then $\overline{\rho}|_{I_l}$ does indeed have one of the forms specified in Theorem 2.2. Furthermore $\overline{\rho}$ gives rise to exactly one finite flat group*

*scheme over $\mathcal{O}_{F'}$ with descent data to $\mathbb{Q}_l$ satisfying the necessary relations on the Dieudonné module of its closed fibre.*

**Remark 7.12.** The relation $F + TV = F + abV = 0$ is indeed satisfied on the Dieudonné modules of the closed fibres of the above group schemes. One may check that on our basis $\mathbf{v}$,$\mathbf{w}$, $F$ and $V$ act via the matrices

$$\begin{pmatrix} -b & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix}$$

respectively.

## 8. Maps between rank 2 Breuil modules

Our strategy for proving that certain pairs of our rank 2 Breuil modules with descent data arise from the same representation is to study maps between these rank 2 modules. By Lemma 4.1.4 of [BCDT], if two of our $\mathcal{M}(r, a, c; s, b, d; n, 1)$ arise from the same representation of $G_{\mathbb{Q}_l}$, they both map to a maximal model with descent data for this representation, and are also mapped to by a minimal model with descent data, where the maps are generic fibre isomorphisms. A scheme-theoretic closure argument (see Lemma 4.1.3 of [BCDT]) shows that for any of the Breuil modules described in theorem 7.6, the maximal and minimal models with descent data are again an extension of rank 1 Breuil modules with descent data, and hence are among the Breuil modules of theorem 7.6. In particular, in the case when $(a, c) \neq (b, d)$, the maximal and minimal models both must obtain the structure of an $\mathcal{M}(r, a, c; s, b, d; n, 1)$; this is because the diagonal characters coming from the maximal and minimal models must be the same as those from the original group scheme.

In the remainder of this section, we will study maps from $\mathcal{M}(r,a,c;s,b,d;n,h_n)$ to $\mathcal{M}(r_1,a_1,c_1;s_1,b_1,d_1;n_1,h_{n,1})$. (We will allow $h_n=0$ in order to accomodate split Breuil modules in our notation, so $h_n,h_{n,1}$ will be 0 or 1.) We will always let $\mathbf{e}$ and $\mathbf{e}'$ denote our standard basis elements for $\mathcal{M}(r,a,c;s,b,d;n,h_n)$, while $\mathbf{f}$ and $\mathbf{f}'$ will denote our basis elements for $\mathcal{M}(r_1,a_1,c_1;s_1,b_1,d_1;n_1,h_{n,1})$.

We are therefore searching for maps $\mathbf{e}\mapsto V\mathbf{f}+W\mathbf{f}'$, $\mathbf{e}'\mapsto Y\mathbf{f}+Z\mathbf{f}'$, extended linearly to the whole module and compatible with the filtration, $\phi_1$, and descent data structures on our objects. Typically $V,W,Y,Z$ will all be monomials. In this situation, notice that if $W=0$, $V\neq 0$, $Z\neq 0$, and $\deg(V)+\deg(Z)-\deg(Y)<l(l^2-1)$, then every element of $\mathcal{M}(r,a,c;s,b,d;n,h_n)$ which is mapped to 0 under the homomorphism is annihilated by $u^{\max(\deg(Z),\deg(V)+\deg(Z)-\deg(Y)}$; this implies that the kernel of our homomorphism contains no free $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$-submodules. Using the following result, we conclude that our homomorphism must be an isomorphism on the descended generic fibre representation; this is a criterion we will use repeatedly.

**Proposition 8.1.** *Let $\mathcal{G}\to\mathcal{G}'$ be a map of finite flat group schemes over $\mathcal{O}_K$ of equal order, where $\mathcal{O}_K$ are the integers of a finite extension $K/\mathbb{Q}_l$ with residue field $\mathbf{k}$ and ramification index $e$. If the kernel of the corresponding map $\mathcal{M}'\to\mathcal{M}$ of Breuil modules does not contain a free $\mathbf{k}[u]/u^{el}$-submodule, then $\mathcal{G}\to\mathcal{G}'$ is an isomorphism on generic fibres.*

*Proof.* Assume $f:\mathcal{G}\to\mathcal{G}'$ does not induce an isomorphism on generic fibres. Then the image of $f_{/K}$ in $G'_{/K}$ is not all of $G'_{/K}$, and taking scheme-theoretic closure of

this image yields an exact sequence of group schemes

$$0 \longrightarrow \mathcal{H} \longrightarrow \mathcal{G}' \xrightarrow{g} \mathcal{H}' \longrightarrow 0$$

with $\mathcal{H}' \neq 0$ and $g \circ f = 0$. If $\mathcal{N}'$ is the Breuil module of $\mathcal{H}'$, then $\mathcal{N}' \hookrightarrow \ker(\mathcal{M}' \to \mathcal{M})$, since short-exact sequences of group schemes yield short-exact sequences of Breuil modules. □

8.0.1. *The case $h_n = 1$, $h_{n,1} = 1$.* We begin a general analysis of maps

$$\Psi : \mathcal{M}(r, a, c; s, b, d; n, 1) \to \mathcal{M}(r_1, a_1, c_1; s_1, b_1, d_1; n_1, 1).$$

Assume that $\Psi$ is an isomorphism on the descended generic fibre representations. Since at the very least we know what the diagonal characters of these representations are, we either have $a = a_1$, $c = c_1$ and $b = b_1$, $d = d_1$, or $a = b_1$, $c = d_1$ and $b = a_1$, $d = c_1$, and the latter can occur only when the representation splits. Notice that the existence of $n$ and $n_1$ implies that $r', r_1' \leq l$ and $s', s_1' \geq 1$. At times we will refrain from using the inequalities on $r', s'$ so that certain pieces of our discussion still hold in the $h_n = 0$ case, so the reader should take note if an inequality appears not to be best-possible.

To begin our analysis,

$$\Psi([\zeta](\mathbf{e})) = \Psi(\zeta^{(l+1)d-ls'}\mathbf{e}) = \zeta^{(l+1)d-ls'}V\mathbf{f} + \zeta^{(l+1)d-ls'}W\mathbf{f}',$$

whereas

$$[\zeta](\Psi(\mathbf{e})) = [\zeta](V\mathbf{f} + W\mathbf{f}') = \zeta^{(l+1)d_1-ls_1'}\tilde{V}\mathbf{f} + \zeta^{(l+1)c_1-lr_1'}\tilde{W}\mathbf{f}'$$

with $V(\zeta u) = \tilde{V}(u)$ and $\tilde{W}$ defined similarly. Since we must have $\Psi([\zeta](\mathbf{e})) = [\zeta](\Psi(\mathbf{e}))$, we can equate both right-hand sides to conclude that

$$V(u) = u^{(l+1)(d-d_1)+l(s_1'-s')} v(u^{l^2-1})$$

and

$$W(u) = u^{(l+1)(d-c_1)+l(r_1'-s')} w(u^{l^2-1})$$

for polynomials $v$, $w$. The fact that $\Psi$ commutes with the action of $[\varphi]$ yields that $v$ and $w$ have coefficients in $\mathbb{F}_l$. Similarly

$$Y(u) = u^{(l+1)(c-d_1)+l(s_1'-r')} y(u^{l^2-1})$$

and

$$Z(u) = u^{(l+1)(c-c_1)+l(r_1'-r')} z(u^{l^2-1})$$

for $y$,$z$ polynomials with coefficients in $\mathbb{F}_l$. Next, $\Psi(\phi_1(u^s\mathbf{e})) = \Psi(b\mathbf{e}) = bV\mathbf{f} + bW\mathbf{f}'$ whereas

$$\begin{aligned}
\phi_1(\Psi(u^s\mathbf{e})) &= \phi_1(u^s V\mathbf{f} + u^s W\mathbf{f}') \\
&= \phi_1\left(\left(\frac{u^s V}{u^{s_1}} - \frac{u^{s+n_1}W}{u^{r_1+s_1}}\right)(u^{s_1}\mathbf{f}) + \frac{u^s W}{u^{r_1}}(u^{r_1}\mathbf{f}' + u^{n_1}\mathbf{f})\right) \\
&= \left(\frac{u^s V}{u^{s_1}} - \frac{u^{s+n_1}W}{u^{r_1+s_1}}\right)^l b_1\mathbf{f} + \left(\frac{u^s W}{u^{r_1}}\right)^l a_1\mathbf{f}'.
\end{aligned}$$

Equating coefficients, we have

$$bW = \left(\frac{u^s W}{u^{r_1}}\right)^l a_1.$$

If $W \neq 0$, this equation implies via the usual argument that $W$ is a monomial: indeed, two nonzero terms on the right-hand side, and therefore of $W$ differ in degree by at least $l$; but feeding this into the right-hand side again they must differ in degree by at least $l^2$, and so $l^3$, and so on. Therefore if $W \neq 0$, we quickly

see $r_1' \geq s'$ and $W = wu^{l(r_1'-s')}$ for constant $w$. Matching this with our previous discussion yields $d = c_1$, $w \in \mathbb{F}_l$, and so $a_1 = b$.

Turning to an analysis of $V$, we see that $V$ must be a monomial. For example, $V$ is an $l^{\text{th}}$ power, so all terms are of degree divisible by $l$, while simultaneously any two terms of $V$ differ in degree by a multiple of $l^2 - 1$. Since $\deg(V) < l(l^2-1)$, we obtain the desired conclusion. When $W = 0$ we need that $V \neq 0$ (or else $\Psi$ would not induce an isomorphism on representations). We then see by a standard argument that $V = vu^{l(s_1'-s')}$ with $v \in \mathbb{F}_l$, $s_1' \geq s'$, and $b = b_1$, $d = d_1$. If $W \neq 0$, we can also see that $V \neq 0$: for if $V = 0$, we would have

$$\left(\frac{u^{s+n_1}(wu^{l(r_1'-s')})}{u^{r_1+s_1}}\right)^l = 0$$

which implies $n_1 + (r_1' - s') - s_1 \geq l^2 - 1$. This is impossible since $n_1 < s_1$ and $r_1' \leq l$. Since $V$ is a monomial, it follows that $\deg(V) = l(n_1 - s_1 + r_1' - s')$ (or else $V$ would have two terms, one of which cancels the contribution of $W$). Then

$$\deg((u^sV/u^{s_1})^l) = l(l(n_1 - s_1) + lr_1' - s' - s_1) \leq l(-l + l^2 - (l-1)) < l(l^2-1).$$

The conclusion is that the $(u^sV/u^{s_1})^l$ term does contribute a term to $V$, and therefore $\deg(V) = l\deg(u^sV/u^{s_1})$. Hence $V = vu^{l(s_1'-s')}$ in this case as well, and again $d = d_1$. The equation $\deg(V) = l(n_1 - s_1 + r_1' - s')$ implies $n_1 = ls_1' - r_1'$ and so $c_1 = d_1$. In order to satisfy the equality (and not just the congruence condition) as well as $n_1 < s_1$, we also need $r_1 > s_1$. Next, equating coefficients we get $bv = (v-w)^l b_1$, i.e.

$$w = \left(1 - \frac{b}{b_1}\right)v,$$

and $w \neq 0$ implies $b \neq b_1$. Since if $W \neq 0$ we get $b \neq b_1$, and by our initial observation $a_1 = b$, $c_1 = d$, $a = b_1$, and $d = d_1$, and this case can only occur if the

underlying representations are split. We already had $c_1 = d_1$, and in summary we have obtained that if $\Psi$ exists, then:

- in any case, $s_1 \geq s$, $d_1 = d$, and $v \in \mathbb{F}_l^\times$;
- if $W = 0$, then $b = b_1$ and $\mathbf{e} \mapsto vu^{l(s_1' - s')}\mathbf{f}$;
- if $W \neq 0$, then $r_1' \geq s'$, $r_1' > s_1'$, $c = d = c_1 = d_1$, $a_1 = b \neq b_1 = a$, and $\mathbf{e} \mapsto vu^{l(s_1' - s')}\mathbf{f} + \left(1 - \frac{b}{b_1}\right) vu^{l(r_1' - s')}\mathbf{f}'$

We next consider the implications of $\Psi$ on the other basis element for $\mathcal{M}_1$. To begin with,

$$\Psi(\phi_1(u^r\mathbf{e}' + u^n\mathbf{e})) = \Psi(a\mathbf{e}') = aY\mathbf{f} + aZ\mathbf{f}',$$

whereas

$$\begin{aligned}
\phi_1(\Psi(u^r\mathbf{e}' + u^n\mathbf{e})) &= \phi_1(u^r(Y\mathbf{f} + Z\mathbf{f}') + u^n(V\mathbf{f} + W\mathbf{f}')) \\
&= \phi_1\left(\left(\frac{u^rZ + u^nW}{u^{r_1}}\right)(u^{r_1}\mathbf{f}' + u^{n_1}\mathbf{f})\right) \\
&\quad + \phi_1\left(\left(\frac{u^rY + u^nV}{u^{s_1}} - \frac{u^{r+n_1}Z + u^{n+n_1}W}{u^{r_1+s_1}}\right)(u^{s_1}\mathbf{f})\right) \\
&= \left(\frac{u^rZ + u^nW}{u^{r_1}}\right)^l a_1\mathbf{f}' \\
&\quad + \left(\frac{u^{r+r_1}Y + u^{n+r_1}V - u^{r+n_1}Z - u^{n+n_1}W}{u^{r_1+s_1}}\right)^l b_1\mathbf{f}.
\end{aligned}$$

As usual this implies that $Y$, $Z$ are monomials. Analyzing

$$aZ = \left(\frac{u^rZ + u^nW}{u^{r_1}}\right)^l a_1$$

we see that if $W = 0$ then we need $Z \neq 0$ (for the map to be an isomorphism on representations), and in fact $Z = zu^{l(r_1 - r)}$ with $r_1 \geq r$, $c = c_1$, $a = a_1$, and $z \in \mathbb{F}_l$.

On the other hand, if $W \neq 0$ then

$$\deg(u^n W/u^{r_1}) = n + l(r_1' - s') - r_1 = (n-s) + r_1' - s' < l - 1$$

and so (as with $V$ above), $Z$ is nonzero and $\deg(Z) = l(n-s+r_1'-s')$. Continuing, we obtain

$$\deg(u^r Z/u^{r_1}) = l(n-s) + r_1' + (l-1)r' - ls' \leq -l + l + (l-1)l - l < l^2 - 1$$

and so its $l^{\text{th}}$ power contributes an additional term to $Z$. As $Z$ is a monomial, this forces $\deg(Z) = l(r_1' - r')$ and $c = c_1$ again, while $l(r_1' - r') = l(n - s + r_1' - s')$ gives $n = ls' - r'$ and $c = d$, $r > s$. Solving for $z$ in terms of $v$ gives

$$z = \left(\frac{a}{a_1} - 1\right)^{-1} \left(1 - \frac{b}{b_1}\right) v$$

and so $a \neq a_1$.

We now turn to the task of examining $Y$, which seems at first rather daunting, but is not as awful as it looks. If $W \neq 0$, a rather remarkable thing happens: the terms $u^{n+r_1}V$, $-u^{r+n_1}Z$, and $-u^{n+n_1}W$ all have degree equal to $ls_1' + r_1 - r'$, and moreover their coefficients sum to

$$v - \left(1 - \frac{b}{b_1}\right) v + \left(1 - \frac{a}{a_1}\right)^{-1} \left(1 - \frac{b}{b_1}\right) v = v \frac{1 - \frac{ab}{a_1 b_1}}{1 - \frac{a}{a_1}} = 0$$

since $ab = a_1 b_1$, and we are simply left with the condition

$$aY = b_1 \left(\frac{u^r Y}{u^{s_1}}\right)^l.$$

Thus $Y = 0$ is always permitted, and $Y = yu^{l(s_1' - r')}$ is possible only when $s_1 \geq r$.

If $W = 0$, we will find that except in a few very special cases, a necessary and sufficient condition to guarantee the existence of $Y$ for *some* choice of $v$, $z$ is that

$$n - (ls' - r') = n_1 - (ls_1' - r_1').$$

If $Y = 0$ is to be possible, then the terms $u^{n+r_1}V$ and $u^{r+n_1}Z$ must be exactly equal, so $v = z$ and these terms have the same degree, so

$$n + r_1 + l(s_1' - s') = n_1 + r + l(r_1' - r')$$

which is easily seen to be equivalent to the above condition. If $Y \neq 0$, then

$$aY = \left( \frac{u^{r+r_1}Y + u^{n+r_1}V - u^{r+n_1}Z}{u^{r_1+s_1}} \right)^l b_1 \,.$$

One sees easily, as before, that the $V$ and $Z$ terms are not divisible by $u^{l^2-1}$ so that their $l^{\text{th}}$ powers are not 0. If $u^{r-s_1}Y$ were divisible by $u^{l^2-1}$, then since $Y$ is a monomial, the $V$ and $Z$ terms would have to be of equal degree and we would have

$$\deg(Y) = l(n + \deg(V) - s_1) = l(n - s' - s + s_1') \leq l(s_1' - s - 1) \,.$$

But then

$$\deg Y + r - s_1 \leq s_1 + r - ls - l \leq (l+1) + l(l-1) - l - l < l^2 - 1 \,,$$

a contradiction. Therefore, the right-hand side of our expression for $aY$ has three nonzero terms, and since $Y$ is to be a monomial, either one pair of terms on the right-hand side must have the same degree and cancel one another out, or else all three terms on the right-hand side have the same degree. If the $V$ and $Z$ terms have the same degree (or if all three terms have the same degree) then we have already seen that $n_1 - (ls_1' - r_1') = n - (ls' - r')$. If $v = z$, then $Y = yu^{l(s_1' - r')}$, $a = b_1$, and $s_1 > r$. If $v \neq z$, then the condition that all three terms must have the same degree implies $n = ls' - r'$ and $n_1 = ls_1' - r_1$, $c = d$, $r > s$, and $r_1 > s_1$.

If instead the $V$ and $Y$ terms cancel, their terms must have the same degree, and so

$$\deg(Y) + r - s_1 = n - ls' + s_1' \,.$$

But we can say more: $Y$ is given by the remaining term coming from $Z$, and so we can compute

$$\deg(Y) = l(n_1 - s_1 + r_1' - r').$$

Combining these two expressions for $\deg(Y)$ yields

$$l(n_1 - (ls_1' - r_1')) = n - (ls' - r').$$

However, we know that $n-(ls'-r')$ is a number divisible by $l+1$ and lies between $-l(l+1)$ and $r'-s' \geq l-1$, so the only possibilities in the above equation are $n_1-(ls_1'-r_1') = n-(ls'-r') = 0$ (our usual equality) or $n-(ls'-r') = -l(l+1)$ and $n_1-(ls_1'-r_1') = -(l+1)$. Our congruence condition on $n$ implies that $c = d-1$, and the only way that $n-(ls'-r') = -l(l+1)$ is to have $n=0$, $s' = l+1$, and $r' = 0$. Therefore, this last case can only arise in considering maps out of the Breuil module $\mathcal{M}(0, a, d-1; l^2-1, b, d; 0, 1)$.

Similarly, if the $Z$ and $Y$ terms cancel, we find either our usual equality, or else that $n-(ls'-r') = -(l+1)$ and $n_1-(ls_1'-r_1') = -l(l+1)$. This time, we are therefore considering only maps into $\mathcal{M}(0, a, d-1; l^2-1, b, d; 0, 1)$.

To summarize the conditions for the existence of $\Psi$, we have:

- in any case $r_1 \geq r$, $s_1 \geq s$, and $c_1 = c$, $d_1 = d$, $v \in \mathbb{F}_l^\times$;
- if $W = 0$, we have $a = a_1$, $b = b_1$, and $\mathbf{e} \mapsto vu^{l(s_1'-s')}\mathbf{f}$, $\mathbf{e}' \mapsto Y\mathbf{f} + zu^{l(r_1'-r')}\mathbf{f}'$, with $z \in \mathbb{F}_l^\times$. A suitable choice of $Y$, $v$, and $z$ will exist if and only if $n-(ls'-r') = n_1-(ls_1'-r_1')$, with the exception of maps

$$\mathcal{M}(0, a, d-1; s'(l-1), b, d; ls'-(l+1), 1) \to \mathcal{M}(0, a, d-1; l^2-1, b, d; 0, 1)$$

for $2 \leq s' \leq l$ and maps

$$\mathcal{M}(0, a, d-1; l^2-1, b, d; 0, 1) \to \mathcal{M}(r'(l-1), a, d-1; l^2-1, b, d; l^2-1-r', 1)$$

for $1 \leq r' \leq l-1$.

- if $W \neq 0$, we have $a = b_1 \neq a_1 = b$, $c_1 = c = d = d_1$, $r > s$ and $r_1 > s_1$, the underlying representations are split, and

$$\mathbf{e} \mapsto vu^{l(s_1'-s')}\mathbf{f} + \left(1 - \frac{b}{b_1}\right) vu^{l(r_1'-s')}\mathbf{f}',$$

$$\mathbf{e}' \mapsto Y\mathbf{f} + \left(\frac{a}{a_1} - 1\right)^{-1} \left(1 - \frac{b}{b_1}\right) vu^{l(r_1'-r')}\mathbf{f}'.$$

In the case $W = 0$, we see that $\deg(V) + \deg(Z) \leq l(s_1' + r_1') < l(l^2-1)$, so by the criterion preceeding this section, the resulting maps really are isomorphisms on the generic fibre. The same is true in the $W \neq 0$, $Y = 0$ case.

8.0.2. *The case $h_n = 0$, $h_{n,1} = 1$.* Here, we investigate the maps from split Breuil modules into nonsplit ones. The argument analyzing $V$, $W$, in the preceeding case carries over word-for-word, except that now $r = l^2 - 1$ and $s = 0$ are permitted. However, we were careful never to use $r < l^2 - 1$ or $s > 0$ in any of our estimates in that portion of the preceeding section (we used only the analogous inequalities for $r_1$,$s_1$), and so our analysis carries over wholesale, i.e. we again obtain:

- in any case, $s_1 \geq s$, $d_1 = d$, and $v \in \mathbb{F}_l^\times$;
- if $W = 0$, then $b = b_1$ and $\mathbf{e} \mapsto vu^{l(s_1'-s')}\mathbf{f}$;
- if $W \neq 0$, then $r_1' \geq s'$, $c = d = c_1 = d_1$, $r_1' > s_1'$, $a_1 = b \neq b_1 = a$, and $\mathbf{e} \mapsto vu^{l(s_1'-s')}\mathbf{f} + \left(1 - \frac{b}{b_1}\right) vu^{l(r_1'-s')}\mathbf{f}'$

We also note that the analysis for $\mathbf{e}'$ in this split case should proceed exactly as the analysis for $\mathbf{e}$ (replacing $V$,$W$,$s$,$b$,$d$ by $Y$,$Z$,$r$,$a$,$c$) and so we will obtain:

- in any case, $s_1 \geq r$, $d_1 = c$, and $y \in \mathbb{F}_l^\times$;
- if $Z = 0$, then $a = b_1$ and $\mathbf{e}' \mapsto yu^{l(s_1'-r')}\mathbf{f}$;
- if $Z \neq 0$, then $r_1' \geq r'$, $c = d = c_1 = d_1$, $r_1' > s_1'$, $a_1 = a \neq b_1 = b$, and $\mathbf{e}' \mapsto yu^{l(s_1'-r')}\mathbf{f} + \left(1 - \frac{a}{b_1}\right) yu^{l(r_1'-r')}\mathbf{f}\,'$

Since $W$ and $Z$ cannot both be 0, we see that no matter what, $c = d = c_1 = d_1$. Moreover, either $W$ or $Z$ must be zero (as we cannot have both $a_1 = b \neq b_1 = a$ and $a_1 = a \neq b_1 = b$). Putting everything together, we find the desired maps exactly when

- $c = d = c_1 = d_1$, $r_1 > s_1 \geq \max(r, s)$;
- $a_1 = a \neq b_1 = b$, or $a_1 = b \neq b_1 = a$.

In the former of the two possibilities in the last item, our map has the form

$$\mathbf{e} \mapsto vu^{l(s_1'-s')}\mathbf{f}\ ,\ \mathbf{e}' \mapsto yu^{l(s_1'-r')}\mathbf{f} + \left(1 - \frac{a}{b_1}\right) yu^{l(r_1'-r')}\mathbf{f}\,'$$

whereas in the latter case our map has the form

$$\mathbf{e} \mapsto vu^{l(s_1'-s')}\mathbf{f} + \left(1 - \frac{b}{b_1}\right) vu^{l(r_1'-s')}\mathbf{f}\,'\ ,\ \mathbf{e}' \mapsto yu^{l(s_1'-r')}\mathbf{f}\,.$$

By the criterion at the beginning of this section, any example of one of the above maps must indeed be an isomorphism on the underlying representations.

8.0.3. *The case $h_n = 1$, $h_{n,1} = 0$.* In this case, the analysis of $\mathbf{e} \mapsto V\mathbf{f} + W\mathbf{f}\,'$ yields

$$\left(\frac{u^s V}{u^{s_1}}\right)^l b_1 = bV \text{ and } \left(\frac{u^s V}{u^{r_1}}\right)^l a_1 = bW$$

and so

- if $V \neq 0$, then $d = d_1$, $b = b_1$, $s_1 \geq s$, and $V = vu^{l(s_1'-s')}$;
- if $W \neq 0$, then $d = c_1$, $b = a_1$, $r_1 \geq s$, and $W = wu^{l(r_1'-s')}$;
- at least one of $V$, $W$ is nonzero.

Turning to $\mathbf{e}' \mapsto Y\mathbf{f} + Z\mathbf{f}'$, we get

$$aZ = \left(\frac{u^r Z + u^n W}{u^{r_1}}\right)^l a_1$$

and

$$aY = \left(\frac{u^r Y + u^n V}{u^{s_1}}\right)^l b_1.$$

If $Z = 0$ then $W \neq 0$, while $(u^n W/u^{r_1})^l = 0$, which implies $n+l(r_1'-s')-r_1 \geq l^2-1$, which we know to be impossible. So $Z \neq 0$, and as usual $Z = zu^{l(r_1'-r')}$. Similarly $Y \neq 0$ and $Y = yu^{l(s_1'-r')}$.

Now if $V \neq 0$, our usual analysis gives $n + \deg(V) = r + \deg(Y)$, so $n = ls' - r'$ and $c = d$, $r > s$, and $a \neq b_1$. Since $a \neq b_1$ and the pair of corner characters of the underlying representations must be the same, we get $a = a_1 \neq b_1 = b$ and $c_1 = c = d = d_1$. In the same fashion, if $W \neq 0$ we get $r > s$, $b_1 = a \neq a_1 = b$, $c = d = c_1 = d_1$. Plainly we cannot, then, have both $V = 0$ and $W = 0$. In summary, if we obtain the desired maps, we have:

- $c = d = c_1 = d_1$, $\min(r_1, s_1) \geq r > s$,
- $a = a_1 \neq b_1 = b$ or $b_1 = a \neq a_1 = b$.

In the former of the two possibilities in the last item, our map has the form

$$\mathbf{e} \mapsto vu^{l(s_1'-s')}\mathbf{f}\ ,\ \mathbf{e}' \mapsto \left(\frac{a}{b_1} - 1\right)^{-1} vu^{l(s_1'-r')}\mathbf{f} + zu^{l(r_1'-r')}\mathbf{f}'$$

whereas in the latter case our map has the form

$$\mathbf{e} \mapsto wu^{l(r_1'-s')}\mathbf{f}\ ,\ \mathbf{e}' \mapsto yu^{l(s_1'-r')}\mathbf{f} + \left(\frac{a}{a_1} - 1\right)^{-1} wu^{l(r_1'-r')}.$$

By the criterion preceeding section 8.0.1, any example of one of the above maps must indeed be an isomorphism on the underlying representations.

8.1. **Non-split Breuil modules with split representations.** In this subsection, we assume $(a,c) \neq (b,d)$. Evidently the split Breuil module $\mathcal{M}(r,a,c) \oplus \mathcal{M}(s,b,d)$ maps to $\mathcal{M}(l^2-1,a,c) \oplus \mathcal{M}(l^2-1,b,d)$ and is mapped to by $\mathcal{M}(0,a,c) \oplus \mathcal{M}(0,b,d)$. By the criteria in the preceeding two subsections (and specifically by the necessary inqualities among $r$,$s$,$r_1$,$s_1$), there cannot exist a non-split Breuil module to which $\mathcal{M}(l^2-1,a,c) \oplus \mathcal{M}(l^2-1,b,d)$ maps, nor can there exist a non-split Breuil module which maps to $\mathcal{M}(0,a,c) \oplus \mathcal{M}(0,b,d)$. It follows that $\mathcal{M}(l^2-1,a,c) \oplus \mathcal{M}(l^2-1,b,d)$ and $\mathcal{M}(0,a,c) \oplus \mathcal{M}(0,b,d)$ are, respectively, the maximal and minimal integral models with descent data for our representation. If $\mathcal{M}(r,a,c;s,b,d;n,1)$ is a nonsplit Breuil module, its underlying representation is split if and only if it is mapped to by $\mathcal{M}(0,a,c) \oplus \mathcal{M}(0,b,d)$ with a map which is an isomorphism on underlying representations (equivalently, if and only if it maps to $\mathcal{M}(l^2-1,a,c) \oplus \mathcal{M}(l^2-1,b,d)$). By the preceeding subsections, this happens precisely when $r > s$, $c = d$, and $a \neq b$. That is, we have proved:

**Proposition 8.2.** *Suppose $(a,c) \neq (b,d)$. The Breuil module $\mathcal{M}(r,a,c;s,b,d;n,1)$ is an integral model with descent data for a split representation of $G_{\mathbb{Q}_l}$ if and only if the Breuil module is of the form $\mathcal{M}(r,a,c;s,b,c;n,1)$ with $r > s$ and $a \neq b$.*

We now remark that by this result, $\mathcal{M}(l(l-1),a,-j;(l-1),b,-j;0,1)$ has an underlying representation which is split if $a \neq b$; if instead $a = b$, then we are in the case $(a,c) = (b,d)$, so the underlying representation has both diagonal characters equal to $\chi_a \omega^{1+j}$ and has centralizer larger than $\mathbb{F}_l$. This completes one of the claims preceeding Proposition 7.11. (Notice also that, desirably, $\mathcal{M}((l-1),a,-j;l(l-1),b,-j;0,1)$ does not have a split underlying representation.)

8.2. **Peu-ramifié representations.** Suppose $\mathcal{M}(r,a,d-1;s,b,d;n,1)$ is a non-split Breuil module. Then $n$ satisfies the congruence

$$n \equiv -(l+1) + ls' - r' \pmod{l^2-1}$$

and the inequalities

$$\max(0, r+s-(l^2-1)) \leq n < s.$$

If $r' = l$ and $s' \leq 2$, then certainly $n = (l^2-1) + ls' - (2l+1) \geq (l-1)s'$, a contradiction; on the other hand, if $r' = l$ and $s' > 2$, then $n = ls' - (2l+1)$, and this fails to satisfy

$$ls' - 2l - 1 = n \geq r + s - (l^2-1) = l(l-1) + s - (l^2-1) = s - l + 1$$

(which is equivalent to $s' \geq l+2$), also a contradiction. Therefore $r' \leq l-1$.

We now claim that there exists a map

$$\mathcal{M}(r,a,d-1;s,b,d;n,1) \to \mathcal{M}((l-1)^2,a,d-1;l^2-1,b,d;l(l-1),1)$$

which is an isomorphism on underlying representations. Plainly all the criteria from the end of section 8.0.1 are satisfied except possibly the existence of suitable $Y$, and our map must take the form:

$$\mathbf{e} \mapsto vu^{l(l+1-s')}\mathbf{f}\,, \mathbf{e}' \mapsto Y\mathbf{f} + zu^{l(l-1-r')}\mathbf{f}'$$

with $Y$ a monomial satisfying

$$\begin{aligned} \frac{a}{b}Y &= \left(\frac{u^{r+r_1}Y + u^{n+r_1}V - u^{r+n_1}Z - u^{n+n_1}W}{u^{r_1+s_1}}\right)^l \\ &= \left(\frac{u^{r+(l-1)^2}Y + vu^{n-ls'+(2l^2-l+1)} - zu^{-r'+2(l^2-l)}}{u^{2(l^2-l)}}\right)^l \end{aligned}$$

Recall that $n \equiv -(l+1)+ls'-r' \pmod{l^2-1}$, with $1 \leq s' \leq l+1$ and $0 \leq r' \leq l-1$. Then $-l \leq -(l+1)+ls'-r' \leq l^2-1$. We can have $-(l+1)+ls'-r' = l^2-1$ only if $s' = l+1$ and $r' = 0$, in which case we have $n = 0$. In that case we need

$$\frac{a}{b}Y = \left( \frac{u^{(l-1)^2}Y + vu^{(l-1)^2} - zu^{2(l^2-l)}}{u^{2(l^2-l)}} \right)^l$$

which can plainly be satisfied by taking $Y = y$ to be constant, and more precisely by requiring $y = -v = -(b/a)z$. Another possibility is that $s'$ is still large enough that $n = -(l+1)+ls'-r'$, so that $n - ls' + (2l^2 - l + 1) = -r' + 2(l^2 - l)$, so we can take $v = z$ and $Y = 0$. The final possibility is that $-(l+1)+ls'-r' < 0$. Since $r' \leq l-1$, this occurs if and only if $s' = 1$, in which case $n = l^2 - 2 - r'$. But then it is certainly false that $n < s = l-1$, so this possibility cannot occur.

**Theorem 8.3.** *For all choices of $r$,$s$, and $n$ such that*

$$\mathcal{M}(r, a, d-1; s, b, d; n, 1)$$

*is a nonsplit Breuil module, the underlying representation is peu-ramifié.*

*Proof.* The above discussion shows that each of these Breuil modules in an integral model for the same underlying representation. To see that this representation is peu-ramifié, we note (see, e.g., section 8 of [Edi92]) that peu-ramifié representations of $G_{\mathbb{Q}_l}$ have models over $\mathbb{Z}_l$. Therefore at least one of the above Breuil modules is a model with descent data for a peu-ramifié representation. Consequently, they all are. □

This completes the proof of Proposition 7.11.

8.3. **Spaces of rank 2 models.** We now unify the above discussion with our classification in theorem 7.6 of all rank 2 models with descent data for representations of the form

$$\begin{pmatrix} \chi_a\omega^{1-c} & * \\ 0 & \chi_b\omega^{1-d} \end{pmatrix}.$$

This section plays no role in the proof of the main results of this thesis. However, it may be helpful in gaining an intuition for the collection of group schemes under consideration.

Let $\mathcal{M} = \mathcal{M}(r, a, c; s, b, d; n, 1)$ be a model for such a representation. Since $n$ exists satisfying the conditions $n \neq (l+1)(c-d) + ls' - r'$ and $\max(0, r+s-(l^2-1)) \leq n < s$ then $s > 0$ and $r < l^2 - 1$. Moreover, since $n < s$ we see that $n - (ls' - r') < r' - s' \leq l - 1$, while certainly $n - (ls' - r') \geq -l(l+1)$. Since $n - (ls' - r')$ is divisible by $l+1$, we find that $n - (ls' - r') = -k(l+1)$ for an integer $k$ between 0 and $l$. We see that $k \equiv d - c \pmod{l-1}$, so we have $k = 0$ or $l-1$ if $c \equiv d \pmod{l-1}$, we have $k = 1$ or $l$ if $c \equiv d - 1 \pmod{l-1}$, and we have $k$ lying between 2 and $l-2$ otherwise. We call $k$ the *invariant* of $\mathcal{M}$.

**Remark 8.4.** If $k = l$, then $n = 0$, $s' = l+1$, and $r' = 0$. If $k = l-1$, then $s' = l$ or $l+1$ and $r' = 0$ or 1.

**Proposition 8.5.** *For fixed $k$, the pairs $(r', s')$ for which $n = (ls' - r') - k(l+1)$ satisfies the desired inequalities are precisely the pairs satisfying:*

$$0 \leq r' \leq l - k$$

*and*

$$k + 1 \leq s' \leq l + 1$$

*with the exceptions that for $k = 0$ we require $r' > s'$, and for $k = 1$ the pair $(0, l+1)$ is excluded.*

*Proof.* We shall prove that for fixed $k > 0$ the desired pairs $(r', s')$ are the lattice points inside the convex quadrilateral bounded by the inequalities

$$r' \geq 0$$

$$s' \leq l + 1$$

$$ls' - r' \geq (l + 1)k$$

$$s' - lr' + (l^2 - 1) \geq (l + 1)k\,,$$

and, if $k = 1$, the region excludes the extremal point $(0, l + 1)$. For $k = 0$, we shall similarly prove that the pairs $(r', s')$ for which $n = (ls' - r') - k(l + 1)$ are precisely the lattice points inside the triangle bounded by the inequalities

$$r' > s'$$

$$ls' - r' \geq (l + 1)k$$

$$s' - lr' + (l^2 - 1) \geq (l + 1)k\,.$$

It is easy to see that the lattice points inside these regions are exactly the ones described in the statement of the proposition.

At the outset, we know that we must satisfy the inequalities

$$0 \leq s' \leq l + 1\,,$$

$$0 \leq r' \leq l + 1\,,$$

$$0 \leq n < s\,,$$

$$r + s - (l^2 - 1) \leq n\,.$$

From $n = (ls' - r') - k(l+1) < s$ we get $-k(l+1) < r' - s'$. This is no condition if $k \geq 2$, but if $k = 1$ we exclude $(0, l+1)$ and if $k = 0$ we need $r' > s'$. The condition $n \geq 0$ translates into $ls' - r' \geq (l+1)k$, and the condition $n \geq r + s - (l^2 - 1)$ translates into $s - lr' + (l^2 - 1) \geq (l+1)k$. Therefore, the conditions in the proposition are necessary. We need to show that they are sufficient.

If $k = 0$, the inequalities $ls' \geq r' > s'$ imply $s > 0$, so $r > 0$, while the inequalities $r' + (l^2 - 1) > s' + (l^2 - 1) \geq lr'$ imply $r' < l + 1$, so $s' < l + 1$.

If $k > 0$, the inequalities $r' \geq 0$ and $ls' - r' \geq (l+1)k > 0$ imply $s > 0$, while the inequalities $s' \leq l + 1$ and $s' - lr' + (l^2 - 1) \geq (l+1)k > 0$ imply $r' < l + 1$. □

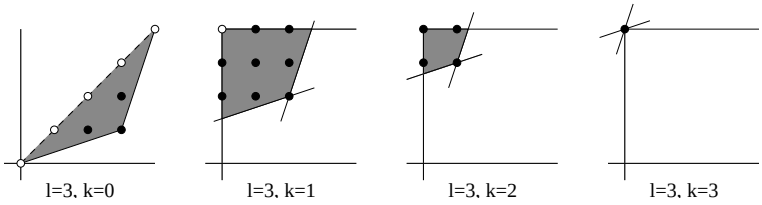


FIGURE 1. The regions of proposition 8.5 when $l = 3$

As our next application of the invariant, notice that the conclusions of section 8.0.1 imply the following:

**Proposition 8.6.** *Suppose we have two Breuil modules $\mathcal{M} = \mathcal{M}(r, a, c; s, b, d; n, 1)$ and $\mathcal{M}' = \mathcal{M}(r_1, a, c; s_1, b, d; n_1, 1)$ with $(d - c) \not\equiv 0, 1 \pmod{l-1}$. Then there is a map from $\mathcal{M}$ to $\mathcal{M}'$ which is an isomorphism on the generic fibre precisely whenever $r_1 \geq r$, $s_1 \geq s$.*

*Proof.* Since $(d-c) \not\equiv 0, 1 \pmod{l-1}$, there is only one possibility for the invariant attached to $\mathcal{M}$ and $\mathcal{M}'$, and so these invariants are equal. The result follows immediately from the $W = 0$ case of the conclusions of section 8.0.1. □

The results of section 8.2 show, similarly, that when $d - c \equiv 1 \pmod{l-1}$ the integral models for the peu-ramifié representation

$$\begin{pmatrix} \chi_a \omega^{1-c} & * \\ 0 & \chi_b \omega^{-c} \end{pmatrix}$$

are in correspondence with the models with invariant $k = 1$ and $k = l$, that maps correspond to arrows upwards and to the right (inclusively) in the union of the spaces for $k = 1$ and $k = l$ described in proposition 8.5, and that the maximal and minimal models are

$$\mathcal{M}((l-1)^2, a, c; (l+1)(l-1), b, d; l^2 - l, 1)$$

and

$$\mathcal{M}(0, a, c; 2(l-1), b, d; l-1, 1)\,.$$

Further, the results of section 8.1 show that in case $c = d$ and $a \neq b$, the Breuil module $\mathcal{M} = \mathcal{M}(r, a, c; s, b, c; n, 1)$ correspond to the split representation

$$\begin{pmatrix} \chi_a \omega^{1-c} & 0 \\ 0 & \chi_b \omega^{1-c} \end{pmatrix}$$

if and only if $\mathcal{M}$ has invariant 0, while it corresponds to the non-split representation

$$\begin{pmatrix} \chi_a \omega^{1-c} & * \\ 0 & \chi_b \omega^{1-c} \end{pmatrix}$$

if and only if $\mathcal{M}$ has invariant $l - 1$.

In the former case, the maximal and minimal models are $\mathcal{M}(l^2-1,a,c)\oplus\mathcal{M}(l^2-1,b,c)$ and $\mathcal{M}(0,a,c)\oplus\mathcal{M}(0,b,c)$. The lattice of models is as described in the invariant 0 case of 8.5, except that the split Breuil modules are included in the obvious fashion, and that $\mathcal{M}(r,a,c;s,b,c;n,1)$ and $\mathcal{M}(r,b,c;s,a,c;n,1)$ are isomorphic (hence are in the same lattice).

In the invariant $k=l-1$ case, the maximal and minimal models are $\mathcal{M}((l-1),a,c;(l^2-1),b,c;l,1)$ and $\mathcal{M}(0,a,c;l(l-1),b,c;1,1)$ and the lattice of models is as described in proposition 8.5. In fact, there are exactly four models in this lattice, corresponding to $r'=0,1$ and $s'=l,l+1$.

We summarize these results as follows:

**Theorem 8.7.** *Fix $a,b\in\mathbb{F}_l^\times$ and $c,d\in\mathbb{Z}/(l-1)\mathbb{Z}$, and let $\rho$ be a representation*

$$\begin{pmatrix}\chi_a\omega^{1-c} & *\\ 0 & \chi_b\omega^{1-d}\end{pmatrix}$$

*of $G_{\mathbb{Q}_l}$, with $*\neq 0$ and $(a,c)\neq(b,d)$. If $d-c\equiv 1 \pmod{l-1}$, suppose $*$ is peu-ramifié. Let $k$ be the integer between 1 and $l-1$ congruent to $d-c \pmod{l-1}$. Then the Breuil modules corresponding to the integral models with descent data for $\rho$ over $\mathcal{O}_{F'}$ are the Breuil modules $\mathcal{M}(r,a,c;s,b,d;n,1)$ with*

$$0\leq r'\leq l-k$$

*and*

$$k+1\leq s'\leq l+1.$$

*The lattice of these Breuil modules is a square of side $l-k+1$, and maps exist from $\mathcal{M}(r,a,c;s,b,d;n,1)$ to $\mathcal{M}(r',a,c;s',b,d;n',1)$ whenever $r'\geq r$ and $s'\geq s$.*

*In particular, there are* $(l-k+1)^2$ *such integral models, and the maximal and minimal models for this representation correspond to the Breuil modules*

$$\mathcal{M}((l-k)(l-1), a, c; (l+1)(l-1), b, d; l^2-kl, 1)$$

*and*

$$\mathcal{M}(0, a, c; (k+1)(l-1), b, d; l-k, 1)\,.$$

*If* $*$ *were très-ramifié, then* $\rho$ *would have no such integral models.*

*Proof.* Our analysis in section 8.1 shows that the representations underlying these Breuil modules are indeed non-split. The claim regarding maximal and minimal models is easily verified by referring to proposition 8.5. □

We leave the study of the case $(a, c) = (b, d)$ to the interested reader.

## 9. Rank 4 Calculations

Recall that our list of nonsplit rank 2 Breuil modules satisfying our Dieudonné module conditions was

$$\mathcal{M}((l-1)(l+1-i), a, 1-i-j; (l-1)i, b, -j; 0, 1)$$

and

$$\mathcal{M}((l-1)i, a, -j; (l-1)(l+1-i), b, 1-i-j; 0, 1).$$

We have shown that we also no longer need to consider $\mathcal{M}((l-1)l, a, -j; (l-1), b, -j; 0, 1)$ (since its underlying representation either splits or has nontrivial centralizer), nor do we need to consider $\mathcal{M}((l-1), a, -j; (l-1)l, a, -j; 0, 1)$ (since its underlying representation has nontrivial centralizer). Notice that the change of variables $i \mapsto l+1-i$ and $j \mapsto i+j-1$ interchanges $m$ and $lm$, thus leaving our

Dieudonné module conditions the same. We are therefore reduced to showing, for each

$$\mathcal{M} = \mathcal{M}((l-1)i, a, -j; (l-1)(l+1-i), b, 1-i-j; 0, 1)$$

with $i = 1, \ldots, l-1$ and $j \in \mathbb{Z}/(l-1)\mathbb{Z}$, and $a \neq b$ if $i = 1$, that the space of extensions of $\mathcal{M}$ by $\mathcal{M}$ still satisfying the desired Dieudonné module relations is at most 1-dimensional. We now begin this computation. For clarity we will continue to write $r'$ for $i$ and $s'$ for $l+1-i$, since that is what we are used to. Note that $r' + s' = l+1$, $ls' - r' = (l-i)(l+1)$, and $lr' - s' = (l+1)(i-1)$.

Let $(\mathcal{N}, \mathcal{N}_1, \phi_1)$ be an arbitrary extension of $\mathcal{M}$ by $\mathcal{M}$. We will let $\mathbf{e}, \mathbf{e}'$ denote the standard basis for the submodule $\mathcal{M}$ of $\mathcal{N}$, while $\mathbf{f}, \mathbf{f}'$ will denote lifts of the standard basis for the quotient $\mathcal{M}$ of $\mathcal{N}$. Then

$$\mathcal{N} = \langle \mathbf{e}, \mathbf{e}', \mathbf{f}, \mathbf{f}' \rangle,$$

$$\mathcal{N}_1 = \langle u^{(l-1)s'}\mathbf{e}, u^{(l-1)r'}\mathbf{e}' + \mathbf{e}, u^{(l-1)s'}\mathbf{f} + A\mathbf{e} + B\mathbf{e}', u^{(l-1)r'}\mathbf{f}' + \mathbf{f} + C\mathbf{e} + D\mathbf{e}' \rangle.$$

To begin with, we wish to see that we may take $A = B = C = D = 0$ by using the fact that any $\mathbf{f} \mapsto \mathbf{f} + \alpha\mathbf{e} + \beta\mathbf{e}'$, $\mathbf{f}' \mapsto \mathbf{f}' + \gamma\mathbf{e} + \delta\mathbf{e}'$ is an allowable change of basis for $\mathcal{N}$. That is, we wish to find $\tilde{\mathbf{f}} = \mathbf{f} + \alpha\mathbf{e} + \beta\mathbf{e}'$ and $\tilde{\mathbf{f}}' = \mathbf{f}' + \gamma\mathbf{e} + \delta\mathbf{e}'$ so that $u^{(l-1)s'}\tilde{\mathbf{f}}, u^{(l-1)r'}\tilde{\mathbf{f}}' + \tilde{\mathbf{f}} \in \mathcal{N}_1$ (for they are then automatically a basis). To begin with, replacing $u^{(l-1)s'}\mathbf{f} + A\mathbf{e} + B\mathbf{e}'$ with $u^{(l-1)s'}\mathbf{f} + A\mathbf{e} + B\mathbf{e}' - A(u^{(l-1)r'}\mathbf{e}' + \mathbf{e})$ in our basis for $\mathcal{N}_1$, and making a similar change for $\tilde{\mathbf{f}}'$, we can simplify matters greatly by taking $A = C = 0$. To eliminate $B$, note that since $u^{l^2-1}\mathbf{f} \in u^{l^2-1}\mathcal{N} \subset \mathcal{N}_1$ and $u^{(l-1)r'}(u^{(l-1)s'}\mathbf{f} + B\mathbf{e}') \in \mathcal{N}_1$, we obtain $u^{(l-1)r'}B\mathbf{e}' \in \mathcal{N}_1$. This implies $u^{(l-1)s'} | B$. Writing $B = u^{(l-1)s'}B'$, we may take $\tilde{\mathbf{f}} = \mathbf{f} + B'\mathbf{e}'$ to eliminate $B$. Assuming, then, that $A = B = C = 0$, we wish to alter $\mathbf{f}'$ to eliminate $D$. By

the same considerations as before, we can see $u^{(l-1)s'}D\mathbf{e}' \in \mathcal{N}_1$, and so $u^{(l-1)r'}|D$. Putting $D = u^{(l-1)r'}D'$ we can take $\tilde{\mathbf{f}}' = \mathbf{f}' + D'\mathbf{e}'$ to eliminate $D$.

Thus we may assume

$$\mathcal{N}_1 = \langle u^{(l-1)s'}\mathbf{e}, u^{(l-1)r'}\mathbf{e}' + \mathbf{e}, u^{(l-1)s'}\mathbf{f}, u^{(l-1)r'}\mathbf{f}' + \mathbf{f} \rangle$$

and the next thing we want to do is determine the ways we can still alter $\mathbf{f}, \mathbf{f}'$ to $\tilde{\mathbf{f}}, \tilde{\mathbf{f}}'$ while preserving this form for $\mathcal{N}_1$, i.e., keeping $u^{(l-1)s'}\tilde{\mathbf{f}}$, $u^{(l-1)r'}\tilde{\mathbf{f}}' + \tilde{\mathbf{f}} \in \mathcal{N}_1$. Indeed, suppose

$$\mathbf{f} \mapsto \tilde{\mathbf{f}} = \mathbf{f} + A\mathbf{e} + B'\mathbf{e}', \ \mathbf{f}' \mapsto \tilde{\mathbf{f}}' = \mathbf{f}' + C\mathbf{e} + D'\mathbf{e}'.$$

Then

$$u^{(l-1)s'}\tilde{\mathbf{f}} = u^{(l-1)s'}\mathbf{f} + Au^{(l-1)s'}\mathbf{e} + B'u^{(l-1)s'}\mathbf{e}',$$

and this is in $\mathcal{N}_1$ provided $u^{(l-1)r'}$ divides $B'$. Write $B' = u^{(l-1)r'}B$. Now

$$u^{(l-1)r'}\tilde{\mathbf{f}}' + \tilde{\mathbf{f}} = (u^{(l-1)r'}\mathbf{f}' + \mathbf{f}) + (A + u^{(l-1)r'}C - B - D')\mathbf{e} + (B + D')(u^{(l-1)r'}\mathbf{e}' + \mathbf{e}).$$

Thus $C$ may be arbitrary so long as we select $D'$ such that $u^{(l-1)s'}$ divides $A + u^{(l-1)r'}C - B - D'$. Writing

$$A + u^{(l-1)r'}C - B - D' = u^{(l-1)s'}D$$

we may evidently make $D$ arbitrary and put

$$D' = A + u^{(l-1)r'}C - B - u^{(l-1)s'}D.$$

So our most general change of variables is

$$\tilde{\mathbf{f}} = \mathbf{f} + A\mathbf{e} + u^{(l-1)r'}B\mathbf{e}', \ \tilde{\mathbf{f}}' = \mathbf{f}' + C\mathbf{e} + (A - B + u^{(l-1)r'}C + u^{(l-1)s'}D)\mathbf{e}'$$

with $A, B, C, D$ arbitrary. We now turn to the question of $\phi_1$. We take

$$\mathcal{N}_1 = \langle u^{(l-1)s'}\mathbf{e}, u^{(l-1)r'}\mathbf{e}' + \mathbf{e}, u^{(l-1)s'}\mathbf{f}\,, u^{(l-1)r'}\mathbf{f}\,' + \mathbf{f}\,\rangle$$

with

$$\phi_1(u^{(l-1)s'}\mathbf{e}) = b\mathbf{e}\,, \phi_1(u^{(l-1)r'}\mathbf{e}' + \mathbf{e}) = a\mathbf{e}'$$

$$\phi_1(u^{(l-1)s'}\mathbf{f}\,) = b\mathbf{f}\, + V\mathbf{e} + W\mathbf{e}'\,, \phi_1(u^{(l-1)r'}\mathbf{f}\,' + \mathbf{f}\,) = a\mathbf{f}\,' + Y\mathbf{e} + Z\mathbf{e}'.$$

Using the general change-of-variables we have computed above, we wish to simplify $V$,$W$,$Y$,$Z$. To begin with, we try $\tilde{\mathbf{f}}\, = \mathbf{f}\, + A\mathbf{e} + u^{(l-1)r'}B\mathbf{e}'$ (with a commensurate choice of $\tilde{\mathbf{f}}\,'$, which for now will be irrelevant). Then

$$\begin{aligned}
\phi_1(u^{(l-1)s'}\tilde{\mathbf{f}}\,) &= \phi_1(u^{(l-1)s'}\mathbf{f}\, + Au^{(l-1)s'}\mathbf{e} + Bu^{l^2-1}\mathbf{e}') \\
&= \phi_1(u^{(l-1)s'}\mathbf{f}\, + Bu^{(l-1)s'}(u^{(l-1)r'}\mathbf{e}' + \mathbf{e}) + (A-B)u^{(l-1)s'}\mathbf{e}) \\
&= b\mathbf{f}\, + V\mathbf{e} + W\mathbf{e}' + B^l u^{l(l-1)s'}a\mathbf{e}' + (A-B)^l b\mathbf{e} \\
&= b\tilde{\mathbf{f}}\, + (V - bA + b(A-B)^l)\mathbf{e} \\
&\qquad +(W + u^{(l-1)r'}(aB^l u^{(l-1)(ls'-r')} - bB))\mathbf{e}'\,.
\end{aligned}$$

Since $B$ may be arbitrary and $ls' - r' > 0$ we may make $(aB^l u^{(l-1)(ls'-r')} - bB)$ arbitrary, and we may use this choice to eliminate all terms in $W$ of degree at least $r$. Thus we may assume $\deg(W) < r$. Making this change completely determines $u^{(l-1)r'}B$, so we may now make this change and assume henceforth that $B = 0$ and $\deg(W) < r$. Then $V$ is altered to $V + b(A^l - A)$ by our choice of $A$, which we can use to eliminate every term of $V$ except the constant term. In total, we can therefore suppose $V$ is a constant $v$, $W$ is a polynomial $w$ of degree less than $r$; the only allowable change of $\mathbf{f}$ is then $\mathbf{f} \mapsto \mathbf{f} + \alpha\mathbf{e}$, with $\alpha$ a constant, moving $V \mapsto V + b(\alpha^l - \alpha)$.

Consider the additive map from $\mathbb{F}_{l^2} \to \mathbb{F}_{l^2}$ sending $x$ to $x^l - x$. The kernel is exactly $\mathbb{F}_l$, while if $x^l - x \in \mathbb{F}_l$ then $(x^l - x)^l = x^l - x$; since $x^{l^2} = x$ and $l \neq 2$ we find $x^l = x$. So our map induces an isomorphism $\mathbb{F}_{l^2}/\mathbb{F}_l \to \mathbb{F}_{l^2}/\mathbb{F}_l$. Thus we may select $\alpha$ above so that $V \in \mathbb{F}_l$, and then $V$ is completely fixed, while $\mathbf{f} \mapsto \mathbf{f} + \alpha\mathbf{e}$ with $\alpha \in \mathbb{F}_l$ is the only possible change of $\mathbf{f}$.

To reduce further, we now wish to apply descent data to these extensions. Suppose

$$[\zeta]\mathbf{f} = \zeta^{(l+1)d-ls'}\mathbf{f} + A_\zeta\mathbf{e} + B_\zeta\mathbf{e}'.$$

Then

$$[\zeta](u^s\mathbf{f}) = (\zeta u)^s(\zeta^{(l+1)d-ls'}\mathbf{f} + A_\zeta\mathbf{e} + B_\zeta\mathbf{e}') \in \mathcal{N}_1$$

which requires $u^r \,|B_\zeta$, say $B_\zeta = u^r B'_\zeta$. We obtain

$$\begin{aligned}\phi_1([\zeta](u^s\mathbf{f})) &= \phi_1(\zeta^{(l+1)d-s'}(u^s\mathbf{f}) + (\zeta^s u^s B'_\zeta)(u^r\mathbf{e}' + \mathbf{e}) + \zeta^s(A_\zeta - B_\zeta)(u^s\mathbf{e}) \\ &= \zeta^{(l+1)d-ls'}(b\mathbf{f} + v\mathbf{e} + w\mathbf{e}') + (\zeta^s u^s B'_\zeta)^l a\mathbf{e}' + \zeta^{sl}(A_\zeta - B'_\zeta)^l b\mathbf{e}\end{aligned}$$

whereas

$$\begin{aligned}[\zeta](\phi_1(u^s\mathbf{f})) &= [\zeta](b\mathbf{f} + v\mathbf{e} + w\mathbf{e}') \\ &= \zeta^{(l+1)d-ls'}b\mathbf{f} + (v\zeta^{(l+1)d-ls'} + bA_\zeta)\mathbf{e} + (\tilde{w}\zeta^{(l+1)c-lr'} + bB_\zeta)\mathbf{e}'\end{aligned}$$

with $\tilde{w}(u) = w(\zeta u)$, and so matching coefficients we get

$$A_\zeta = \zeta^{sl}(A_\zeta - B'_\zeta)^l$$

and

$$\tilde{w}\zeta^{(l+1)c-lr'} + bB_\zeta = w\zeta^{(l+1)d-ls'} + a\zeta^{sl}u^{sl}(B'_\zeta)^l$$

This latter equation is actually a tremendous help: since $w$ is of degree at most $r-1$ whereas $B_\zeta$ and $u^{sl}$ are divisible by $u^r$, we must have

$$\tilde{w}\zeta^{(l+1)c-lr'} = w\zeta^{(l+1)d-ls'}$$

and

$$bB_\zeta = a\zeta^{sl}u^{sl}(B'_\zeta)^l.$$

In the former equation, we use the fact that $(l+1)d-ls' \equiv (l+1)c-r' \pmod{l^2-1}$ to see $\tilde{w} = \zeta^r w$, and since $\deg w < r$ we must have $w = 0$. In the latter equation, if the left-hand side has lowest nonzero term of degree $k$ , then for the right-hand side the lowest term has degree $sl + l(k-r)$. Equating these degrees gives $k = r + (r' - ls') < r$, contradicting our divisibility condition on $B_\zeta$. Thus $B_\zeta = 0$. Taking $B'_\zeta = 0$, we finally obtain

$$A_\zeta = \zeta^{sl}A_\zeta^l$$

which implies that $A_\zeta$ is a constant: indeed $A_\zeta \in \zeta^{-ls'}\mathbb{F}_l$. One now checks, using $[\zeta_2][\zeta_1] = [\zeta_2\zeta_1]$, that the map $\zeta \mapsto \zeta^{-(l+1)d+ls'}A_\zeta$ is a homomorphism from $\mathbb{F}_{l^2}^\times$ to $\mathbb{F}_l$, so must be the zero map. We have thus shown $A_\zeta = B_\zeta = 0$ and $w = 0$. Similarly, we analyze $[\varphi](\mathbf{f}) = \mathbf{f} + A_\varphi\mathbf{e} + B_\varphi\mathbf{e}'$. From $\phi_1([\varphi](u^s\mathbf{f})) = [\varphi](\phi_1(u^s\mathbf{f}))$ we get $B_\varphi = u^r B'_\varphi$ and

$$bA_\varphi = b(A_\varphi - B'_\varphi)^l\,,\ bB_\varphi = a(B'_\varphi u^s)^l$$

from which we conclude that $B_\varphi = 0$ and $A_\varphi \in \mathbb{F}_l$. But $\varphi^2 = 1$ implies that $A_\varphi + A_\varphi^l = 0$ and so $A_\varphi = 0$.

Next we consider the significantly more intricate problem of simplifying $Y$,$Z$, and $[\zeta]\mathbf{f}\,'$ by altering $\mathbf{f}\,'$. Taking $A = B = 0$, we select

$$\tilde{\mathbf{f}}\,' = \mathbf{f}\,' + C\mathbf{e} + (u^{(l-1)r'}C + u^{(l-1)s'}D)\mathbf{e}'\,.$$

(The diligent reader may trace through the following computation to see that if we take $A = \alpha \in \mathbb{F}_l$ then the simplification of $Y$,$Z$ we achieve is exactly the same, so we may as well take $\alpha = 0$ for simplicity.) Then

$$\begin{aligned}
&\phi_1(u^{(l-1)r'}\tilde{\mathbf{f}}\,' + \mathbf{f}\,) \\
&= \phi_1((u^{(l-1)r'}\mathbf{f}\,' + \mathbf{f}\,) + Cu^{(l-1)r'}\mathbf{e} + (u^{(l-1)r'}C + u^{(l-1)s'}D)(u^{(l-1)r'}\mathbf{e}')) \\
&= \phi_1((u^{(l-1)r'}\mathbf{f}\,' + \mathbf{f}\,) - Du^{(l-1)s'}\mathbf{e} + (u^{(l-1)r'}C + u^{(l-1)s'}D)(u^{(l-1)r'}\mathbf{e}' + \mathbf{e}) \\
&= a\mathbf{f}\,' + Y\mathbf{e} + Z\mathbf{e}' - bD^l\mathbf{e} + (u^{(l-1)r'}C + u^{(l-1)s'}D)^l a\mathbf{e}' \\
&= a\tilde{\mathbf{f}}\,' + (Y - aC - bD^l)\mathbf{e} + (Z - a(u^{(l-1)r'}C + u^{(l-1)s'}D) \\
&\qquad + a(u^{(l-1)r'}C + u^{(l-1)s'}D)^l)\mathbf{e}'\,.
\end{aligned}$$

Whatever $D$ is, we will certainly want to take $aC = Y - bD^l$ to eliminate $Y$ (which completely determines $C$ in terms of $D$). We may therefore assume $Y = 0$ and $aC = -bD^l$, and then our map alters

$$Z \mapsto Z - (bu^rD^l - au^sD)^l + (bu^rD^l - au^sD)\,.$$

Noting this, we now turn to the consideration of descent data. Suppose for each $\zeta$ that

$$[\zeta]\mathbf{f}\,' = [\zeta]^{(l+1)c-lr'}\mathbf{f}\,' + E_\zeta\mathbf{e} + F_\zeta\mathbf{e}'\,.$$

We then have

$$\begin{aligned}
[\zeta](u^r\mathbf{f}' + \mathbf{f}) &= (\zeta u)^r(\zeta^{(l-1)c-lr'}\mathbf{f}' + E_\zeta \mathbf{e} + F_\zeta \mathbf{e}') + \zeta^{(l-1)c-r'}\mathbf{f} \\
&= \zeta^{(l+1)c-r'}(u^r\mathbf{f}' + \mathbf{f}) + \zeta^r E_\zeta u^r \mathbf{e} + \zeta^r F_\zeta u^r \mathbf{e}' \\
&= \zeta^{(l+1)c-r'}(u^r\mathbf{f}' + \mathbf{f}) + \zeta^r(E_\zeta u^r - F_\zeta)\mathbf{e} + \zeta^r F_\zeta(u^r\mathbf{e}' + \mathbf{e})
\end{aligned}$$

so $u^s \,|\zeta^r(E_\zeta u^r - F_\zeta) = u^s\Delta_\zeta$ and

$$\phi_1[\zeta](u^r\mathbf{f}' + \mathbf{f}) = \zeta^{(l+1)c-lr'}(a\mathbf{f}' + Z\mathbf{e}') + \Delta_\zeta^l b\mathbf{e} + a\zeta^{lr}F_\zeta^l a\mathbf{e}'.$$

Matching coefficients with

$$[\zeta]\phi_1(u^r\mathbf{f}' + \mathbf{f}) = [\zeta](a\mathbf{f}' + Z\mathbf{e}') = \zeta^{(l+1)c-lr'}a\mathbf{f}' + aE_\zeta\mathbf{e} + aF_\zeta\mathbf{e}' + \tilde{z}\zeta^{(l+1)c-lr'}$$

gives

$$aE_\zeta = b\Delta_\zeta^l$$

and

$$aF_\zeta + \zeta^{(l+1)c-lr'}\tilde{Z} = a\zeta^{lr}F_\zeta^l + \zeta^{(l+1)c-lr'}Z.$$

With these equations in hand, we are finally in a position to begin reducing the possibilities for $Z$, $E_\zeta$, and $F_\zeta$. Observe that (writing $E_\zeta = E_\zeta(u)$ , $F_\zeta = F_\zeta(u)$)

$$\begin{aligned}
[\zeta_1][\zeta_2]\mathbf{f}' &= [\zeta_1](\zeta_2^{(l+1)c-lr'}\mathbf{f}' + E_{\zeta_2}\mathbf{e} + F_{\zeta_2}\mathbf{e}') \\
&= \zeta_2^{(l+1)c-lr'}(\zeta_1^{(l+1)c-lr'}\mathbf{f}' + E_{\zeta_1}\mathbf{e} + F_{\zeta_1}\mathbf{e}') \\
&\quad + \zeta_1^{(l+1)c-r'}E_{\zeta_2}(\zeta_1 u)\mathbf{e} + \zeta_1^{(l+1)c-lr'}F_{\zeta_2}(\zeta_1 u)\mathbf{e}' \\
&= (\zeta_1\zeta_2)^{(l+1)c-lr'}\mathbf{f}' + (\zeta_2^{(l+1)c-lr'}E_{\zeta_1} + \zeta_1^{(l+1)c-lr'}\zeta_1^r E_{\zeta_2}(\zeta_1 u))\mathbf{e} \\
&\quad + (\zeta_2^{(l+1)c-lr'}F_{\zeta_1} + \zeta_1^{(l+1)c-lr'}F_{\zeta_2}(\zeta_1 u))\mathbf{e}' \\
&= (\zeta_1\zeta_2)^{(l+1)c-lr'}\mathbf{f}' + E_{\zeta_1\zeta_2}\mathbf{e} + F_{\zeta_1\zeta_2}\mathbf{e}'
\end{aligned}$$

and matching coefficients we get

$$E_{\zeta_1\zeta_2} = \zeta_2^{(l+1)c-lr'} E_{\zeta_1} + \zeta_1^{(l+1)c-lr'} (\zeta_1^r E_{\zeta_2}(\zeta_1 u))$$

and

$$F_{\zeta_1\zeta_2} = \zeta_2^{(l+1)c-lr'} F_{\zeta_1} + \zeta_1^{(l+1)c-lr'} F_{\zeta_2}(\zeta_1 u)\,,$$

i.e.,

$$(\zeta_1\zeta_2)^{-(l+1)c+lr'} E_{\zeta_1\zeta_2} = \zeta_1^{-(l+1)c+lr'} E_{\zeta_1} + \zeta_1^r (\zeta_2^{-(l+1)c+lr'} E_{\zeta_2}(\zeta_1 u))$$

and

$$(\zeta_1\zeta_2)^{-(l+1)c+lr'} F_{\zeta_1\zeta_2} = \zeta_1^{-(l+1)c+lr'} F_{\zeta_1} + \zeta_2^{-(l+1)c+lr'} F_{\zeta_2}(\zeta_1 u)\,.$$

This proves that the map $\zeta \mapsto \zeta^{-(l+1)c+lr'} E_\zeta$ is a cocycle in the group cohomology $H^1(\mathbb{F}_{l^2}^\times, \mathbb{F}_{l^2}[u]/u^{l(l^2-1)})$ where $\mathbb{F}_{l^2}^\times$ acts on $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ via $\zeta \cdot f(u) = \zeta^r f(\zeta u)$. Similarly $\zeta \mapsto \zeta^{-(l+1)c+lr'} F_\zeta$ is a cocycle in the group cohomology $H^1(\mathbb{F}_{l^2}^\times, \mathbb{F}_{l^2}[u]/u^{l(l^2-1)})$ where $\mathbb{F}_{l^2}^\times$ acts on $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ via $\zeta \cdot f(u) = f(\zeta u)$. However, both of these cohomology groups are trivial, because $\mathbb{F}_{l^2}^\times$ has order $l^2-1$, whereas $\mathbb{F}_{l^2}[u]/u^{l(l^2-1)}$ is an $l$-torsion module. So both of our cocycles are coboundaries, and we therefore obtain the existence of polynomials $P(u)$,$Q(u)$ such that

$$\zeta^{-(l+1)c+lr'} E_\zeta = \zeta^r Q(\zeta u) - Q(u)$$

and

$$\zeta^{-(l+1)c+lr'} F_\zeta = P(\zeta u) - P(u)\,.$$

Setting $R(u) = u^r Q(u) - P(u)$, we compute

$$\begin{aligned} E_\zeta u^r - F_\zeta &= \zeta^{(l+1)c-lr'} (\zeta^r u^r Q(\zeta u) - u^r Q(u) - P(\zeta u) + P(u)) \\ &= \zeta^{(l+1)c-lr'} (R(\zeta u) - R(u))\,. \end{aligned}$$

Recalling that $u^s\Delta_\zeta = \zeta^r(E_\zeta u^r - F_\zeta)$, so that

$$\Delta_\zeta = \zeta^{(l+1)c-r'}\frac{R(\zeta u)-R(u)}{u^s}$$

we find that $R(u)$ must have no terms of degree less than $s$, except possibily for a constant term. (In general $f(\zeta u) = f(u)$ for all $\zeta$ implies that $f$ has only terms of degree divisible by $l^2-1$.) We write $R(u) = r_0 + r_s u^s + \cdots = r_0 + u^s R_0(u)$. Then the equation $aE_\zeta = b\Delta_\zeta^l$ gives us:

$$\left(\frac{R(\zeta u)-R(u)}{u^s}\right)^l = \frac{a}{b}(\zeta^r Q(\zeta u) - Q(u))\,.$$

Writing $Q(u) = q_0 + q_1 u + \cdots$, we examine the above equation term-by-term. Using that $r \equiv ls \pmod{l^2-1}$, the left-hand side has terms of the form $r_{i+s}^l(\zeta^{il+r}-1)u^{il}$ while the right-hand side has terms of the form $\frac{a}{b}q_j(\zeta^{r+j}-1)u^j$. Thus $q_j = 0$ unless $j$ is divisible by $l$ or $j \equiv s \pmod{l^2-1}$. If $j = il$ is divisible by $l$ and is not $s \pmod{l^2-1}$ then we can match $q_{il} = \frac{b}{a}r_{i+s}^l$. The conclusion, from this analysis, is that we have an equality

$$Q(u) = \frac{b}{a}R_0(u)^l + (\text{terms of degree} \equiv s \pmod{l^2-1})\,.$$

Therefore

$$\begin{aligned} P(u) &= u^r Q(u) - R(u) \\ &= \frac{b}{a}u^r R_0(u)^l - u^s R_0(u) + (\text{terms of degree divisible by } l^2-1) \end{aligned}$$

We recall now that

$$aF_\zeta + \zeta^{(l+1)c-lr'}\tilde{Z} = a\zeta^{lr}F_\zeta^l + \zeta^{(l+1)c-lr'}Z.$$

Combining this with

$$F_\zeta = \zeta^{(l+1)c-lr'}(P(\zeta u) - P(u))$$

we get

$$aP(\zeta u) - aP(\zeta u)^l + Z(\zeta u) = aP(u) - aP(u)^l + Z(u)$$

and so this polynomial contains only terms of degree divisible by $l^2 - 1$, in other words

$$\begin{aligned} Z &= a(P^l - P) + (\text{terms of degree divisible by } l^2 - 1) \\ &= (bu^r R_0(u)^l - au^s R_0(u))^l - (bu^r R_0(u)^l - au^s R_0(u)) \\ &\quad + (\text{terms of degree divisible by } l^2 - 1) \end{aligned}$$

*Taking $D = R_0$ in our change-of-variables for $\mathbf{f}'$ therefore transforms $Z$ into a polynomial with all terms of degree divisible by $l^2 - 1$.*

We still wish to reduce $Z$ further, which is easier now that we can assume $Z$ has no terms of low degree except a constant term. If we alter $Z$ via some choice of $D$, we suppose that $D = \sum_i d_i u^i$ has no terms of degree less than $s' - r'$. Then the lowest nonzero term of

$$\frac{b}{a} u^{lr} D^{l^2} - (\frac{b}{a} u^r + u^{ls}) D^l + u^s D$$

has degree $ls' - r'$, and specifically the lowest term is

$$(-\frac{b}{a} d_{s'-r'}^l + d_{s'-r'}) u^{ls'-r'} .$$

The equation $x = (-\frac{b}{a} d_{s'-r'}^l + d_{s'-r'}) u^{ls'-r'}$ may be solved for

$$d_{s'-r'} = \left(1 - \frac{b^2}{a^2}\right)^{-1} \left(x + \frac{b}{a} x^l\right)$$

unless $x \neq 0$, $a = \pm b$. If $x \neq 0$ and $a = b$, then a solution can be found if and only if $x^{l-1} = -1$, while if $x \neq 0$ and $a = -b$ then a solution can be found if and only if $x \in \mathbb{F}_l$.

The terms of degree $i > ls' - r'$ in our transformation of $Z$ are

$$u^s(d_{i-s}u^{i-s}) - u^{ls}(d_{\frac{i-ls}{l}}u^{\frac{i-ls}{l}})^l - \frac{b}{a}u^r(d_{\frac{i-r}{l}}u^{\frac{i-r}{l}})^l + \frac{b}{a}u^{lr}(d_{\frac{i-lr}{l^2}}u^{\frac{i-lr}{l^2}})^{l^2}$$

Since $i-s > (i-ls)/l$, $(i-r)/l$, $(i-lr)/l^2$ for $i > ls' - r'$ we see that taking $d_{i-s} = 0$ for $i$ up to $ls' - r'$ and solving the resulting *linear* equations for $d_{i-s}$ for $i > ls' - r'$, we may alter $Z$ to remove all terms of degree greater than $ls' - r'$ (without introducing a term of degree $ls' - r'$ if there wasn't one to begin with). Therefore unless $ls' - r' = l^2 - 1$, i.e. unless $r' = 1$,$s' = l$, we may take $Z$ to be a constant. In case $r' = 1$,$s' = l$ we may take $Z$ to be a constant plus a term of $z_{l^2-1}u^{l^2-1}$ degree $l^2 - 1$; however, this term can be removed by the above argument if $a \neq b$, or if $a = -b$ and $z_{l^2-1} \in \mathbb{F}_l$. (The case $a = b$ is excluded automatically if $r' = 1$,$s' = l$.) So we can suppose $Z$ is a constant unless $r' = 1$, $s' = l$, $a = -b$, and $z \notin \mathbb{F}_l$.

In case $a = \pm b$ and $s' \geq r'$, let $\eta$ be a choice of $(a/b)^{1/(l-1)}$. We note, for future reference, that for and $d \in \mathbb{F}_l$ by the above argument there is a change-of-$Z$ of the form $D = \eta d u^{s'-r'}$ + (higher terms) which leaves $Z$ fixed.

Now observe that because we have reduced $Z$ to a simple form, we get $aF_\zeta = a\zeta^{lr}F_\zeta^l$, and since $u$ divides $F_\zeta$ we find $F_\zeta = 0$. Then our equation for $E_\zeta$ becomes

$$aE_\zeta = b\left(\frac{(\zeta u)^r E_\zeta}{u^s}\right)^l$$

and so by the usual argument if $E_\zeta$ is nonzero then it is a monomial of degree $u^{l(s'-r')}$ and $s' \geq r'$. Moreover, if $r' = 1$, $s' = l$, then $\zeta^r\zeta^{l(s'-r')} = 1$ and so $\zeta \mapsto \zeta^{-(l+1)c+lr'}E_\zeta$ is homomorphism from $\mathbb{F}_{l^2}^\times$ to an additive $l$-torsion group, so $E_\zeta$ is automatically zero. Note that if $E_\zeta$ is nonzero, then $a/b$ is an $(l-1)^{\text{st}}$ power, and so is $\pm 1$. This is good fortune, for we can hope to use the above transformations

fixing $Z$ (which exist only if $a = \pm b$, $s' \geq r'$) to eliminate $E_\zeta$. It suffices to show that we can make $E_\zeta = 0$ for $\zeta$ a primitive root of $\mathbb{F}_{l^2}^\times$, as then the result follows for the others. Recall that we have chosen $\eta$ with $\eta^{l-1} = a/b$. The coefficient of $u^{s'-r'}$ in $E_\zeta$ is in $\eta\zeta^{-lr'}\mathbb{F}_l$, say $E_\zeta = \eta\zeta^{-lr'}eu^{l(s'-r')}$ with $e \in \mathbb{F}_l$. Suppose $D = \eta du^{s'-r'} +$ (higher terms) is such that its transformation leaves $Z$ fixed. Using $a = -b$ we have $C = D^l = -\eta du^{l(s'-r')} +$ (higher terms). Our new basis element in this transformation is $\tilde{\mathbf{f}}' = \mathbf{f}' + C\mathbf{e} + (\mathbf{e}' \text{ term})$, and we compute

$$\begin{aligned}
[\zeta]\tilde{\mathbf{f}}' &= [\zeta](\mathbf{f}' + C\mathbf{e} + (\mathbf{e}' \text{ term})) \\
&= \zeta^{(l+1)c-lr'}\mathbf{f}' + E_\zeta\mathbf{e} + [\zeta](C\mathbf{e}) + (\mathbf{e}' \text{ term}) \\
&= \zeta^{(l+1)c-lr'}\tilde{\mathbf{f}}' + E_\zeta\mathbf{e} + [\zeta](C\mathbf{e}) - \zeta^{(l+1)c-lr'}C\mathbf{e} + (\mathbf{e}' \text{ term})
\end{aligned}$$

and so we have transformed $E_\zeta$ into

$$E_\zeta - \eta d(\zeta u)^{l(s'-r')}\zeta^{(l+1)c-r'} + \eta d\zeta^{(l+1)c-lr'}u^{l(s'-r')} + \text{ (higher terms)}$$

which equals

$$u^{l(s'-r')}\eta\zeta^{-lr'}(e + d\zeta^{(l+1)c}(1 - \zeta^{ls'-r'})) + \text{ (higher terms)}$$

and since $\zeta^{ls'-r'} \neq 1$ (as we have already handled the case $r' = 1$, $s' = l$) we can certainly select $d$ so as to leave $E_\zeta$ with no term of degree $u^{l(s'-r')}$. However, notice that after applying this transformation to $\mathbf{f}'$, since $Z$ is unchanged we still obtain $F_\zeta = 0$, and now our new $E_\zeta$, having no term of degree $u^{l(s'-r')}$, is also 0!

In summary, we have shown that in every case we may alter $\mathbf{f}'$ so that $Z$ is a constant (or, if $r' = 1$, $s' = l$, $a = -b$, a constant plus a term of degree $l^2 - 1$) and $[\zeta]\mathbf{f}' = \zeta^{(l+1)c-lr'}\mathbf{f}'$. Moreover, in the exceptional situation $r' = 1$, $s' = l$,

$a = -b$, we have not yet used up our latitude to alter $\mathbf{f}'$ in such a way as to leave $Z$ unchanged.

It remains to understand the action of $[\varphi]$ on $\mathbf{f}'$. Suppose $[\varphi]\mathbf{f}' = \mathbf{f}' + C_\varphi \mathbf{e} + D_\varphi \mathbf{e}'$. Then

$$\begin{aligned} [\varphi](\phi_1(u^r\mathbf{f}' + \mathbf{f})) &= [\varphi](a\mathbf{f}' + Z\mathbf{e}') \\ &= a\mathbf{f}' + aC_\varphi \mathbf{e} + (aD_\varphi + Z^{(l)})\mathbf{e}' \end{aligned}$$

where $Z^{(l)}$ denotes the polynomial whose coefficients are the $l^{\text{th}}$ powers of the coefficients of $Z$. We also have

$$\begin{aligned} \phi_1([\varphi](u^r\mathbf{f}' + \mathbf{f})) &= \phi_1(u^r\mathbf{f}' + \mathbf{f} + u^r C_\varphi \mathbf{e} + u^r D_\varphi \mathbf{e}') \\ &= a\mathbf{f}' + Z\mathbf{e}' + \phi_1(D_\varphi(u^r\mathbf{e}' + \mathbf{e}) + (u^r C_\varphi - D_\varphi)\mathbf{e}) \\ &= a\mathbf{f}' + Z\mathbf{e}' + D_\varphi^l a\mathbf{e}' + \left(\frac{u^r C_\varphi - D_\varphi}{u^s}\right)^l b\mathbf{e}\,. \end{aligned}$$

Matching coefficients, we find:

$$aD_\varphi + Z^{(l)} = Z + aD_\varphi^l$$

and

$$aC_\varphi = \left(\frac{u^r C_\varphi - D_\varphi}{u^s}\right)^l b\,.$$

Note that the latter equation implies that $u$ divides $D_\varphi$, hence from the first equation we must have $Z(0)^l = Z(0)$. Thus the constant term of $Z$ is in $\mathbb{F}_l$.

We now consider separately the two outstanding cases. First, suppose that $r' = 1, s' = l, a = -b$, so what we know is that $Z = z_0 + z_{l^2-1}u^{l^2-1}$, with $z_0 \in \mathbb{F}_l$. We then have that $a(D_\varphi - D_\varphi^l)$ consists of a single solitary term of degree $u^{l^2-1}$, from which it follows easily that $D_\varphi$ is a monomial of degree $u^{l^2-1}$ plus a constant

term. But as before $u$ divides $D_\varphi$, so this constant term is 0. Then $D_\varphi^l = 0$ and so $D_\varphi = \left(\frac{z_{l^2-1} - z_{l^2-1}^l}{a}\right) u^{l^2-1}$. Let $\delta = (z_{l^2-1} - z_{l^2-1}^l)/a$, and observe that $\delta^l = -\delta$. Now our equation involving $C_\varphi$ in this situation $r' = 1$, $s' = l$ becomes

$$aC_\varphi = \left(\frac{C_\varphi}{u^{(l-1)^2}} - \delta u^{l-1}\right)^l b$$

and if the lowest-degree term of $C_\varphi$ has degree $(l-1)^2 + k$ with $k < l-1$ this would require $(l-1)^2 + k = kl$, i.e., $k = l+1$, a contradiction. Hence the lowest-degree term of $C_\varphi$ must have degree exactly $l(l-1)$. Now we may apply the usual argument to prove that $C_\varphi$ is a monomial of degree $l(l-1)$. If $C_\varphi = \gamma u^{l(l-1)}$ our equation for $c$ is

$$a\gamma = (\gamma - \delta)^l b$$

Since $a = -b$ this equation yields $-\gamma = \gamma^l - \delta^l$. Taking $l^{\text{th}}$ powers yields $-\gamma^l = \gamma - \delta$, and so $\delta^l = \delta$. Since we already knew $\delta^l = -\delta$ it follows that $\delta = 0$, and so $z_{l^2-1} \in \mathbb{F}_l$. Recall, however, that $z_{l^2-1} \in \mathbb{F}_l$ was exactly the condition we needed in this case in order to be able to alter $Z$ to make $z_{l^2-1} = 0$! Performing this transformation, we may now assume $Z$ is a constant. The last thing we need to do in this case is to show that $C_\varphi$ can be taken to be 0, and to do this we need to use up our latitute in altering $\mathbf{f}'$ via a transformation which leaves $Z$ fixed. Notice now that $\gamma^l = -\gamma$, so $\gamma = \eta\theta$ for some $\theta \in \mathbb{F}_l$. We set $D = \eta\lambda u^{s'-r'} +$ (higher terms) $= \eta\lambda u^{l-1} +$ (higher terms), with $\lambda \in \mathbb{F}_l$, so that $C = -\eta\lambda u^{l(l-1)} +$ (higher terms) and the corresponding transformation $\tilde{\mathbf{f}}' = \mathbf{f}' + C\mathbf{e} + (\mathbf{e}'$ term) leaves $Z$

fixed. Then

$$\begin{aligned}
[\varphi]\tilde{\mathbf{f}}' &= [\varphi]\mathbf{f}' + [\varphi]C\mathbf{e} + (\mathbf{e}' \text{ term}) \\
&= \mathbf{f}' + C_\varphi \mathbf{e} + C^{(l)}\mathbf{e} + (\mathbf{e}' \text{ term}) \\
&= \tilde{\mathbf{f}}' + (C_\varphi + C^{(l)} - C)\mathbf{e} + (\mathbf{e}' \text{ term}) \\
&= \tilde{\mathbf{f}}' + \eta(\theta - \eta^{l-1}\lambda + \lambda)\mathbf{e} + (\mathbf{e}' \text{ term})
\end{aligned}$$

and since $\eta^{l-1} = -1$ we will take $\lambda = -\theta/2$. This shows that with this choice of $\mathbf{f}'$, the resulting $C_\varphi$ has no $u^{l(l-1)}$ term. However, we still have $Z$ constant, and by the arguments over the last few pages we still see that $[\zeta]\mathbf{f}' = \zeta^{(l+1)c-lr'}\mathbf{f}'$, and we still find that $D_\varphi$ must still be 0 and $C_\varphi$ is still a monomial of degree $u^{l(l-1)}$. Now that $C_\varphi$ has no $u^{l(l-1)}$ term, it must be 0. This completes the case $r' = 1$, $s' = l$, $a = -b$.

In the other cases, we know already that $Z$ is a constant in $\mathbb{F}_l$, and so $D_\varphi = D_\varphi^l$. Thus $D_\varphi$ is both a constant and divisible by $u$, and so $D_\varphi = 0$. This leaves us with

$$aC_\varphi = b\left(\frac{u^r C_\varphi}{u^s}\right)^l.$$

By our usual arguments, if $C_\varphi \neq 0$ then $a = \pm b$, $s' \geq r'$, and $C_\varphi = \eta\gamma u^{l(s'-r')}$ with $\gamma \in \mathbb{F}_l$ and for $\eta$ any choice of $\eta^{l-1} = a/b$. We wish to show that $\gamma = 0$. To do so, we look at the relation $[\zeta]^l = [\varphi][\zeta][\varphi]$. Witness:

$$\begin{aligned}
[\varphi][\zeta][\varphi](\mathbf{f}') &= [\varphi][\zeta](\mathbf{f}' + \eta\gamma u^{l(s'-r')})\mathbf{e} \\
&= [\varphi](\zeta^{(l+1)c-lr'}\mathbf{f}' + \eta\gamma(\zeta u)^{l(s'-r')}\zeta^{(l+1)c-r'}\mathbf{e} \\
&= \zeta^{(l+1)c-r'}(\mathbf{f}' + \eta\gamma u^{l(s'-r')}\mathbf{e}) + \eta^l\gamma\zeta^{s'-r'}\zeta^{(l+1)c-lr'}u^{l(s'-r')}\mathbf{e}
\end{aligned}$$

and so if $\gamma \neq 0$ it follows that

$$\zeta^{(l+1)c-r'} + \eta^{l-1}\zeta^{(l+1)c-lr'+s'-r'} = 0$$

and so

$$\eta^{l-1}\zeta^{s'-lr'} = -1$$

for *all* $\zeta \in \mathbb{F}_{l^2}^{\times}$. It quickly follows that $\eta^{l-1} = -1$ (so $a = -b$) and $\zeta^{s'-lr'} = 1$ for all $\zeta$, so $l^2 - 1$ divides $s' - lr'$. But among the pairs of $r'$, $s'$ we are considering in this section, the only way that $l^2 - 1 \,|s' - lr'$ is to have $r' = 1$, $s' = l$. This leaves us squarely in the case $r' = 1$, $s' = l$, $a = -b$ case which we have already completed! Thus $\gamma = 0$.

To summarize, we have proven

**Theorem 9.1.** *For the $\mathcal{M}$ under consideration, any $\mathcal{N} \in \mathrm{Ext}^1(\mathcal{M}, \mathcal{M})$ with descent data has the form*

$$\mathcal{N} = \langle \mathbf{e}, \mathbf{e}', \mathbf{f}\,, \mathbf{f}\,' \rangle$$

*with*

$$\mathcal{N}_1 = \langle u^s\mathbf{e}, u^r\mathbf{e}' + \mathbf{e}, u^s\mathbf{f}\,, u^r\mathbf{f}\,' + \mathbf{f}\,\rangle$$

*and*

$$\phi_1(u^s\mathbf{e}) = b\mathbf{e}\,,\ \phi_1(u^r\mathbf{e}' + \mathbf{e}) = a\mathbf{e}'$$

$$\phi_1(u^s\mathbf{f}\,) = b\mathbf{f}\, + v\mathbf{e}\,,\ \phi_1(u^r\mathbf{f}\,' + \mathbf{f}\,) = a\mathbf{f}\,' + z\mathbf{e}'$$

*with $v$, $z \in \mathbb{F}_l$, and descent data satisfying*

$$[\zeta](\mathbf{e}) = \zeta^{(l+1)d-ls'}\mathbf{e}\,,\ [\zeta](\mathbf{f}\,) = \zeta^{(l+1)d-ls'}\mathbf{f}$$

$$[\zeta](\mathbf{e}') = \zeta^{(l+1)c-lr'}\mathbf{e}'\,,\ [\zeta](\mathbf{f}\,') = \zeta^{(l+1)c-lr'}\mathbf{f}\,'$$

$$[\varphi](\mathbf{e}) = \mathbf{e}\,,\ [\varphi](\mathbf{e}') = \mathbf{e}'\,,\ [\varphi](\mathbf{f}\,) = \mathbf{f}\,\,,\ [\varphi](\mathbf{f}\,') = \mathbf{f}\,'\,.$$

*Therefore this* $\mathrm{Ext}^1$ *is at most two-dimensional over* $\mathbb{F}_l$*.*

9.1. **Dieudonné module relations.** It remains to determine which of these extensions satisfies the desired relations on their Dieudonné module. We check from the compatibility between Breuil theory and Dieudonné theory described in section 4 that each of the above extensions yields a Dieudonné module with basis $\mathbf{v}, \mathbf{w}, \mathbf{v}', \mathbf{w}'$ on which $F$ and $V$ act through the matrices

$$F = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -b & 0 & 0 & 0 \\ -v & -b & 0 & 0 \end{pmatrix}$$

and

$$V = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/a & 0 & 0 & 0 \\ -z/a^2 & 1/a & 0 & 0 \end{pmatrix}.$$

(Note that these matrices only describe the actions of $F$, $V$ on this particular basis: the actions of $F$, $V$ are extended to the full Dieudonné module *semilinearly.*)

To see this, we will have $\mathbf{v}, \mathbf{w}, \mathbf{v}', \mathbf{w}'$ correspond respectively to the images of $\mathbf{e}, \mathbf{f}, \mathbf{e}', \mathbf{f}'$ in $\mathcal{N}/u\mathcal{N}$. Observe that $\phi(\mathbf{e}) = \phi_1(u^{l^2-1}\mathbf{e}) = u^r b\mathbf{e}$ which maps to 0 in $\mathcal{N}/u\mathcal{N}$, and similarly $\phi(\mathbf{f}) = 0$ in $\mathcal{N}/u\mathcal{N}$. This gives the first two rows of the matrix for $F$. Next, $\phi(\mathbf{e}') = \phi_1(u^{l^2-1}\mathbf{e}') = \phi_1(u^s(u^r\mathbf{e}' + \mathbf{e}) - u^s\mathbf{e}) = -b\mathbf{e}$ in $\mathcal{N}/u\mathcal{N}$, while similarly $\phi(\mathbf{f}')$ in $\mathcal{N}/u\mathcal{N}$ is $-\phi_1(u^s\mathbf{f}) = -b\mathbf{e} - v\mathbf{f}$.

To obtain the matrix for $V$, we note that $\phi_1^{-1}(\mathbf{e}) = b^{-1}u^s\mathbf{e}$ is 0 in $\mathcal{N}/u\mathcal{N}$, and similar for $\phi_1^{-1}(\mathbf{f})$. On the other hand $\phi_1^{-1}(\mathbf{e}') = a^{-1}(u^r\mathbf{e}' + \mathbf{e})$, which is $a^{-1}\mathbf{e}$ in

$\mathcal{N}/u\mathcal{N}$, and

$$\phi_1^{-1}(\mathbf{f}\,') = a^{-1}(u^r\mathbf{f}\,' + \mathbf{f}\,) - \frac{z}{a^2}(u^r\mathbf{e}' + \mathbf{e})$$

which indeed is $a^{-1}\mathbf{f} - \frac{z}{a^2}\mathbf{e}$ in $\mathcal{N}/u\mathcal{N}$.

We know that in this case $T = \text{Teich}(\det(\overline{\rho}))(s)$ reduces in $\mathbb{F}_l$ to $ab$, and so $F + TV = 0$ precisely when

$$-v - \frac{b}{a}z = 0\,.$$

The resulting space of extensions is therefore at most 1-dimensional. This completes the proof of Theorem 2.2.

## 10. An example

This section describes joint work with W. Stein which is still in progess. Let $C$ be the curve

$$y^2 + (x^3 + x^2 + 1)y = -x^5 - x^4 - 2x^3 - 4x^2 - 2x - 1\,.$$

X. Wang [Wan95] noted that the space $S_2(175)$ contains a pair of quadratic conjugate newforms $f, f'$, and found that the 2-dimensional quotient $A$ of $J_0(175)$ corresponding to this pair of newforms is canonically principally polarized; numerical calculations using theta functions suggested to Wang that $A = \text{Jac}(C)$, and so $\text{Jac}(C)$ is conjecturally modular of level 175.

Let $l = 5$, and let $\rho$ be the global Galois representation attached to $f$. The form $f$ has coefficients in $\mathbb{Q}(\sqrt{5})$, hence $\rho$ is defined over $\mathbb{Q}_5(\sqrt{5})$ and has mod 5 reduction $\overline{\rho}$ over $\mathbb{F}_5$. By a theorem of [BCDT], since $\overline{\rho}$ is odd and has cyclotomic determinant (by the Weil pairing), we know $\overline{\rho}$ is modular. Since 25 exactly divides 175, the 5-adic representation $\rho$ associated to $f$ should be potentially semi-stable

with tame 5-type. Since this representation conjecturally comes from $\mathrm{Jac}(C)$, the Hodge-Tate weights should be 0 and 1.

Examining $\overline{f}$, a mod 5 reduction of $f$, one sees that the enough different pairs ($p \bmod 5, \mathrm{a_p}$) appear in order to force $\rho|_{G_{\mathbb{Q}(\sqrt{5})}}$ to be absolutely irreducible.

A calculation using the modular forms package HECKE in the computational package Magma shows that the newform $f$ is not equal to $g \otimes \chi$ for $g$ of lower level and $\chi$ of conductor 5. We conclude that the 5-type of $\rho$ must be of the form $\tilde{\omega}_2^m \oplus \tilde{\omega}_2^{5m}$ rather than $\tilde{\omega}^i \oplus \tilde{\omega}^j$.

Next, we find a mod 5 form $\overline{g}$ of weight 4 level 7 such that $\overline{f}$ is a twist of $\overline{g}$. Moreover, $\overline{g}$ is of low level and weight and is ordinary ($a_5(\overline{g}) \neq 0$) and so by results of Deligne the representation of $G_{\mathbb{Q}_5}$ corresponding to $\overline{g}$ (which is simply a twist of $\overline{\rho}$) is ordinary. Finally, we check that a companion form does not exist for $\overline{g}$, and so $\overline{\rho}$ is ordinary and not a direct sum of two characters.

These calculations verify that the conditions of theorem 2.4 ought to hold for $\rho$, provided that Wang's prediction is indeed correct. Therefore, we hope to use theorem 2.4 to prove that $\rho$ is modular. We know automatically that $\overline{\rho}$ is modular, and so we may still use most of the above computations with modular forms in order to prove that $\rho$ is modular. However, for example, we would also need to see that $\mathrm{Jac}(C)$ has good reduction over $\mathbb{Q}_5(5^{1/24})$ and not over $\mathbb{Q}_5(5^{1/4})$, which we have not yet done.

## References

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$, to appear, J.A.M.S.

[BM00] C. Breuil and A. Mézard, *Multiplicités modulaires et représentations de* $\mathrm{GL}_2(\mathbf{Z}_p)$ *et de* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *en* $l = p$, preprint, 2000.

[Bre98] C. Breuil, *Schémas en groupes sur un anneau de valuation discrèt complet très ramifié*, Orsay preprint, 1998.

[Bre99a] ———, *Modules faiblement admissibles et groupes p-divisibles*, prépublication Université de Paris-Sud, 1999.

[Bre99b] ———, *Représentations semi-stables et modules fortement divisibles*, Invent. math. **136** (1999), no. 1, 89–122.

[Bre99c] ———, *Schémas en groupe et modules filtrés*, C. R. Acad. Sci. Paris. Sér. I Math. **328** (1999), no. 2, 93–97.

[Bre00] ———, *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. (2) **152** (2000), no. 2, 489–549.

[CDT99] B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J.A.M.S. **12** (1999), 521–567.

[CF00] P. Colmez and J.-M. Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. math. **140** (2000), no. 1, 1–43.

[Con] B. Conrad, *Wild ramification and deformation rings*, Münster preprint.

[Del71] P. Deligne, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki, Exposés 347–363, Lecture Notes in Mathematics, vol. 179, Springer-Verlag, 1971, pp. 139–172.

[Dia96] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. 144 (1996), 137–166.

[DS74] P. Deligne and J-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup. **7** (1974), 507–530.

[Edi92] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. math. **109** (1992), no. 3, 563–594.

[FI93] J.-M. Fontaine and L. Illusie, *p-adic periods: a survey*, Proceedings of the Indo-French Conference on Geometry, Hindustan Book Agency, 1993, pp. 57–93.

[FM95] J.-M. Fontaine and B. Mazur, *Geometric Galois Representations*, Elliptic curves, modular forms, & Fermat's last theorem (J. Coates and S.-T. Yau, eds.), International Press, 1995, pp. 41–78.

[Fon94] J.-M. Fontaine, *Representations p-adiques semi-stables*, Astérisque **223** (1994), 113–184.

[Lan80] R. P. Langlands, *Base Change for GL(2)*, Annals of Math. Studies **96** (1980).

[Maz95] B. Mazur, *An introduction to the deformation theory of Galois representations*, Modular forms and Fermat's last theorem, Springer-Verlag, 1995, pp. 243–311.

[Ram93] R. Ramakrishna, *On a variant of Mazur's deformation functor*, Compositio Math. **87** (1993), no. 3, 269–286.

[Ray74] M. Raynaud, *Schémas en groupes de type* $(p, p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

[Ser87] J-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[Ser89] ———, *Abelian l-adic representations and elliptic curves*, Advanced Book Classics, Addison-Wesley, 1989, with the collaboration of Willem Kuyk and John Labute.

[Shi71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.

[SW97] C. Skinner and A. Wiles, *Ordinary representations and modular forms*, Proc. Nat. Adam. Sci. U.S.A. **94** (1997), no. 20, 10520–10527.

[Tat67] J. Tate, *p-divisible groups*, Proc. Conf. Local Fields (Driebergen, 1966), Springer-Verlag, 1967, pp. 158–183.

[Tay00] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, preprint, 2000.

[Tun81] J. Tunnell, *Artin's Conjecture for representations of octahedral type*, Bull. AMS **5** (1981), 173–175.

[TW95] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **142** (1995), 553–572.

[Wan95] X. Wang, 2-*dimensional simple factors of* $J_0(N)$, Manuscripta Math. **87** (1995), 179–197.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics **142** (1995), 443–551.