JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Byoung Du (BD) KIM

Local conditions of adjoint representations with supersingular reduction, and representable functors of deformations with higher weight liftings

Tome 37, nº 1 (2025), p. 325-355.

https://doi.org/10.5802/jtnb.1323

CENTRE MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **37** (2025), 325–355

Local conditions of adjoint representations with supersingular reduction, and representable functors of deformations with higher weight liftings

par Byoung Du (BD) KIM

Résumé. Soit W l'anneau des entiers d'une extension de $\mathbb{Q}_p$, et soit $T_E = W^2$ une représentation cristalline de rang 2 de $G_{\mathbb{Q}_p}$ à poids de Hodge–Tate $[0,1]$ ayant réduction non ordinaire. On note $\overline{T}_E$ la représentation résiduelle de T_E. Soit $l \geq 2$ et soit N un entier fixé suffisamment grand, qui ne dépend que de T_E. Nous montrons que le groupe $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ d'extensions admettant des relèvements cristallins de poids $[0, l-1]$ qui sont eux-mêmes extensions de représentations de $G_{\mathbb{Q}_p}$ congrues à T_E modulo p^N (cf. Définition 2.30), est isomorphe au groupe d'extensions finies plates $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ (cf. [18, Chapitre 1.1]). En outre, nous construisons le foncteur $\mathcal{D}$ des déformations de $\overline{T}_E$ de poids $[0, l-1]$ ayant relèvements d'un certain type et satisfaisant certaines congruences avec T_E et montrons que $\mathcal{D}$ admet une enveloppe représentable. Nous conjecturons que $t_{\mathcal{D}} \subset \mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ et $V_{\mathbf{T}_\mathfrak{m}} \otimes W/\mathfrak{m}_W \in \mathcal{D}(\mathbf{T}_\mathfrak{m} \otimes W/\mathfrak{m}_W)$, où $\mathbf{T}$ est l'algèbre de Hecke $\mathbf{T}_l(\Gamma_1(M))$, $\mathbf{m}$ son idéal maximal donné par une forme propre de poids l et de niveau $\Gamma_1(M)$ dont la représentation galoisienne est congrue à T_E modulo p^N, et $V_{\mathbf{T}_\mathfrak{m}}$ la représentation galoisienne associée. Enfin, nous donnons des résultats à l'appui de cette conjecture.

Abstract. Let $T_E = W^2$ be a rank 2 crystalline $G_{\mathbb{Q}_p}$-representation of weights $[0,1]$ with non-ordinary reduction where W is the ring of integers of some extension of $\mathbb{Q}_p$, and let $\overline{T}_E$ be its residual representation. Suppose $l \geq 2$ and fix some big enough N which only depends on T_E. We show that the group $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ (Definition 2.30) of extensions with crystalline liftings of weights $[0, l-1]$, which are themselves extensions of $G_{\mathbb{Q}_p}$-representations which are congruent to $T_E \pmod{p^N}$, is isomorphic to the group of finite flat extensions $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ ([18, Chapter 1.1]). In addition, we construct a certain functor $\mathcal{D}$ of deformations of $\overline{T}_E$ with liftings of certain type and weights $[0, l-1]$, satisfying certain congruences with T_E, show $\mathcal{D}$ has a representable hull, and demonstrate some evidence that $t_{\mathcal{D}} \subset \mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ and

Manuscrit reçu le 24 novembre 2023, révisé le 12 novembre 2024, accepté le 28 décembre 2024.
2020 *Mathematics Subject Classification.* 11S25, 11R34, 12G05, 11F85, 11G99.
Mots-clefs. Local conditions of adjoint representations, Gorenstein Hecke algebras, patching, congruences of p-adic L-functions.

$V_{\mathbf{T}_\mathfrak{m}} \otimes W/\mathfrak{m}_W \in \mathcal{D}(\mathbf{T}_\mathfrak{m} \otimes W/\mathfrak{m}_W)$ where $\mathbf{T}$ is the Hecke algebra $\mathbf{T}_l(\Gamma_1(M))$, $\mathbf{m}$ is its maximal ideal given by a weight l eigenform of level $\Gamma_1(M)$ whose Galois representation is congruent modulo p^N to T_E, and $V_{\mathbf{T}_\mathfrak{m}}$ is its associated Galois representation.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}_p$, $T_E = T_pE$, and $\overline{T}_E = T_E/pT_E(\cong E[p])$. Recall that $\mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$ is the set of extensions of $\overline{T}_E$ by itself as representations of $G_{\mathbb{Q}_p}$, i.e., the set of $G_{\mathbb{Q}_p}$-representations $\hat{\overline{T}}$ with a short exact $G_{\mathbb{Q}_p}$-equivariant sequence $0 \to \overline{T}_E \to \hat{\overline{T}} \to \overline{T}_E \to 0$.

Now, suppose $E/\mathbb{Q}_p$ has good reduction, and moreover, has supersingular reduction. (T_E in this paper will be a little more general: $T_E \otimes \mathbb{Q}_p$ will be a dimension 2 vector space over some local field with linear $G_{\mathbb{Q}_p}$-action, crystalline of Hodge–Tate weights $[0, 1]$. But, for this introduction, an elliptic curve over $\mathbb{Q}_p$ will be enough.) Let $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ be the set of extensions in $\mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$ given by p-torsions of finite flat group schemes over $\mathbb{Z}_p$. As an application of Fontaine and Laffaille's theory ([4, 5]) of classifying finite group schemes over local rings by Honda systems, we have $\dim_{\mathbb{F}_p} \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E) = 2$ ([13]), which can be used in important ways as in [17]. (Taylor and Wiles' patching needs more than this, in addition to patching itself. More on this below.)

We would like to consider a higher weight analogue of $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$, and to do so, we interpret it as follows: We can think of the elements of $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ as $G_{\mathbb{Q}_p}$-representations $\hat{\overline{T}}_E$ (with $\overline{T}_E \to \hat{\overline{T}}_E \to \overline{T}_E$) which have crystalline, weight $[0, 1]$ liftings $\overline{T}_E(\cong \mathbb{Z}_p^4)$ with $T \to \hat{\overline{T}}_E \to T$ for some $G_{\mathbb{Q}_p}$-representation T where $T \equiv T_E \pmod p$. Then, for a fixed $l \geq 2$, we can consider its weight $[0, l-1]$ analogue $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$, the set of $\hat{\overline{T}}$ (with $\overline{T}_E \to \hat{\overline{T}} \to \overline{T}_E$) which have crystalline, weight $[0, l-1]$ liftings $\hat{T}$ with $T \to \hat{T} \to T$ where $T \equiv T_E \pmod{p^N}$. (N is determined by E.) See Definition 2.30. The congruences $T \equiv T_E \pmod{p^N}$ help apply the techniques from [7].

Are $\dim_{\mathbb{F}_p} \mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ and $\dim_{\mathbb{F}_p} \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ equal? The first part of this paper answers this question. (Throughout the introduction, we may write $\mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$ for $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ in short.)

Theorem 2.31. $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E) \cong \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$.

Theorem 2.31 is supposed to help control the number of generators of certain deformation rings R_Q as the set Q of auxiliary primes varies in patching if R_Q is known (more on this below). But, patching requires more parts than Theorem 2.31. For the rest of the paper, we work on completing the rest of them as much as possible.

First, from now on, let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p, and f_E be its associated newform of some level which divides M ($(M,p)=1$). Again, f_E can be more generally any newform of weight 2, but for the introduction, an elliptic curve is fine. Suppose there is an eigenform f of level $\Gamma_1(M)$ and weight l so that $a_q(f_E) \equiv a_q(f) \pmod{p^N}$ for all but finitely many primes q (the same assumption in [7]). We can assume $W = \mathbb{Z}_p[f]$ for now.

One needs to define a representable functor of deformations. We define (Definition 3.3) $\mathcal{D}$ as the set of deformations of $\overline{T}_E$ which have crystaline liftings of certain type ("$\mathcal{S}$"; see Definition 3.2), weights $[0, l-1]$, and certain congruence properties with T_E. As a first step, we show $\mathcal{D}$ is a category that has a (pro-)representable hull by some $R \in \widehat{\mathcal{C}}_{\overline{k}}$ (Propositions 3.4 and 3.5). This is almost as good as a representable functor. (We will not worry about $\mathcal{D}_Q$ for sets of auxiliary primes Q for now because we believe they will be similar to $\mathcal{D}$. Similarly, we will not worry about $\mathbf{T}_Q$ below, either.)

Then, one needs $t_{\mathcal{D}} \subset \mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$ (which is to say every representation $V_{\overline{k}[\epsilon]} = \overline{k}[\epsilon]^2 \in \mathcal{D}(\overline{k}[\epsilon])$ is in $\mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$). This is necessary to interpret $t_{\mathcal{D}}$ as a Selmer group of $\mathrm{ad}^0(\overline{T}_E)$ with local condition $\mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$. We show that in some special cases, namely, when $V_{\overline{k}[\epsilon]}$ has a lifting $V_R (= R^2)$ where $R = W[\epsilon_1] \times_C W[\epsilon_2]$ some $C \in \mathcal{C}_{\overline{k}}$ (Proposition 3.6). Generally, R should be a more complicated fiber product (Definitionss 3.2 and 3.3), but will it need an essentially different proof? The author is not yet ready to answer this, but is hopeful that Proposition 3.6 points to a general proof.

Another important piece of groundwork for patching is the following: Let $\mathbf{T} := \mathbf{T}_l(\Gamma_1(M))$, a Hecke algebra generated over W. Let $\mathfrak{m} = \ker(\mathbf{T} \to \overline{k})$ given by $t \mapsto a_t$ for each $t \in \mathbf{T}$ where $tf = a_t f$. There is a well-known $G_{\mathbb{Q}}$-representation $V_{\mathbf{T}_\mathfrak{m}} (\cong \mathbf{T}_\mathfrak{m}^2)$, unramified outside the prime divisors of M, etc. The last piece we need is $V_{\mathbf{T}_\mathfrak{m}} \otimes W/(\pi) \in \mathcal{D}(\mathbf{T}_\mathfrak{m} \otimes W/(\pi))$ (so that there is $R \to \mathbf{T}_\mathfrak{m} \otimes W/(\pi)$).

Again we show this only in a special case, which we hope will shed light on the general case. We assume there are only two eigenforms g_1, g_2 of level $\Gamma_1(M)$ and weight l which are congruent to $f \pmod{\pi}$ (one of which is of course f itself) so that $\mathbf{T}_\mathfrak{m} \hookrightarrow W \times W$ by assuming W is big enough if necessary. Towards to the end of Section 3, we present a simple argument for showing $\mathbf{T}_\mathfrak{m} \cong W \times_{W/(\pi^r)} W$. (The argument itself is purely algebraic, and has little to do with Hecke algebras.) $W \times_{W/(\pi^r)} W$ itself is not in $\mathcal{S}$ unless $r = 1$, but probably it can be resolved by changing the definition of $\mathcal{S}$ slightly. Last, there is the issue that eigenforms $g (\equiv f \pmod{\pi})$ are not necessarily $g \equiv f \pmod{p^N}$. We briefly discuss how one may resolve this. Again, the general case should be more complicated. But, will it be essentially different from the above case? Just as the first issue, we hope our argument for the above case points towards a general proof.

To sum up, we obtain complete solutions for some technical problems, but we only partially solve some other problems. We hope readers will get the impression that this work is heading in the right direction.

Last, we will briefly discuss the initial motivation for this work. Choi and I ([1]) showed congruences between two-variable (analytic) p-adic L-functions of congruent modular forms (of different congruent weights) when p is non-ordinary, but we had to assume certain Hecke algebras (of weights higher than 2 in particular) are Gorenstein. I noted that Taylor and Wiles' patching not only shows $R \overset{\sim}{\to} T$, but also R, T are Gorenstein. But, as noted above, to apply patching to higher weight Hecke algebras for non-ordinary p, many technical issues need to be resolved, and this work is, in some sense, a result of the effort to resolve them. On the other hand, some important pieces are already in place for patching in this instance. For example, we have modular congruences in [8], which generalize [15], and Diamond's version of patching ([3]), which likely works well with the congruences in [8].

2. Congruent cocycles of higher weight adjoint representations

Throughout, k is a finite extension of $\mathbb{Q}_p$ with residue field $\bar{k}$. (So, $\bar{k}$ is a finite field, not the algebraic closure.) We fix a uniformizer π of k. Let $\mathfrak{m} = \mathfrak{m}_{\mathcal{O}_k}(= (\pi))$. We fix $\overline{T} = \bar{k}^2$ with action of $G_{\mathbb{Q}_p}$.

Throughout, where V is a representation of $G_{\mathbb{Q}_p}$, its Dieudonne module $D(V)$ is given by $(V \otimes B_{cris})^{G_{\mathbb{Q}_p}}$ which has φ action and filtration through B_{cris} and B_{dR}. The convention of Hodge–Tate weights is fixed in such a way that where T_E is the p-adic Tate module of an elliptic curve $E/\mathbb{Q}_p$ (with good reduction) and $V_E = T_E \otimes \mathbb{Q}_p$, the weights of V_E are $[0, 1]$. (So, $\mathrm{Fil}^{-1} D(V_E) = D(V_E)$, and $\dim \mathrm{Fil}^0 D(V_E) = 1$.)

When we speak of p^N, we allow $N \in \mathbb{Q}$ in the following sense: where $\frac{1}{v} = v_p(\pi)$, $p^{\frac{1}{v}} = \pi$. (In and of itself, this is wrong, but it will make sense in a proper context, and we want to use it so that the presentation looks similar to [7].)

2.1. Suppose $V_E \cong k^2$ has continuous $G_{\mathbb{Q}_p}$-action, is crystalline with Hodge–Tate weights $[0, 1]$, and the characteristic of φ on $D(V_E) = (B_{cris} \otimes V_E)^{G_{\mathbb{Q}_p}}$ is $x^2 - \frac{a_p}{\epsilon \cdot p} x + \frac{1}{\epsilon \cdot p}$ for some p-adic unit ϵ. We choose $m_E \in D(V_E)$ satisfying $\varphi m_E \in \mathrm{Fil}^0 D(V_E)$.

For any $a, b \in k$, let $\beta = a + b\varphi$. In the following, the notation $V_{X_E^\beta}$ suggests it is a π-adic Tate module of a group scheme X_E^β, but we do not need to assume it for now. In any case, we can indeed construct such X_E^β, and we will indeed use it. See the proof of Proposition 2.25. We let $V_{X_E^\beta} \cong k^4$ be a crystalline representation of $G_{\mathbb{Q}_p}$ (which implicitly implies $G_{\mathbb{Q}_p}$ acts continuously) so that $D(V_{X_E^\beta})$ satisfies:

$$0 \longrightarrow D(V_E) \longrightarrow D(V_{X_E^\beta}) \longrightarrow D(V_E) \longrightarrow 0$$

such that for a lifting $\widehat{m}_E \in D(V_{X_E^\beta})$ of m_E satisfying $\varphi\widehat{m}_E \in \mathrm{Fil}^0 D(V_{X_E^\beta})$, we have

$$\left(\varphi^2 - \frac{a_p}{\epsilon \cdot p}\varphi + \frac{1}{\epsilon \cdot p}\right)\widehat{m}_E = \beta m_E.$$

Let α, α' be the roots of $x^2 - \frac{a_p}{\epsilon \cdot p}x + \frac{1}{\epsilon \cdot p} = 0$.

Assumption 2.1 (Supersingular reduction assumption)**.** From now on, we assume neither of α, α' is a p-adic unit. If their p-adic valuations are different, we choose α to be the one with

$$-\frac{1}{2} \leq v_p(\alpha) < 0.$$

In other words, we assume that the group scheme E which V_E is supposed to be associated to has supersingular/non-ordinary reduction. Everything in this section probably works without Assumption 2.1, but in the ordinary reduction case, we have a much easier method for dealing with our question.

Definition 2.2. We let

$$v_E = (\varphi - \alpha')m_E, \quad \widehat{v}_E = (\varphi - \alpha')^2\widehat{m}_E.$$

Then, the following is clear.

Proposition 2.3. *We have*

$$(\varphi - \alpha)v_E = 0, \quad (\varphi - \alpha)\widehat{v}_E = \beta v_E.$$

In the following, $\beta_m (\in W(R) \subset A_{cris} \subset B_{cris})$'s are as in [12], i.e., we let

$$\widetilde{\beta}_m = (\zeta_{p^{m+n}})_{n\geq 0} \in R \overset{\text{def}}{=} \left\{(x^{(n)})_{n\geq 0} \,\middle|\, x^{(n)} \in \mathcal{O}_{\mathbb{C}_p}, (x^{(n+1)})^p = x^{(n)}\right\},$$

for every $m \geq 0$, and

$$\beta_m = [\widetilde{\beta}_m] \in W(R).$$

See [7] for how they are used because the following method is adopted and adapted from it.

Definition 2.4. We define $\delta_n^\beta \in A_{cris}[\frac{1}{p}] \otimes D(V_{X_E^\beta})$ by

$$\begin{bmatrix} \delta_n^\beta \\ \theta_n^\beta \end{bmatrix} = \sum_{m=0}^{\infty} (\varphi^m(\beta_n) - 1) \otimes \begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix}^m \cdot \begin{bmatrix} \widehat{v}_E \\ v_E \end{bmatrix}$$

We may drop β from $\delta_n^\beta, \theta_n^\beta$ and simply write δ_n, θ_n where appropriate.

Definition 2.5. We let

$$v'_E = (\varphi - \alpha) m_E, \quad \widehat{v}'_E = (\varphi - \alpha)^2 \widehat{m}_E.$$

Let

$$M(V_E) = \mathcal{O}_k(m_E, \varphi(m_E)) = \mathcal{O}_k \cdot m_E + \mathcal{O}_k \cdot \varphi(m_E) \subset D(V_E).$$

Recall that by [11, Section 2.3.4 Lemme], or [6, Proposition 6.24], for some $s \geq 0$,

$$A_{cris} \otimes M(V_E) \subset (\varphi - 1) p^{-s} \operatorname{Fil}^0 \left(A_{cris} \otimes M(V_E)\right). \tag{2.1}$$

Similar to the above, let

$$M(V_{X_E^\beta}) = \mathcal{O}_k \left(\widehat{m}_E, m_E, \varphi(\widehat{m}_E), \varphi(m_E)\right) \subset D(V_{X_E^\beta}).$$

Then, we have the following.

Proposition 2.6. *There is*

$$\begin{bmatrix} \lambda_n \\ \nu_n \end{bmatrix} \in p^{-2s-1} \operatorname{Fil}^0 A_{cris} \otimes M(V_{X_E^\beta}) \oplus p^{-s-\frac{1}{2}} \operatorname{Fil}^0 A_{cris} \otimes M(V_E)$$

so that

$$(\varphi - 1) \left(\begin{bmatrix} \delta_n^\beta \\ \theta_n^\beta \end{bmatrix} + \begin{bmatrix} \lambda_n \\ \nu_n \end{bmatrix} \right) = 0.$$

Proof. Let $\sum_i a_i \otimes n_i \in A_{cris} \otimes M(V_{X_E^\beta})$, and let $\overline{n}_i = n_i \pmod{D(V_E)}$ (so $\overline{n}_i \in M(V_{X_E^\beta})/M(V_E) \cong M(V_E)$). By (2.1) above,

$$\sum_i a_i \otimes \overline{n}_i = (\varphi - 1) \sum_j a_j \otimes \overline{n}_j$$

for some $\sum_j a_j \otimes \overline{n}_j \in p^{-s} \operatorname{Fil}^0 A_{cris} \otimes M(V_E)$. Choose a lifting $n_j \in M(V_{X_E^\beta})$ of each n_j. Then, we have

$$\sum_i a_i \otimes n_i - (\varphi - 1) \sum_j a_j \otimes n_j \in p^{-s} A_{cris} \otimes M(V_E).$$

Again by (2.1) above, we can find some $\sum_k a_k \otimes n_k \in p^{-2s} \operatorname{Fil}^0 A_{cris} \otimes M(V_E)$ so that

$$\sum_i a_i \otimes n_i = (\varphi - 1) \left(\sum_j a_j \otimes n_j + \sum_k a_k \otimes n_k \right).$$

In other words, we have shown

$$A_{cris} \otimes M(V_{X_E^\beta}) \subset (\varphi - 1) p^{-2s} \operatorname{Fil}^0 A_{cris} \otimes M(V_{X_E^\beta}).$$

(The point is that s only depends on V_E, not on $V_{X_E^\beta}$.)

Now, since $\varphi\widehat{v}_E = \alpha\widehat{v}_E + \beta v_E$ and $\varphi v_E = \alpha v_E$,

$$\begin{aligned}(\varphi-1)\begin{bmatrix}\delta_n^\beta\\ \theta_n^\beta\end{bmatrix} &= \sum_{m=0}^{\infty}(\varphi^{m+1}(\beta_n)-1)\otimes\begin{bmatrix}\alpha & \beta\\ 0 & \alpha\end{bmatrix}^m\cdot\begin{bmatrix}\varphi\widehat{v}_E\\ \varphi v_E\end{bmatrix}\\ &\qquad -\sum_{m=0}^{\infty}(\varphi^{m}(\beta_n)-1)\otimes\begin{bmatrix}\alpha & \beta\\ 0 & \alpha\end{bmatrix}^m\cdot\begin{bmatrix}\widehat{v}_E\\ v_E\end{bmatrix}\\ &= \sum_{m=0}^{\infty}(\varphi^{m+1}(\beta_n)-1)\otimes\begin{bmatrix}\alpha & \beta\\ 0 & \alpha\end{bmatrix}^{m+1}\cdot\begin{bmatrix}\widehat{v}_E\\ v_E\end{bmatrix}\\ &\qquad -\sum_{m=0}^{\infty}(\varphi^{m}(\beta_n)-1)\otimes\begin{bmatrix}\alpha & \beta\\ 0 & \alpha\end{bmatrix}^m\cdot\begin{bmatrix}\widehat{v}_E\\ v_E\end{bmatrix}\\ &= -(\beta_n-1)\otimes\begin{bmatrix}\widehat{v}_E\\ v_E\end{bmatrix}.\end{aligned}$$

(Since $\widehat{v}_E \in p^{-1}M(V_{X_E^\beta}))$ by the above discussion, for some $\lambda_n \in p^{-2s-1}\operatorname{Fil}^0 A_{cris}\otimes M(V_{X_E^\beta})$ and $\nu_n \in p^{-s-\frac{1}{2}}\operatorname{Fil}^0 A_{cris}\otimes M(V_E)$, we have

$$(\beta_n-1)\otimes\begin{bmatrix}\widehat{v}_E\\ v_E\end{bmatrix} = (\varphi-1)\begin{bmatrix}\lambda_n\\ \nu_n\end{bmatrix}. \qquad \square$$

Later, we may need to write

$$\lambda_n = \widehat{t}_n\otimes\widehat{v}_E + t_n\otimes v_E + \widehat{t}'_n\otimes\widehat{v}'_E + t'_n\otimes v'_E$$

for some $\widehat{t}_n, t_n, \widehat{t}'_n, t'_n \in p^{-2s-2}A_{cris}$.(On the other hand, we may not need ν_n again.)

Definition 2.7. We set

$$T^\beta = \mathcal{O}_k[G_{\mathbb{Q}_p}]\left((\delta_n+\lambda_n)^{\sigma_n}-(\delta_n+\lambda_n)\;\middle|\; n\geq 0,\ \sigma_n\in G_{\mathbb{Q}_p(\zeta_{p^n})}\right).$$

By construction, T^β is an $\mathcal{O}_k$-submodule of $\operatorname{Fil}^0(B_{cris}\otimes D(V_{X_E^\beta}))^{\varphi=1} \cong V_{X_E^\beta}$, and it will become clear that indeed it is a lattice (see Proposition 2.11 and [7, Lemma 3.3]).

Definition 2.8. Fix an integer $l \geq 2$. Let V_l be a 2-dimensional k-vector space on which $G_{\mathbb{Q}_p}$ acts continuously so that

- V_l is crystalline with Hodge–Tate weights $[0, l-1]$,
- the characteristic of φ on $D(V_l)$ is $x^2 - \frac{a_l}{\epsilon' p^{l-1}}x + \frac{1}{\epsilon' p^{l-1}}$ for some $a_l \in \mathcal{O}_k$ and a p-adic unit ϵ' such that where α_l, α'_l are roots of $x^2 - \frac{a_l}{\epsilon' p^{l-1}}x + \frac{1}{\epsilon' p^{l-1}} = 0$, we have

$$\alpha_l \equiv \alpha \pmod{p^N}$$

  for some $N > 0$ (as mentioned, we allow $N \in \frac{1}{v}\mathbb{Z}$ where $v_p(\pi) = \frac{1}{v}$).

Remark 2.9. Definition 2.8 implies that V_l is congruent to V_E (or more precisely, a lattice inside V_l is congruent to a lattice inside V_E) if N is big enough ("enough" depends on V_E). See [7].

Now, suppose $G_{\mathbb{Q}_p}$ acts continuously on some crystalline $\widehat{V}_l^{\beta} \cong k^4$ (which *we will also denote by* $\widehat{V}$ *or* $\widehat{V}_l$ for simplicity) satisfying

$$0 \longrightarrow V_l \longrightarrow \widehat{V}_l^{\beta} \longrightarrow V_l \longrightarrow 0$$

so that for some $m_l \in D(V_l)$ with $\varphi m_l \in \mathrm{Fil}^0 D(V_l)$ and its lifting $\widehat{m}_l \in D(\widehat{V}_l^{\beta})$ satisfying $\varphi \widehat{m}_l \in \mathrm{Fil}^0 D(\widehat{V}_l^{\beta})$,

$$\left(\varphi^2 - \frac{a_l}{\epsilon' p^{l-1}}\varphi + \frac{1}{\epsilon' p^{l-1}}\right)\widehat{m}_l = \beta m_l,$$

(which determines $\widehat{V}_l^{\beta}$).

Definition 2.10.

(a) Similar to Definition 2.5, let

$$v_l = (\varphi - \alpha_l')m_l, \quad \widehat{v}_l = (\varphi - \alpha_l')^2 \widehat{m}_l,$$

and define

$$M(\widehat{V}_l^{\beta}) = \mathcal{O}_k\left(\widehat{m}_l, m_l, \varphi(\widehat{m}_l), \varphi(m_l)\right) \subset M(\widehat{V}_l^{\beta}).$$

(b) We define $\delta_n^{(l),\beta} \in A_{cris}[\frac{1}{p}] \otimes M(V_l^{\beta})$ by

$$\begin{bmatrix} \delta_n^{(l),\beta} \\ \theta_n^{(l),\beta} \end{bmatrix} = \sum_{m=0}^{\infty} (\varphi^m(\beta_n) - 1) \otimes \begin{bmatrix} \alpha_l & \beta \\ 0 & \alpha_l \end{bmatrix}^m \cdot \begin{bmatrix} \widehat{v}_l \\ v_l \end{bmatrix}.$$

Again, we may drop β from $\delta_n^{(l),\beta}$ and simply write $\delta_n^{(l)}$ where appropriate.

It is easy to see the following.

Proposition 2.11.

$$\delta_n^{\beta} = \sum_{m=0}^{\infty} \alpha^m (\varphi^m(\beta_n) - 1) \otimes \widehat{v}_E + \beta \sum_{m=1}^{\infty} m\alpha^{m-1}(\varphi^m(\beta_n) - 1) \otimes v_E,$$

$$\delta_n^{(l),\beta} = \sum_{m=0}^{\infty} \alpha_l^m (\varphi^m(\beta_n) - 1) \otimes \widehat{v}_l + \beta \sum_{m=1}^{\infty} m\alpha_l^{m-1}(\varphi^m(\beta_n) - 1) \otimes v_l.$$

Recall (before Definition 2.7) that we write

$$\lambda_n = \widehat{t}_n \otimes \widehat{v}_E + t_n \otimes v_E + \widehat{t}_n' \otimes \widehat{v}_E' + t_n' \otimes v_E'.$$

Proposition 2.12. *Suppose $N > 4s+4$. Then, there are $\widehat{t}_n^{(l)}, t_n^{(l)} \in A_{cris}[\frac{1}{p}] \otimes \mathcal{O}_k$ so that*

$$\widehat{t}_n^{(l)} \equiv \widehat{t}_n, \quad t_n^{(l)} \equiv t_n \pmod{p^N p^{-2s} A_{cris} \otimes \mathcal{O}_k)}$$

$$(\varphi - 1)\left(\delta_n^{(l),\beta} + \widehat{t}_n^{(l)} \otimes \widehat{v}_l + t_n^{(l)} \otimes v_l\right) = 0.$$

Proof. On the whole, this proof follows that of [7, Proposition 3.8].

From the proof of Proposition 2.6, recall$(\beta_n - 1) \otimes \widehat{v}_E = (\varphi - 1)\lambda_n$. In other words,

$$(\beta_n - 1) \otimes \widehat{v}_E = (\varphi - 1)\left(\widehat{t}_n \otimes \widehat{v}_E + t_n \otimes v_E\right).$$

(It also implies $0 = (\varphi - 1)(\widehat{t}'_n \otimes \widehat{v}'_E + t'_n \otimes v'_E)$, but it will not be relevant in this argument.)

By expansion, we have

$$\alpha\varphi(\widehat{t}_n) - \widehat{t}_n = \beta_n - 1,$$
$$\beta\varphi(\widehat{t}_n) + \alpha\varphi(t_n) = t_n.$$

Then, compute

$$\begin{aligned}
&(\varphi - 1)\left(\widehat{t}_n \otimes \widehat{v}_l + t_n \otimes v_l\right) \\
&\qquad = \left(\alpha_l\varphi(\widehat{t}_n) - \widehat{t}_n\right) \otimes \widehat{v}_l + \left(\beta\varphi(\widehat{t}_n) + \alpha_l\varphi(t_n) - t_n\right) \otimes v_l \\
&\qquad = (\alpha_l - \alpha)\varphi(\widehat{t}_n) \otimes \widehat{v}_l + (\beta_n - 1) \otimes \widehat{v}_l + (\alpha_l - \alpha)\varphi(t_n) \otimes v_l.
\end{aligned}$$

Since $(\varphi - 1)\delta_n^{(l),\beta} = -(\beta_n - 1) \otimes \widehat{v}_l$, we get

$$(\varphi - 1)\left(\delta_n^{(l),\beta} + \widehat{t}_n \otimes \widehat{v}_l + t_n \otimes v_l\right) = (\alpha_l - \alpha)\varphi(\widehat{t}_n) \otimes \widehat{v}_l + (\alpha_l - \alpha)\varphi(t_n) \otimes v_l.$$

Note that, by Proposition 2.6 and Definition 2.8, $(\alpha_l - \alpha)\varphi(\widehat{t}_n)$, $(\alpha_l - \alpha)\varphi(t_n) \in p^N p^{-2s-2} A_{cris}$.

Now, suppose $\widehat{t}'_n \otimes \widehat{v}_l + t'_n \otimes v_l$ is a maximal element in

$$\mathcal{T} = \left\{\widehat{t}'_n \otimes \widehat{v}_l + t'_n \otimes v_l \;\middle|\; \widehat{t}'_n \equiv \widehat{t}_n, t'_n \equiv t_n \pmod{p^{N-4s-4} A_{cris})}\right\}$$

in the sense that

$$\begin{aligned}
&(\varphi - 1)\delta_n^{(l)} + (\varphi - 1)\left(\widehat{t}'_n \otimes \widehat{v}_l + t'_n \otimes v_l\right) \\
&\qquad\qquad = -(\beta_n - 1) \otimes \widehat{v}_l + (\varphi - 1)\left(\widehat{t}'_n \otimes \widehat{v}_l + t'_n \otimes v_l\right) \\
&\qquad\qquad = \widehat{c} \otimes \widehat{v}_l + c \otimes v_l
\end{aligned}$$

is closest to 0. ("Closest" means $\widehat{c}, c \in p^{t-2s-2} A_{cris}$ for biggest t, which could be ∞.) In fact, we will show $t = \infty$ (thus $\widehat{c}, c = 0$).

By the above, $\widehat{t}_n \otimes \widehat{v}_l + t_n \otimes v_l \in \mathcal{T}$, and $t \geq N$.

As in the proof of Proposition 2.6, there are $\widehat{d}, d \in p^{t-4s-4}A_{cris}$ (which is well-defined because $N > 4s+4$) so that

$$(\varphi - 1)(\widehat{d} \otimes \widehat{v}_E + d \otimes v_E) = \widehat{c} \otimes \widehat{v}_E + c \otimes v_E.$$

Thus,

$$- (\beta_n - 1) \otimes \widehat{v}_l + (\varphi - 1)\left((\widehat{t}'_n - \widehat{d}) \otimes \widehat{v}_l + (t'_n - d) \otimes v_l\right)$$
$$= (\alpha - \alpha_l)\varphi(\widehat{d}) \otimes \widehat{v}_l + (\alpha - \alpha_l)\varphi(d) \otimes v_l.$$

Since $(\alpha - \alpha_l)\varphi(\widehat{d}), (\alpha - \alpha_l)\varphi(\widehat{d}) \in p^{N+t-4s-4}A_{cris}$, $N > 2s+2$, and (clearly) $(\widehat{t}'_n - \widehat{d}) \otimes \widehat{v}_l + (t'_n - d) \otimes v_l \in \mathcal{T}$ (because $t \geq N$), the above implies $\widehat{t}'_n \otimes \widehat{v}_l + t'_n \otimes v_l$ is not maximal unless $t = \infty$. □

Definition 2.13.

$$v'_l = (\varphi - \alpha_l)m_l, \quad \widehat{v}'_l = (\varphi - \alpha_l)^2 \widehat{m}_l.$$

Proposition 2.14. *There are* $\widehat{t}_n^{(l)'}, t_n^{(l)'} \in A_{cris}[\frac{1}{p}] \otimes \mathcal{O}_k$ *so that*

$$\widehat{t}_n^{(l)} \otimes \widehat{v}_l + t_n^{(l)} \otimes v_l + \widehat{t}_n^{(l)'} \otimes \widehat{v}'_l + t_n^{(l)'} \otimes v'_l \in \mathrm{Fil}^0\left(A_{cris}\left[\frac{1}{p}\right] \otimes M(\widehat{V}_l^{\beta})\right).$$

Proof. We can write

$$\widehat{v}_l = \widehat{a}\widehat{m}_l + \widehat{b}\varphi(\widehat{m}_l) + \widehat{c}m_l + \widehat{d}\varphi(m_l),$$
$$\widehat{v}'_l = \widehat{a}'\widehat{m}_l + \widehat{b}'\varphi(\widehat{m}_l) + \widehat{c}'m_l + \widehat{d}'\varphi(m_l),$$
$$v_l = cm_l + d\varphi(m_l),$$
$$v'_l = c'm_l + d'\varphi(m_l),$$

for some coefficients in k. Clearly $\widehat{a}', c' \neq 0$ (as well as $\widehat{a}, c$). Noting that $\varphi(\widehat{m}_l), \varphi(m_l) \in \mathrm{Fil}^0 M(\widehat{V}_l^{\beta})$, we can see that the claim is true by simple linear algebra. □

Recall that we also let $\widehat{V}$ denote $\widehat{V}_l^{\beta}$.

Definition 2.15.

(a) $\mathbb{A}_l = A_{cris}[\frac{1}{p}] \otimes \widehat{v}'_l + A_{cris}[\frac{1}{p}] \otimes v'_l$.
(Technically, we should write $1 \otimes \widehat{v}'_l$ instead of $\widehat{v}'_l$ and so on, but it would be detrimental for readability.)

(b) $\mathbb{A}_l^0 = \mathbb{A}_l \cap \mathrm{Fil}^0(B_{dR} \otimes D(\widehat{V}))$.

Following [7, Section 3.3], we make the following: Since $B_{cris} \otimes \widehat{V} = B_{cris} \otimes D(\widehat{V})$, from $0 \to \mathbb{Q}_p \to B_{cris} \to (B_{dR}/B_{dR}^0) \oplus B_{cris} \to 0$ (given by $b \mapsto (b, (\varphi - 1)b)$), we have

$$0 \longrightarrow \widehat{V} \longrightarrow (B_{cris} \otimes D(\widehat{V}))^{\varphi=1} \longrightarrow \frac{B_{dR} \otimes D(\widehat{V})}{\mathrm{Fil}^0(B_{dR} \otimes D(\widehat{V}))} \longrightarrow 0.$$

In other words,

$$\frac{\big(B_{cris}\otimes D(\widehat{V})\big)^{\varphi=1}}{\widehat{V}}\cong\frac{B_{dR}\otimes D(\widehat{V})}{\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big)}. \tag{2.2}$$

Proposition 2.16. *The map*

$$\big(B_{cris}\otimes D(\widehat{V})\big)^{\varphi=1}+\mathbb{A}_l\longrightarrow\frac{B_{dR}\otimes D(\widehat{V})}{\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big)}$$

has kernel $\widehat{V}+\mathbb{A}_l^0$.

Proof. Through (2.2), we have a *surjective* map

$$\iota: B_{dR}\otimes D(\widehat{V})\longrightarrow\frac{\big(B_{cris}\otimes D(\widehat{V})\big)^{\varphi=1}}{\widehat{V}}\longrightarrow\frac{\big(B_{cris}\otimes D(\widehat{V})\big)^{\varphi=1}+\mathbb{A}_l}{\widehat{V}+\mathbb{A}_l}.$$

By design, we have $\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big)\subset\ker\iota$, and so

$$\mathrm{Ker}\overset{\mathrm{def}}{=}\ker\left(\big(B_{cris}\otimes D(\widehat{V})\big)^{\varphi=1}+\mathbb{A}_l\longrightarrow\frac{B_{dR}\otimes D(\widehat{V})}{\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big)}\right)\subset\widehat{V}+\mathbb{A}_l.$$

Since $\widehat{V}\subset\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big)$, if $\widehat{v}+a\in\mathrm{Ker}$ for some $\widehat{v}\in\widehat{V}$ and $a\in\mathbb{A}_l$,

$$a\in\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big)\cap\mathbb{A}_l=\mathbb{A}_l^0.$$

On the other hand, if $a\in\mathbb{A}_l^0$, by definition $a\in\mathrm{Ker}$. Hence

$$\mathrm{Ker}=\widehat{V}+\mathbb{A}_l^0.$$

□

Proposition 2.17. *We set*

$$\lambda_n^{(l)}=\widehat{t}_n^{(l)}\otimes\widehat{v}_l+t_n^{(l)}\otimes v_l+\widehat{t}_n^{(l)\prime}\otimes\widehat{v}_l'+t_n^{(l)\prime}\otimes v_l',$$

and recall we let $\delta_n^{(l)}$ *denote* $\delta_n^{(l),\beta}$ *for simplicity.*

Then, for all $\sigma_n\in G_{\mathbb{Q}_p(\zeta_{p^n})}$,

$$(\sigma_n-1)\left(\delta_n^{(l)}+\lambda_n^{(l)}\right)\in\widehat{V}+\mathbb{A}_l^0.$$

Proof. By Proposition 2.11, and because $\zeta_{p^n}\equiv\beta_n \pmod{\mathrm{Fil}^1(B_{dR})}$ by [12, Section 1.5.3], we have

$$\delta_n^{(l)}\equiv\sum_{m=0}^{n}\alpha_l^m\left(\zeta_{p^{n-m}}-1\right)\otimes\widehat{v}_l$$
$$+\beta\sum_{m=1}^{n}m\alpha_l^{m-1}\left(\zeta_{p^{n-m}}-1\right)\otimes v_l\ \left(\mathrm{mod}\,\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big)\right).$$

(Also see the proof of [7, Corollary 3.11] for clarification.) Thus, we have

$$(\sigma_n-1)\delta_n^{(l)}\in\mathrm{Fil}^0\big(B_{dR}\otimes D(\widehat{V})\big).$$

By Proposition 2.14, $\lambda_n^{(l)} \in \mathrm{Fil}^0(A_{cris}[\frac{1}{p}] \otimes D(\widehat{V}))$. Combined, we have

$$(\sigma_n - 1)\left(\delta_n^{(l)} + \lambda_n^{(l)}\right) \in \mathrm{Fil}^0(B_{dR} \otimes D(\widehat{V})).$$

Because of $\widehat{t}_n^{(l)'}, t_n^{(l)'} \in A_{cris}[\frac{1}{p}] \otimes \mathcal{O}_k$ (by Proposition 2.14) and Proposition 2.12, we have

$$\delta_n^{(l)} + \lambda_n^{(l)} \in \left(B_{cris} \otimes D(\widehat{V})\right)^{\varphi=1} + \mathbb{A}_l.$$

Thus, our claim follows from Proposition 2.16. □

In the following, recall $\mathbb{A}_l = A_{cris}[\frac{1}{p}] \otimes \widehat{v}_l' + A_{cris}[\frac{1}{p}] \otimes v_l'$ from Definition 2.15.

Definition 2.18.

(a) $\mathrm{proj}_l :$
$$\widehat{V} + \mathbb{A}_l^0 \longrightarrow A_{cris}\left[\frac{1}{p}\right] \otimes \widehat{v}_l + A_{cris}\left[\frac{1}{p}\right] \otimes v_l$$
$$\widehat{x} \otimes \widehat{v}_l + x \otimes v_l + \widehat{x}' \otimes \widehat{v}_l' + x' \otimes v_l' \longmapsto \widehat{x} \otimes \widehat{v}_l + x \otimes v_l.$$

(b) Similarly,

$\mathrm{proj}_E :$
$$\widehat{V}_{X_E^\beta} \longrightarrow A_{cris}\left[\frac{1}{p}\right] \otimes \widehat{v}_E + A_{cris}\left[\frac{1}{p}\right] \otimes v_E$$
$$\widehat{x} \otimes \widehat{v}_E + x \otimes v_E + \widehat{x}' \otimes \widehat{v}_E' + x' \otimes v_E' \longmapsto \widehat{x} \otimes \widehat{v}_E + x \otimes v_E.$$

Then, clearly $\mathrm{proj}_l, \mathrm{proj}_E$ are $G_{\mathbb{Q}_p}$-equivariant. Also, by construction, $\mathbb{A}_l^0 \subset \ker(\mathrm{proj}_l)$, hence

$$\mathrm{proj}_l\left(\widehat{V} + \mathbb{A}_l^0\right) = \mathrm{proj}_l\left(\widehat{V}\right).$$

Proposition 2.19. *Suppose $\beta \neq 0$. Then, we have*

$$\mathrm{proj}_l\left(\widehat{V} + \mathbb{A}_l^0\right) = \mathrm{proj}_l\left(\widehat{V}\right) \cong \widehat{V},$$
$$\mathrm{proj}_E(\widehat{V}_{X_E^\beta}) \cong \widehat{V}_{X_E^\beta}.$$

Proof. This is a little harder than the case in [7] because $\widehat{V}$ and so on are not irreducible.

We consider $\widehat{V}$, V_l as subgroups of $B_{cris} \otimes D(\widehat{V})$ and $B_{cris} \otimes D(V_l)$ respectively. Then, $D(\widehat{V})/D(V_l) \xrightarrow{\sim} D(V_l)$ gives an explicit surjective map $\widehat{V} \to V_l$, which gives a short exact sequence $0 \to V_l \to \widehat{V} \to V_l \to 0$.

Similar to above, we can define (like in [7]): (Here, V_l is considered a subgroup of $\frac{B_{cris} \otimes D(\hat{V})}{B_{cris} \otimes D(V_l)}$)

$$\mathrm{proj}_{V_l} : V_l + \mathrm{Fil}^0\left(A_{cris} \otimes \widehat{v}_l\right) \longrightarrow A_{cris}\left[\frac{1}{p}\right] \otimes \widehat{v}_l$$
$$\widehat{x} \otimes \widehat{v}_l + \widehat{x}' \otimes \widehat{v}_l' \longmapsto \widehat{x} \otimes \widehat{v}_l.$$

We can see the image of proj_{V_l} is isomorphic to V_l.

Since

$$\delta_n^{(l)} \equiv \sum_{m=0}^{\infty} \alpha_l^m(\zeta_{p^{n-m}} - 1) \otimes \widehat{v}_l \ \left(\mathrm{mod}\, \mathrm{Fil}^0(B_{dR} \otimes D(\widehat{V})) + A_{cris}\left[\frac{1}{p}\right] \otimes v_l\right),$$

the image of the cocycle

$$\left(\sigma_n \in G_{\mathbb{Q}_p(\zeta_{p^n})} \longmapsto (\sigma_n - 1)\left(\delta_n^{(l)} + \lambda_n^{(l)}\right)\right)$$

under $\widehat{V}_l + \mathbb{A}_l^0 \overset{\mathrm{proj}_l}{\to} A_{cris}[\frac{1}{p}] \otimes \widehat{v}_l + A_{cris}[\frac{1}{p}] \otimes v_l \to A_{cris}[\frac{1}{p}] \otimes \widehat{v}_l$ is non-zero. Thus, there is some $\sigma_n \in G_{\mathbb{Q}_p(\zeta_{p^n})}$ so that $(\sigma_n - 1)\left(\delta_n^{(l)} + \lambda_n^{(l)}\right)$ generates $V_l (\cong \widehat{V}/V_l)$ because V_l is irreducible.

Since $\widehat{V}$ is non-split, $(\sigma_n - 1)\left(\delta_n^{(l)} + \lambda_n^{(l)}\right)$ generates $\widehat{V}$, thus $\mathrm{proj}_l\left(\widehat{V} + \mathbb{A}_l^0\right) \cong \widehat{V}$.

The case for $\mathrm{proj}_E(\widehat{V}_{X_E^\beta})$ is similar. ☐

Alternatively, we may be able to prove $\mathrm{proj}_l(\widehat{V}) \cong \widehat{V}$ from $\mathrm{proj}_E(\widehat{V}_E) \cong \widehat{V}_E$ by Proposition 2.22.

Definition 2.20.

$$\Phi : \frac{A_{cris}[\frac{1}{p}] \otimes \widehat{v}_E + A_{cris}[\frac{1}{p}] \otimes v_E}{p^{N-2s}\left(A_{cris} \otimes \widehat{v}_E + A_{cris} \otimes v_E\right)} \longrightarrow \frac{A_{cris}[\frac{1}{p}] \otimes \widehat{v}_l + A_{cris}[\frac{1}{p}] \otimes v_l}{p^{N-2s}\left(A_{cris} \otimes \widehat{v}_l + A_{cris} \otimes v_l\right)}$$
$$\widehat{a} \otimes \widehat{v}_E + a \otimes v_E \longmapsto \widehat{a} \otimes \widehat{v}_l + a \otimes v_l$$

Now we recall the following:

Proposition 2.21 ([7, Lemma 3.3])**.** *Suppose $n \geq 0$ and $m \in \mathbb{Z}$ with $n \geq m$. For every $\sigma_n \in G_{\mathbb{Q}_p(\zeta_{p^n})}$,*

$$\beta_m^{\sigma_n} - \beta_m \in p^{n-m} A_{cris}.$$

From this, we immediately have the following:

Proposition 2.22. *Suppose $N > 4s + 4$. For all $m, n \geq 0$ and all $\sigma_n \in G_{\mathbb{Q}_p(\zeta_{p^n})}$,*

$$\Phi\left(\mathrm{proj}_E\left((\sigma_n - 1)\left(\delta_n + \lambda_n\right)\right)\right) = \mathrm{proj}_l\left((\sigma_n - 1)\left(\delta_n^{(l)} + \lambda_n^{(l)}\right)\right).$$

(The right-hand side is well-defined because of Proposition 2.17, and similarly, the left-hand side is well-defined because of Proposition 2.6.)

Proof. Since $\alpha_l^m \equiv \alpha^m \pmod{p^{-m/2}p^N}$ and $\varphi^m(\beta_n) = \beta_{n-m}$, by Proposition 2.21

$$(\alpha^m \varphi^m(\beta_n))^{\sigma_n} - \alpha^m \varphi^m(\beta_n) \equiv (\alpha_l^m \varphi^m(\beta_n))^{\sigma_n} - \alpha_l^m \varphi^m(\beta_n) \pmod{p^N A_{cris}}.$$

So, the claim (of congruence) on δ_n and $\delta_n^{(l)}$ follows (see Proposition 2.11). The claim on λ_n and $\lambda_n^{(l)}$ follows from Proposition 2.12. $\square$

Proposition 2.23. *Assume $N > 4s+4$. Recall T^β from Definition 2.7. Similar to Definition 2.10*(b)*, set*

$$T_l^\beta = \mathcal{O}_k[G_{\mathbb{Q}_p}]\left(\left(\delta_n^{(l)}+\lambda_n^{(l)}\right)^{\sigma_n} - \left(\delta_n^{(l)}+\lambda_n^{(l)}\right) \,\middle|\, n \geq 0,\ \sigma_n \in G_{\mathbb{Q}_p(\zeta_{p^n})}\right).$$

Then, Φ induces an isomorphism

$$\begin{aligned}\mathrm{proj}_E(T^\beta)/\,\mathrm{proj}_E(T^\beta) \cap p^{N-2s}(A_{cris}\otimes \widehat{v}_E + A_{cris}\otimes v_E)\\ \cong \mathrm{proj}_l(T_l^\beta)/\,\mathrm{proj}_l(T_l^\beta)\cap p^{N-2s}(A_{cris}\otimes\widehat{v}_l + A_{cris}\otimes v_l).\end{aligned}$$

Proof. This immediately follows from the definitions of T^β, T_l^β, and Proposition 2.22. $\square$

Let T_E be any $G_{\mathbb{Q}_p}$-invariant lattice inside V_E, which is unique up to scalar multiplication because $\overline{T}_E = T_E/\mathfrak{m}T_E$ is irreducible. Similarly, let T_l be any $G_{\mathbb{Q}_p}$-invariant lattice inside V_l. Note $\overline{T}_l(\overset{\text{def}}{=} T_l/\mathfrak{m}T_l) \cong \overline{T}_E$. (Again, see [7].)

Note that any lattice T inside $V_{X_E^\beta}$ satisfies

$$0 \longrightarrow \overline{T}_E \longrightarrow T/\mathfrak{m}T \longrightarrow \overline{T}_E \longrightarrow 0.$$

Definition 2.24.

(a) A lattice T inside $V_{X_E^\beta}$ is *residually non-split* if the above short exact sequence is non-split.

(b) Similarly, a lattice T inside $\widehat{V}$ is *residually non-split* if

$$0 \longrightarrow \overline{T}_l \longrightarrow T/\mathfrak{m}T \longrightarrow \overline{T}_l \longrightarrow 0$$

is non-split.

In the following proof, $T_\pi X$ denotes the π-adic Tate module of the group scheme X (if $\mathcal{O}_k$ acts on X), and $V_\pi X = T_\pi X \otimes \mathbb{Q}_p$.

Proposition 2.25. *If $\beta = 1$ or $\beta = \varphi$, then $V_{X_E^\beta}$ has a residually non-split lattice T inside it.*

Proof. Suppose $E/\mathbb{Z}_p$ is a smooth formal group scheme with Honda type (M, L) where $M \cong \mathcal{O}_k[\mathbf{F}]/(\mathbf{F}^2 - a_p\mathbf{F} + \epsilon\cdot p)$ as an $\mathcal{O}_k[\mathbf{F}]$-module (and $\mathbf{V}$ acts accordingly), and L can be considered as a free $\mathcal{O}_k$-submodule of M with $L/pL \cong M/\mathbf{F}M$. So, $\mathcal{O}_k$ acts on E through M, L.

Suppose X is a formal group scheme (over $\mathbb{Z}_p$) with $\mathcal{O}_k$-action and Honda type (M_X, L_X) so that

$$0 \longrightarrow M \longrightarrow M_X \longrightarrow M \longrightarrow 0, \quad 0 \longrightarrow L \longrightarrow L_X \longrightarrow L \longrightarrow 0.$$

Then, X is characterized by the following: For a generator $l \in L$ and its lifting $\widehat{l} \in L_X$,

$$(\mathbf{F}^2 - a_p\mathbf{F} + \epsilon \cdot p)\widehat{l} = (a + b\mathbf{F})l$$

for some $a, b \in \mathcal{O}_k$.

Then, we can identify $D(V_\pi X) \cong \mathrm{Hom}(M_X, k)$ where φ acts on every $f \in \mathrm{Hom}(M_X, \cdot)$ by

$$(\varphi f)(m) = f(\mathbf{F}^{-1}m).$$

(We can understand $\mathbf{F}^{-1}$ as $\mathbf{V}/p$ because M_X is torsion-free.)

Similarly, we can identify $D(V_\pi E)$ (as a submodule of $D(V_\pi X)$) with $\mathrm{Hom}(M_X/M, k)$, or with $\mathrm{Hom}(M, k)$ (as a quotient of $D(V_\pi X)$ depending on the context). Again, the action $(\varphi f)(m) = f(\mathbf{F}^{-1}m)$ makes sense because $M, M_X/M$ are torsion-free.

From this, we will find the structure of $D(V_\pi X)$. (More specifically, we will find β so that $V_\pi X \cong V_{X_E^\beta}$.)

First, we construct $m_X^* \in D(V_\pi X) = \mathrm{Hom}(M_X, k)$ as follows:

$$\begin{aligned} m_X^* : M_X &\longrightarrow k \\ l &\longmapsto 1 \\ \mathbf{F}l &\longmapsto 0 \\ \widehat{l} &\longmapsto 0 \\ \mathbf{F}\widehat{l} &\longmapsto 0 \end{aligned}$$

Also we construct $m^* \in D(V_\pi E) = \mathrm{Hom}(M_X/M, k)$ by

$$\begin{aligned} m^* : M_X/M &\longrightarrow k \\ l &\longmapsto 0 \\ \mathbf{F}l &\longmapsto 0 \\ \widehat{l} &\longmapsto 1 \\ \mathbf{F}\widehat{l} &\longmapsto 0. \end{aligned}$$

Next, we will find $A, B \in k$ with $\left(\varphi^2 - \frac{a_p}{\epsilon \cdot p}\varphi + \frac{1}{\epsilon \cdot p}\right) m_X^* = (A + B\varphi)m^*$ (so that $V_{X_E^{A+B\varphi}} \cong V_\pi X$). This is somewhat tedious. It is enough to note

$$\mathbf{F}^{-1}l = \frac{a_p}{\epsilon \cdot p}l - \frac{1}{\epsilon \cdot p}\mathbf{F}l,$$

$$\mathbf{F}^{-1}\widehat{l} = \left(\frac{a \cdot a_p}{(\epsilon \cdot p)^2} + \frac{b}{\epsilon \cdot p}\right) l - \frac{a}{(\epsilon \cdot p)^2}\mathbf{F}l + \frac{a_p}{\epsilon \cdot p}\widehat{l} - \frac{1}{\epsilon \cdot p}\mathbf{F}\widehat{l},$$

thus

$$\begin{aligned} \varphi m^* : l &\longmapsto 0 \\ \mathbf{F}l &\longmapsto 0 \\ \widehat{l} &\longmapsto \frac{a_p}{\epsilon \cdot p} \\ \mathbf{F}\widehat{l} &\longmapsto 1 \end{aligned}$$

$$\begin{aligned} \varphi m_X^* : l &\longmapsto \frac{a_p}{\epsilon \cdot p} \\ \mathbf{F}l &\longmapsto 1 \\ \widehat{l} &\longmapsto \frac{a \cdot a_p}{(\epsilon \cdot p)^2} + \frac{b}{\epsilon \cdot p} \\ \mathbf{F}\widehat{l} &\longmapsto 0 \end{aligned}$$

$$\begin{aligned} \varphi^2 m_X^* : l &\longmapsto \frac{a_p^2}{(\epsilon \cdot p)^2} - \frac{1}{\epsilon \cdot p} \\ \mathbf{F}l &\longmapsto \frac{a_p}{\epsilon \cdot p} \\ \widehat{l} &\longmapsto \frac{2a \cdot a_p^2}{(\epsilon \cdot p)^3} + \frac{2b \cdot a_p}{(\epsilon \cdot p)^2} - \frac{a}{(\epsilon \cdot p)^2} \\ \mathbf{F}\widehat{l} &\longmapsto \frac{a \cdot a_p}{(\epsilon \cdot p)^2} + \frac{b}{\epsilon \cdot p}. \end{aligned}$$

So, $\left(\varphi^2 - \frac{a_p}{\epsilon \cdot p}\varphi + \frac{1}{\epsilon \cdot p}\right) m_X^*$ sends

$$\begin{aligned} \widehat{l} &\longmapsto \frac{a \cdot a_p^2}{(\epsilon \cdot p)^3} + \frac{b \cdot a_p}{(\epsilon \cdot p)^2} - \frac{a}{(\epsilon \cdot p)^2} \\ \mathbf{F}\widehat{l} &\longmapsto \frac{a \cdot a_p}{(\epsilon \cdot p)^2} + \frac{b}{\epsilon \cdot p}, \end{aligned}$$

and $(A + B\varphi)m^*$ sends

$$\begin{aligned} \widehat{l} &\longmapsto A + B \cdot \frac{a_p}{\epsilon \cdot p} \\ \mathbf{F}\widehat{l} &\longmapsto B. \end{aligned}$$

By setting them equal, we have

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -(\epsilon \cdot p)^2 & 0 \\ a_p(\epsilon \cdot p) & \epsilon \cdot p \end{bmatrix} \begin{bmatrix} A \\ B \end{bmatrix}.$$

Note that the following are equivalent:

- $T_\pi X / \pi T_\pi X$ is non-split,
- $X[\pi]$ is non-split,

- $0 \longrightarrow M/\pi M \longrightarrow M_X/\pi M_X \longrightarrow M/\pi M \longrightarrow 0$ is non-split,
- $(a,b) \not\equiv (0,0) \pmod{\pi}$.

Now, suppose $\beta(= A + B\varphi) = 1$. By scaling $D(V_\pi E) \subset D(V_\pi X)$, we can assume $A = \frac{1}{p^2}, B = 0$. Then,

$$(a,b) = (-\epsilon^2, \epsilon a_p/p) \not\equiv (0,0) \pmod{\pi}.$$

On the other hand, suppose $\beta(= A + B\varphi) = \varphi$. Again by scaling, we can assume $A = 0, B = \frac{1}{p}$. Then,

$$(a,b) = (0,\epsilon) \not\equiv (0,0) \pmod{\pi}.$$

Each case implies $T_\pi X/\pi T_\pi X$ is non-split. By construction, $V_\pi X \cong V_{X_E^\beta}$ for each β, so our claim follows. ☐

Definition 2.26. For $\beta = 1$ or φ,

(a) Let $\widehat{T}_E^\beta$ be a maximal residually non-split sublattice inside T^β (defined in Definition 2.7). Here, "maximal" means there is no other $\widehat{T}'$ with $\widehat{T}_E^\beta \subsetneq \widehat{T}' \subset T^\beta$ which is residually non-split. (That such $\widehat{T}_E^\beta$ exists is shown in Proposition 2.25, and it satisfies

$$\widehat{T}_E^\beta/\pi\widehat{T}_E^\beta \cong X[\pi]$$

for the group scheme $X/\mathbb{Z}_p$ determined by β.)

(b) Suppose $N(> 4s+4)$ is big enough so that

$$\mathrm{proj}_E(T^\beta) \cap p^{N-2s}(A_{cris} \otimes \widehat{v}_E + A_{cris} \otimes v_E) \subset \pi \cdot \mathrm{proj}_E \widehat{T}_E^\beta.$$

Then, we have the following.

Proposition 2.27. *Assume N is big enough (according to Definition 2.26; Again note that "big enough" only depends on V_E). Recall $V_{X_E^\beta}, \widehat{V}_l^\beta$ for $\beta = 1, \varphi$. There is a lattice $\widehat{T}_l^\beta (\subset T_l^\beta)$ inside $\widehat{V}_l^\beta$ satisfying*

$$\widehat{T}_l^\beta/\pi\widehat{T}_l^\beta \cong \widehat{T}_E^\beta/\pi\widehat{T}_E^\beta$$

(thus $\widehat{T}_l^\beta$ is residually non-split).

Proof. Definition 2.26 (b) implies that $\mathrm{proj}_E \widehat{T}_E^\beta$ inside $\mathrm{proj}_E(T^\beta)/\mathrm{proj}_E(T^\beta) \cap p^{N-2s}(A_{cris} \otimes \widehat{v}_E + A_{cris} \otimes v_E)$ has a quotient isomorphic to $\mathrm{proj}_E \widehat{T}_E^\beta/\pi \cdot \mathrm{proj}_E \widehat{T}_E^\beta \cong \widehat{T}_E^\beta/\pi\widehat{T}_E^\beta$ (this isomorphism is by Proposition 2.19).

Then, this implies that, by Proposition 2.23, there is a sublattice T' inside $\mathrm{proj}_l(T_l^\beta)$ such that

$$T'/\mathfrak{m}T' \cong \widehat{T}_E/\mathfrak{m}\widehat{T}_E,$$

and the claim follows because proj_l is injective on T_l^β. ☐

In fact, if V_l^β has a residually non-split lattice $\widehat{T}_l$, then it is unique up to scalar multiplication as follows: Suppose $\widehat{T}$ is also residually non-split. We may assume $\widehat{T} \subset \widehat{T}_l$ and $\pi^{-1}\widehat{T} \not\subset \widehat{T}_l$.

Where T_l is the unique rank 2 maximal submodule inside $\widehat{T}_l$, in general we have $\widehat{T} = T_l + \pi^i \widehat{T}_l$ for some $i \geq 0$. $\widehat{T}$ is residually split if $i > 0$, thus

$$\widehat{T} = \widehat{T}_l.$$

2.2. Note that toward the end of Section 2.1, N depends on X_E^β (and therefore depends on β). The problem is that we want k to be an arbitrary field, so there are infinitely many β, and we want N to depend only on V_E. So, we want to approach it through linear combinations of $\beta = 1$ and $\beta = \varphi$.

It is well-known that $\mathrm{Ext}^1_{G_{\mathbb{Q}_p}}(*,*)$ is canonically isomorphic to $H^1\left(G_{\mathbb{Q}_p}, \mathrm{ad}(*)\right)$ where $\mathrm{ad}(*)$ is the adjoint reprsentations of $*$ ([10, p. 288]), thus we theoretically know there is a group structure on $\mathrm{Ext}^1_{G_{\mathbb{Q}_p}}(*,*)$. But, we want to be able to explicitly write this group structure so that we can show $\widehat{V}_l^\beta + \widehat{V}_l^{\beta'} = \widehat{V}_l^{\beta+\beta'}$.

Let T be any representation of finite rank over a ring R. Given $0 \to T \to \widehat{T} \to T \to 0$, multiplication by $a \in R^*$ is given by

$$0 \longrightarrow T \longrightarrow \widehat{T} \xrightarrow{\times a} T \longrightarrow 0.$$

We add two extensions as follows: Consider

$$\begin{array}{ccccc} & & \widehat{T} & & \\ & \nearrow & & \searrow & \\ 0 \longrightarrow T & & & & T \longrightarrow 0. \\ & \searrow & & \nearrow & \\ & & \widehat{T}' & & \end{array}$$

Then, we have

$$0 \longrightarrow T \times T \longrightarrow \widehat{T} \times_T \widehat{T}' \longrightarrow T \times_T T \ (\cong T) \longrightarrow 0.$$

Through the (diagonal) embedding $T \to T \times T$ by $t \mapsto (t, -t)$, consider T as a subgroup of $T \times T$. Then, from the above short exact sequence, we have

$$0 \longrightarrow T \times T/T \longrightarrow \widehat{T} \times_T \widehat{T}'/T \longrightarrow T \longrightarrow 0.$$

Since $T \times T/T \cong T$, this exact sequence is an element of $\mathrm{Ext}^1(T,T)$, which we think of as $\widehat{T} + \widehat{T}'$.

Recall $V_l \cong k^2$ $(l \geq 2)$ is a crystalline representation with the characteristic of φ on $D(V_l)$ being $x^2 - \frac{a_l}{\epsilon' p^{l-1}}x + \frac{1}{\epsilon' p^{l-1}}$.

Where $\beta = a + b\varphi, \beta' = a' + b'\varphi$ $(a, b, a', b' \in k)$, let $\widehat{V}^\beta, \widehat{V}^{\beta'} \in \mathrm{Ext}^1_{cr}(V_l, V_l)$ (i.e., extensions which are crystalline). For some $d (\neq 0) \in D(V_l)$ with

$\varphi(d) \in \mathrm{Fil}^0(D(V_l))$ and its liftings $\widehat{d}^\beta \in D(\widehat{V}^\beta)$, $\widehat{d}^{\beta'} \in D(\widehat{V}^{\beta'})$ with $\varphi(\widehat{d}^\beta) \in \mathrm{Fil}^0 D(\widehat{V}^\beta)$, $\varphi(\widehat{d}^{\beta'}) \in \mathrm{Fil}^0 D(\widehat{V}^{\beta'})$,

$$\left(\varphi^2 - \frac{a_l}{\epsilon' p^{l-1}}\varphi + \frac{1}{\epsilon' p^{l-1}}\right)\widehat{d}^\beta = \beta d, \quad \left(\varphi^2 - \frac{a_l}{\epsilon' p^{l-1}}\varphi + \frac{1}{\epsilon' p^{l-1}}\right)\widehat{d}^{\beta'} = \beta' d.$$

Proposition 2.28. *In* $\mathrm{Ext}^1_{cr}(V_l, V_l)$,

$$\widehat{V}^\beta + \widehat{V}^{\beta'} = \widehat{V}^{\beta+\beta'}.$$

Proof. Then,

$$(\widehat{d}^\beta, \widehat{d}^{\beta'}) \in D(\widehat{V}^\beta \times_{V_l} \widehat{V}^{\beta'}/V_l) \cong D(\widehat{V}^\beta) \times_{D(V_l)} D(\widehat{V}^{\beta'})/D(V_l)$$

is a lifting of d because $(\widehat{d}^\beta, \widehat{d}^{\beta'}) \mapsto (d,d) = d$ (through $D(V_l) \times_{D(V_l)} D(V_l) \cong D(V_l)$).

Note

$$\left(\varphi^2 - \frac{a_l}{\epsilon' p^{l-1}}\varphi + \frac{1}{\epsilon' p^{l-1}}\right)(\widehat{d}^\beta, \widehat{d}^{\beta'}) = (\beta d, \beta' d).$$

As explained above, the embedding $D(V_l) \to D(V_l) \times D(V_l)$ is diagonal (i.e., $d \mapsto (d, -d)$), so

$$(\beta d, \beta' d) = (\beta d + \beta' d, 0) = (\beta + \beta')(d, 0) \pmod{D(V_l)}.$$

Thus, by identifying $(d,0) = d$ through $D(V_l) \times D(V_l)/D(V_l) \cong D(V_l)$, the claim follows. □

2.3. Recall $T_E(\subset V_E)$, and suppose N is big enough for $\beta = 1$ and $\beta = \varphi$ as in Definition 2.26. (So, N depends only on T_E.) Also, recall that $\overline{T}_E$ is its residual representation.

In the following, all extensions in Ext^1 are $G_{\mathbb{Q}_p}$-equivariant.

Recall (see [18]) that $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ is the set of extensions $\overline{\widehat{T}}$ of $\overline{T}_E$ by $\overline{T}_E$ which are given by $\overline{\widehat{T}} = G(\overline{\mathbb{Q}})$ for some group scheme $G/\mathbb{Z}_p$ with good reduction.

As noted in Definition 2.26, by Proposition 2.25, there are residually non-split lattices $\widehat{T}^1_E \subset \widehat{V}_{X^1_E}$, $\widehat{T}^\varphi_E \subset \widehat{V}_{X^\varphi_E}$ which are uniquely determined up to scalar multiplication. Thus, their residual representations $\overline{\widehat{T}}{}^1_E, \overline{\widehat{T}}{}^\varphi_E (\neq 0) \in \mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$ are uniquely determined.

Proposition 2.29. $\overline{\widehat{T}}{}^1_E$ *and* $\overline{\widehat{T}}{}^\varphi_E$ *are a basis (over* $\overline{k}$*) of* $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$.

Proof. Recall that there are group schemes $X^1/\mathbb{Z}_p$ and $X^\varphi/\mathbb{Z}_p$ which satisfy $T_\pi X^1 \cong \widehat{T}^1_E$, $T_\pi X^\varphi = \widehat{T}^\varphi_E$. (See the proof of Proposition 2.25.) By comparing their Honda types $\pmod{\pi}$, we can see $\overline{\widehat{T}}{}^1_E$ and $\overline{\widehat{T}}{}^\varphi_E$ are linearly independent over $\overline{k}$.

Since $\dim_{\overline{k}} \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E) = 2$ ([13]), the claim follows. □

As mentioned, canonically $\mathrm{Ext}^1_{G_{\mathbb{Q}_p}}(\overline{T}_E, \overline{T}_E) \cong H^1(\mathbb{Q}_p, \mathrm{ad}(\overline{T}_E))$. It will be useful to note that since $\overline{T}^*_E (\overset{\mathrm{def}}{=} \mathrm{Hom}(\overline{T}_E, \mu_p)) \cong \overline{T}_E$, we have (see [16, Section 4.1]) $\mathrm{ad}^0(\overline{T}_E)^* \cong \mathrm{ad}^0(\overline{T}_E)(1) \cong \mathrm{Sym}^2(\overline{T}_E)$, and

$$\mathrm{ad}(\overline{T}_E) \cong \mathrm{Sym}^2(\overline{T}_E)(-1) \oplus \overline{k} \cong \mathrm{ad}^0(\overline{T}_E) \oplus \overline{k}$$

Wiles ([18]) defines the local condition inside $H^1(\mathbb{Q}_p, \mathrm{ad}(\overline{T}_E))$ as the image of $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ (and the local condition $H^1_f(\mathbb{Q}, \mathrm{ad}^0(\overline{T}_E))$ is defined accordingly). He could define it intrinsically using points of finite group schemes, but one can also (probably equivalently) define it by saying an extension is finite flat if it has a lifting which is crystalline of weights $[0, 1]$.

We define $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ as follows:

Definition 2.30. $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ is the set of extensions $\widehat{\overline{T}} \in \mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$ which has a free lifting $\widehat{T}$ (meaning $\widehat{T}$ is free over $\mathcal{O}_k$ and $\widehat{T}/\pi\widehat{T} \cong \widehat{\overline{T}}$), with $\widehat{T} \to T \to 0$ (the map being a $G_{\mathbb{Q}_p}$-equivariant homomorphism of $\mathcal{O}_k$-modules) for some T so that

- $G_{\mathbb{Q}_p}$ acts on $\widehat{T}$ continuously, and $\widehat{T}$ is crystalline of weights $[0, l-1]$,
- $T/\pi T \cong \overline{T}_E$,
- Recall α, a (fixed) root of the characteristic of φ on $D(V_E)$. The characteristic of φ on $D(T \otimes \mathbb{Q}_p)$ has a root α' with

$$\alpha' \equiv \alpha \pmod{p^N}$$

(the last condition implies the second, [7]) so that the following is commutative:

$$\begin{array}{ccccccccc} (0 & \longrightarrow & T & \longrightarrow) & \widehat{T} & \longrightarrow & T & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \overline{T}_E & \longrightarrow & \widehat{\overline{T}} & \longrightarrow & \overline{T}_E & \longrightarrow & 0 \end{array}$$

where the vertical arrows are given by residual representations (i.e., $\otimes_{\mathcal{O}_k} \overline{k}$).

Readers may wonder how the top line is given. If $\widehat{\overline{T}} = 0$, then it has an obvious lifting $\widehat{T}$, and no more needs to be said. Suppose $\widehat{\overline{T}} \neq 0$. If $T' \to \widehat{T} \to T$ with $T' \ncong T$, then it is a split exact sequence, which implies $\widehat{\overline{T}}$ is a trivial extension, which is a contradiction.

Theorem 2.31.

$$\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E) \cong \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E).$$

Proof. We will write Ext^1_{cr} for $\mathrm{Ext}^1_{cr,[0,l-1]}$ in short.

Take any $\widehat{\overline{T}}(\neq 0) \in \mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$. (By definition, $\widehat{\overline{T}}$ has a lifting $\widehat{T}$ whose residual representation is $\widehat{\overline{T}}$, and $0 \to T \to \widehat{T} \to T \to 0$ for some T with the above properties.)

For $\beta = 1, \varphi$, set $\widehat{V}^\beta_l$ by the discussion after Definition 2.8 where $V_l \stackrel{\mathrm{def}}{=} T \otimes \mathbb{Q}_p$. By Proposition 2.27, there are $\widehat{T}^\beta_l \subset \widehat{V}^\beta_l$ so that

$$\widehat{\overline{T}}^\beta \stackrel{\mathrm{def}}{=} \widehat{T}^\beta_l / \pi \widehat{T}^\beta_l \cong \widehat{T}^\beta_E / \pi \widehat{T}^\beta_E. \tag{2.3}$$

By Proposition 2.29 and the above discussion, it is enough to show

$$\widehat{\overline{T}} = \bar{a}\widehat{\overline{T}}^1 + \bar{b}\widehat{\overline{T}}^\varphi$$

in $\mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$ for some $\bar{a}, \bar{b} \in \bar{k}$. To that end, we will show

$$\widehat{T} = a\widehat{T}^1_l + b\widehat{T}^\varphi_l.$$

for some $a, b \in \mathcal{O}_k$.

First, for $\widehat{V} = \widehat{T} \otimes \mathbb{Q}_p$, we can let

$$\widehat{V} = \widehat{V}^{\beta'}_l$$

for some $\beta' = a + b\varphi$ $(a, b \in k)$. (Again, we follow the notation in the discussion after Definition 2.8, now with β'.) By multiplying a scalar on $V \to \widehat{V}$ (equivalently, by multiplying a scalar on $m \in D(V)$ without changing $\widehat{m} \in D(\widehat{V})$), we can assume

$$a, b \in \mathcal{O}_k, \quad (a, b) \not\equiv (0, 0) \pmod{\mathfrak{m}}.$$

Case 1. $a \not\equiv 0, b \not\equiv 0 \pmod{\mathfrak{m}}$. In other words, $a, b \in \mathcal{O}^*_k$. Then, $a\widehat{T}^1_l + b\widehat{T}^\varphi_l (\in \mathrm{Ext}^1_{cr}(T, T))$ is well-defined (see Section 2.2), and is clearly a lattice inside $a\widehat{V}^1_l + b\widehat{V}^\varphi_l = \widehat{V}^{a+b\varphi}_l$ (see Proposition 2.28). And, because $a, b \in \mathcal{O}^*_k$, it is not hard to see the residual representation of $a\widehat{T}^1_l + b\widehat{T}^\varphi_l$ is $\bar{a}\widehat{\overline{T}}^1 + \bar{b}\widehat{\overline{T}}^\varphi$ from the construction.

Since $\widehat{\overline{T}}^1 (\cong \widehat{\overline{T}}^1_E)$ and $\widehat{\overline{T}}^\varphi (\cong \widehat{\overline{T}}^\varphi_E)$ (see (2.3)) are linearly independent, and $(\bar{a}, \bar{b}) \neq (0, 0)$, $\bar{a}\widehat{\overline{T}}^1 + \bar{b}\widehat{\overline{T}}^\varphi \neq 0$ in $\mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$. In other words, $a\widehat{T}^1_l + b\widehat{T}^\varphi_l$ is residually non-split. Since $\widehat{\overline{T}} \neq 0$, and therefore $\widehat{T}$ is residually non-split, and a residually non-split lattice is unique up to scalar, after scalar multiplication if necessary,

$$\widehat{T} = a\widehat{T}^1_l + b\widehat{T}^\varphi_l,$$

thus $\widehat{\overline{T}} = \bar{a}\widehat{\overline{T}}^1 + \bar{b}\widehat{\overline{T}}^\varphi \in \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ by Proposition 2.29.

Case 2. either $a \equiv 0$ *or* $b \equiv 0 \pmod{\mathfrak{m}}$. Without loss of generality, assume $a \not\equiv 0, b \equiv 0 \pmod{\mathfrak{m}}$. Then,

$$\begin{aligned}\widehat{V} &= \widehat{V}_l^{a+b\varphi} \\ &= \widehat{V}_l^{a+(b-1)\varphi} + \widehat{V}_l^{\varphi}\end{aligned}$$

(by Proposition 2.28). Similar to *Case 1*, $\left(a\widehat{T}_l^1 + (b-1)\widehat{T}_l^{\varphi}\right) + \widehat{T}_l^{\varphi}$ is a lattice inside $\widehat{V}$ where $\left(a\widehat{T}_l^1 + (b-1)\widehat{T}_l^{\varphi}\right)$ (which is well-defined because $a, b-1 \in \mathcal{O}_k^*$) is a lattice inside $\widehat{V}_l^{a+(b-1)\varphi}$.

Again similar to *Case 1* (and because $a, b-1$ are units)

$$\begin{aligned}\overline{\left(a\widehat{T}_l^1 + (b-1)\widehat{T}_l^{\varphi}\right) + \widehat{T}_l^{\varphi}} &= \overline{a\widehat{T}_l^1 + (b-1)\widehat{T}_l^{\varphi}} + \overline{\widehat{T}}^{\varphi} \\ &= \left(\bar{a}\overline{\widehat{T}}^1 + (\bar{b}-1)\overline{\widehat{T}}^{\varphi}\right) + \overline{\widehat{T}}^{\varphi} \\ &= \bar{a}\overline{\widehat{T}}^1 \\ &\neq 0.\end{aligned}$$

So, $(a\widehat{T}_l^1 + (b-1)\widehat{T}_l^{\varphi}) + \widehat{T}_l^{\varphi} = a\widehat{T}_l^1 + b\widehat{T}_l^{\varphi}$ is residually non-split, and similar to *Case 1*, $\widehat{T} = a\widehat{T}_l^1 + b\widehat{T}_l^{\varphi}$ after scalar multiplication if necessary.

Thus, $\overline{\widehat{T}} = \overline{a\widehat{T}_l^1 + b\widehat{T}_l^{\varphi}} = \bar{a}\overline{\widehat{T}}^1 \in \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$.

To be precise, we have shown $\mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E) \subset \mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$, which is enough for this paper, but a close examination of the dimensions shows the equality. ☐

As the referee pointed out, Theorem 2.31 has non-obvious consequences for $l = 2$. Recall the chosen uniformizer π of k. Then, $\mathrm{Ext}^1_{fl}(\overline{T}_E, \overline{T}_E)$ *can* be interpreted as $\mathrm{Ext}^1_{cr,[0,1]}(\overline{T}_E, \overline{T}_E)$, but with congruences modulo π in its definition, not modulo p^N. We will denote this by $\mathrm{Ext}^1_{cr,[0,1]}(\overline{T}_E, \overline{T}_E)'$ to distinguish it from $\mathrm{Ext}^1_{cr,[0,1]}(\overline{T}_E, \overline{T}_E)$.

Clearly, $\mathrm{Ext}^1_{cr,[0,1]}(\overline{T}_E, \overline{T}_E) \subset \mathrm{Ext}^1_{cr,[0,1]}(\overline{T}_E, \overline{T}_E)'$. However, Theorem 2.31 implies equality, which is to say the extensions of $\overline{T}_E$, which have crystalline liftings (of weights $[0,1]$) which are themselves extensions of some T' isomorphic to $T_E \pmod{\pi}$, have crystalline liftings (of weights $[0,1]$) which are extensions of (possibly different) T isomorphic to $T_E \pmod{p^N}$.

3. Pro-representable deformation functors and the local conditions

Theorem 2.31 is the key technical result of this paper, but as explained in the introduction, the initial motivation was applying patching to the deformation functors and Hecke algebras of higher weights, both of which need to be carefully considered.

The *first issue* is that one needs a certain functor $\mathcal{D}$ of deformations with crystalline liftings of higher weights (Definition 3.3), needs to show $\mathcal{D}$ is (pro-)representable or it has a representable hull (Proposition 3.5), and $t_{\mathcal{D}} \subset \mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$ (which we show only in special cases; see Proposition 3.6).

Remark 3.1.

(a) The last point is because we want to interprete $t_{\mathcal{D}}$ as a certain Selmer group of $\mathrm{ad}^0(\overline{T}_E)$ with local condition $\mathrm{Ext}^1_{cr,[0,l-1]}(\overline{T}_E, \overline{T}_E)$.

(b) As mentioned in the introduction, we will not worry about $\mathcal{D}_Q$ for the sets Q of auxiliary primes, which I believe can be handled similarly.

Let $\overline{k}$ be a finite field of characteristic p. If necessary we can think of it as the residue field of $k/\mathbb{Q}_p$. We will recall some terminologies from [10]: A *coefficient ring* R is a complete noetherian local ring with residue field $\overline{k}$ with augmentation $R \to \overline{k}$ and the usual profinite topology, and a coefficient ring homomorphism is a *continuous* homomorphism between coefficient rings commutative with the augmentations ([10, p. 249]). Also see [10, p. 257 and p. 262] for the definitions of deformations, etc.

We let $\widehat{\mathcal{C}}$ be the category of coefficient rings with coefficient ring homomorphisms, and $\mathcal{C}$ be the full subcategory of artinian objects. Let Λ be any coefficient ring (for example, $\overline{k}$, $W(\overline{k})$, $\mathcal{O}_k$, etc.) Then, $\widehat{\mathcal{C}}_\Lambda$ is the category of objects in $\widehat{\mathcal{C}}$ which are Λ-algebras, and, $\mathcal{C}_\Lambda$ is the full subcategory of $\widehat{\mathcal{C}}_\Lambda$ whose objects are *artinian*.

Below, we will use Schlessinger's criteria for pro-representability (see [14] or [10, Section 18, p. 277] for its statement).

For $n \geq 1$, a topological group G, and a coefficient ring A, let $F_n(A, G)$ or simply $F_n(G)$ be the set of representations $V (\cong A^n)$ with A-linear continuous G-action. A morphism in F_n from (A, V) to (A_1, V_1) can be understood in several ways. We can understand it as a coefficient Λ-algebra homomorphism $A \to A_1$ and $V \otimes_A A_1 \cong V_1$ where the tensor is given by the homomorphism $A \to A_1$. Or, it can be understood as: We can choose bases of V and V_1, which give $\rho_V : G \to \mathrm{GL}_n(A)$ and $\rho_{V_1} : G \to \mathrm{GL}_n(A_1)$ so that ρ_{V_1} is given by ρ_V and $A \to A_1$.

Definition 3.2. We fix a coefficient ring W, which is a DVR and of finite rank over $\mathbb{Z}_p$. From now on, a *bipotent* ϵ is a non-zero element with $\epsilon^2 = 0$.

Let $\mathcal{S}$ be the set of

(S1) For any $R \in \widehat{\mathcal{C}}_W$ which is a DVR, we have $R, R[\epsilon] \in \mathcal{S}$ where ϵ is a bipotent.

(S2) If $C_1, C_2 \in \mathcal{S}$ and there are $\alpha_1 : C_1 \to C_3$, $\alpha_2 : C_2 \to C_3$ for some $C_3 \in \mathcal{C}_{\overline{k}}$ (all homomorphisms being W-algebra coefficient ring homomorphisms), then

$$C_1 \times_{C_3} C_2 \in \mathcal{S}.$$

Then any $S \in \mathcal{S}$ looks like (for example) $S = (R_1 \times_{C_1} R_2[\epsilon_2]) \times_{C_2} (R_3[\epsilon_3] \times_{C_3} R_4[\epsilon_4]) \times \cdots \times R_n$. We will call $R_1, R_2[\epsilon_2], \ldots$ factors of S. For each factor R or $R[\epsilon]$, there are obvious homomorphisms $S \to R$ or $S \to R[\epsilon] \to R$.

From now on, suppose f_E is an eigenform of level M for some M prime to p, possibly a newform, and $T_E = W^2$ is its associated Galois representation of $G = G_{\mathbb{Q},\Sigma}$ where Σ is a finite set of places including p, infinite places, and all prime divisors of M.

In addition, we assume there is f, an eigenform of weight $l \geq 2$ of level $\Gamma_1(M)$ with $a_n(f) \in W$ for all n so that for the G-representation $T_f (\cong W^2)$ attached to f,

$$T_f \equiv T_E \pmod{p^N}.$$

Clearly T_f, T_E are deformations of $\overline{T}_E$.

For some choice of basis, $\overline{T}_E$ gives $\bar{\rho} : G \to \mathrm{GL}_2(\bar{k})$.

Definition 3.3. For $A \in \mathcal{C}_{\bar{k}}$ and $V_A \in F_2(A, G)$, $(A, V_A) \in \mathcal{D}(A)$ if

(a) There is $R_A \in \mathcal{S}$ with a coefficient ring homomorphism $\varphi_A : R_A \to A$ (not necessarily surjective) and $V_{R_A} = R_A^2 \in F_2(G)$ so that V_{R_A} and φ_A induce V_A, i.e.,

$$V_{R_A} \otimes_{\varphi_A} A \cong V_A$$

where $\otimes_{\varphi_A}$ means the tensor given by φ_A.

(b) If A has any bipotent ϵ which generates dimension 1 subspace over $\bar{k}$, i.e., $A\epsilon = \bar{k}\epsilon$, for at least one such $\epsilon \in A$, there is a factor $R[\widetilde{\epsilon}]$ of R_A so that $(0, \ldots, 0, \widetilde{\epsilon}, 0, \ldots, 0) \in R_A$ and (where $\widetilde{\epsilon}$ denotes $(0, \ldots, 0, \widetilde{\epsilon}, 0, \ldots, 0)$ by abuse of notation,) $\varphi_A(\widetilde{\epsilon}) = \epsilon$.

(c) For each factor S of R_A, $V_S (= V_{R_A} \otimes S)$ is crystalline of weights $[0, l-1]$,

(d) For each factor $S = R$ or $R[\epsilon]$ of R_A,

$$V_R (:= V_{R_A} \otimes R) \cong T_E \otimes R \pmod{p^N}.$$

Note that Definition 3.3 implies $V_A \otimes \bar{k} \cong \overline{T}_E$, thus V_A is a deformation of $\overline{T}_E$.

From now on, for any $R \in \widehat{\mathcal{C}}$ and any $r \in R$, let $\bar{r}$ denote the image of r under the augmentation $R \to \bar{k}$. First, note that (b) implies that for any $a \in A$, $a\epsilon = \bar{a}\epsilon$.

Then, we need to show that $\mathcal{D}$ is a category.

Proposition 3.4. *Suppose $A, A' \in \mathcal{C}_{\bar{k}}$, $(A, V_A) \in \mathcal{D}(A)$, and there is $\iota : A \to A'$ in $\mathcal{C}_{\bar{k}}$. Then, $V_{A'} = V_A \otimes A'$ is in $\mathcal{D}(A')$. (Therefore, ι induces $\iota : \mathcal{D}(A) \to \mathcal{D}(A')$.)*

Proof. Let $\varphi' : R_A \overset{\varphi_A}{\to} A \to A'$. Clear that $V_{R_A} \otimes_{\varphi'} A' \cong V_A \otimes_\iota A' = V_{A'}$. So, $V_{A'}$ automatically satisfies all the conditions of Definition 3.3 except (b). So, we consider the case that A' has bipotents ϵ with properties in (b), but R_A has no $\widetilde{\epsilon}$ satisfying (b).

Fix any such bipotent $\epsilon' \in A'$, and let

$$R' = R_A \times_{\bar{k}} W[\widetilde{\epsilon}]$$

where $W[\widetilde{\epsilon}] \to \bar{k}$ is the obvious augmentation. Define

$$\varphi'' : R' \longrightarrow A'$$
$$(r, a + b\widetilde{\epsilon}) \longmapsto \varphi'(r) + \bar{b}\epsilon'$$

Take $(r, a + b\widetilde{\epsilon}), (r', a' + b'\widetilde{\epsilon}) \in R'$. Then,

$$\varphi''(r, a + b\widetilde{\epsilon}) = \varphi'(r) + \bar{b}\epsilon', \quad \varphi''(r', a' + b'\widetilde{\epsilon}) = \varphi'(r') + \bar{b}'\epsilon'.$$

We note

$$(r, a + b\widetilde{\epsilon}) \cdot (r', a' + b'\widetilde{\epsilon}) = (rr', aa' + (ab' + a'b)\widetilde{\epsilon}),$$
$$(\varphi'(r) + \bar{b}\epsilon') \cdot (\varphi'(r') + \bar{b}'\epsilon') = \varphi'(rr') + (\varphi'(r)\bar{b}' + \varphi'(r')\bar{b})\epsilon',$$
$$\varphi''(rr', aa' + (ab' + a'b)\widetilde{\epsilon}) = \varphi'(rr') + (\bar{a}\bar{b}' + \bar{a}'\bar{b})\epsilon').$$

Note $\bar{r} \equiv \bar{a}$ by definition, and $\overline{\varphi'(r)} = \bar{r}$ because φ' is a coefficient ring homomorphism. Thus, $\varphi'(r)\epsilon' = \overline{\varphi'(r)}\epsilon' = \bar{a}\epsilon'$, and similarly $\varphi'(r')\epsilon' = \bar{a}'\epsilon'$. Thus, φ'' is a homomorphism, and in fact, a coefficient ring homomorphism.

So Definition 3.3 (b) holds. Now, we will construct $V_{R'}$.

Since T_f is a deformation of $\overline{T}_E$, for some choice of basis, T_f gives $\rho_f : G \to \mathrm{GL}_2(W)$ so that $\rho_f(g) \mapsto \bar{\rho}(g)$ under $W \to \bar{k}$ for each $g \in G$. Similarly, since V_{R_A} is also a deformation of $\overline{T}_E$, $\rho_{R_A}(g) \mapsto \bar{\rho}(g)$ under $R_A \to \bar{k}$ for each $g \in G$.

Let $V_{W[\tilde{\epsilon}]} = T_f \otimes W[\widetilde{\epsilon}]$ (and accordingly define $\rho_{W[\tilde{\epsilon}]} : G \to \mathrm{GL}_2\left(W[\widetilde{\epsilon}]\right)$). Then, $\rho_{W[\tilde{\epsilon}]}(g) = \rho_f(g)$ for all $g \in G$. In other words, the entries of $\rho_{W[\tilde{\epsilon}]}(g)$ are in W. Let $\rho_{R'} = \rho_{R_A \times_{\bar{k}} W[\tilde{\epsilon}]} = \rho_{R_A} \times_{\bar{k}} \rho_{W[\tilde{\epsilon}]}$. In other words, where $\rho_{R_A}(g) = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and $\rho_{W[\tilde{\epsilon}]}(g) = \left[\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right]$, let

$$\rho_{R'}(g) = \begin{bmatrix} (a, a') & (b, b') \\ (c, c') & (d, d') \end{bmatrix}.$$

(Clearly each entry is a well-defined fiber product.) Clearly, $\rho_{R'}$ satisfies Definition 3.3 (c, d) by construction.

As explained above, the construction of $V_{W[\tilde{\epsilon}]}$ implies each entry of $\rho_{R'}(g)$ is in $R_A \times_k W$ (i.e., $a', b', c', d' \in W$). Thus,

$$\varphi''\left(\rho_{R'}(g)\right) = \begin{bmatrix} \varphi'(a) & \varphi'(b) \\ \varphi'(c) & \varphi'(d) \end{bmatrix} = \varphi'\left(\rho_{R_A}(g)\right),$$

which is to say $V_{R'} \otimes_{\varphi''} A' \cong V_{R_A} \otimes_{\varphi'} A' \cong V_{A'}$. Thus, (a) follows. $\square$

Below, H1, H2, H3 are the first three conditions of Schlessinger's criterion (following the notation in [10]).

Proposition 3.5. *$\mathcal{D}$ satisfies Schlessinger's criteria H1, H2, H3.*

Proof. Consider a diagram in $\mathcal{C}_{\bar{k}}$:

$$\begin{array}{ccc} A & & B \\ & \searrow \quad \swarrow & \\ & C & \end{array}$$

with $(A, V_A), (B, V_B), (C, V_C) \in \mathcal{D}$ inducing $V_A \times_{V_C} V_B \in \mathcal{D}(A) \times_{\mathcal{D}(C)} \mathcal{D}(B)$.

Since $\mathcal{D}^{univ}$ is pro-representable ([2], [9], etc.), there is $V_{A \times_C B} \in F_2(G)$ so that $V_{A \times_C B} \mapsto V_A \times_{V_C} V_B$.

By definition, there are $R_A (\in \mathcal{S}) \overset{\varphi_A}{\to} A$ with V_{R_A} and $R_B (\in \mathcal{S}) \overset{\varphi_B}{\to} B$ with V_{R_B} with the properties in Definition 3.3. Then, they naturally induce $R (:= R_A \times_C R_B) \overset{\varphi_A \times \varphi_B}{\to} A \times_C B$ with $R \in \mathcal{S}$ and $V_R := V_{R_A} \times_{V_C} V_{R_B}$ is well-defined. Clearly $V_{A \times_C B}$, R, and V_R satisfy Definition 3.3 except possibly (b), which can be again resolved similar to Proposition 3.4. So, $\mathcal{D}(A \times_C B) \to \mathcal{D}(A) \times_{\mathcal{D}(C)} \mathcal{D}(B)$ is surjective, and H1 follows.

As to H2, by H1, we only need to show $\mathcal{D}(A \times_C B) \to \mathcal{D}(A) \times_{\mathcal{D}(C)} \mathcal{D}(B)$ is injective when $A = k[\epsilon]$, which follows from the pro-representability of $\mathcal{D}^{univ}$.

As to H3, by H2, T_k holds. And, it is clear that $\dim_k(t_{\mathcal{D}})$ $(\leq \dim_k(t_{\mathcal{D}^{univ}}))$ is finite. $\square$

Since $\mathcal{D}(\bar{k})$ is clearly a singleton, by Schlessinger ([14]) $\mathcal{D}$ has a pro-representable hull D_R so that $D_R \to \mathcal{D}$ is smooth and $t_R \cong t_{\mathcal{D}}$. This is likely enough for many applications, though $\mathcal{D}$ may be in fact pro-representable.

Still more need to be done to apply patching. First, one needs $t_{\mathcal{D}} \subset \mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$. As we mentioned, we will prove this only in some special, but possibly illustrative cases.

Suppose $V_{\bar{k}[\epsilon]} \in \mathcal{D}(\bar{k}[\epsilon]) (= t_{\mathcal{D}})$ and $\varphi : R (= R_{\bar{k}[\epsilon]}) \to \bar{k}[\epsilon]$ and V_R are as in Definition 3.3.

In the first case, consider the simplest case of $R = S[\tilde{\epsilon}]$ for some DVR $S \in \widehat{\mathcal{C}}_W$ and bipotent $\tilde{\epsilon}$ (so that $\varphi(\tilde{\epsilon}) = \epsilon$ by definition). Let π be a uniformizer of W. Choose $x_1, \ldots, x_n \in \mathfrak{m}_S$ so that $\mathfrak{m}_S/(\pi, \mathfrak{m}_S^2)$ is $\bar{k}$-linearly generated by $\bar{x}_1, \ldots, \bar{x}_n$. Then, $S/(\pi, \mathfrak{m}_S^2) = \bar{k}[\bar{x}_1, \ldots, \bar{x}_n]$ where each $\bar{x}_i$ is a bipotent. For a chosen basis, V_R induces $\rho_R : G \to \mathrm{GL}_2(R)$, and so for any $g \in G$,

$$\rho_R(g) = \begin{bmatrix} a_0 + \sum_{i=1}^n a_i x_i + \sum_{d \geq 2} * \cdot x^d + \pi \cdot * + (a_0' + \cdots)\tilde{\epsilon}, & b_0 + \cdots \\ c_0 + \cdots & d_0 + \cdots \end{bmatrix}$$

where all coefficients are in W, x^d indicates products of x_i's of degree d, and $* \in S$. Because $V_R \otimes S \equiv T_E \otimes S \pmod{p^N}$, $V_R \otimes \bar{k}[\bar{x}_i] \cong \overline{T}_E \otimes \bar{k}[\bar{x}_i] (\cong \overline{T}_E \oplus \overline{T}_E)$ for each i, thus $V_R \otimes \bar{k}[\bar{x}_i] = 0$ in $\mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$. Thus, $a_i \equiv 0 \pmod{\pi}$ for each i.

Note $\varphi(x_i) = a \cdot \epsilon$ for some $a \in \bar{k}$. If $\varphi(x_i) = 0$, we can drop it from consideration, so we assume $\varphi(x_i) = \epsilon$ for all i by multiplying some scalar to x_i if necessary. Then, $\varphi : R \to \bar{k}[\epsilon]$ induces

$$\begin{aligned}\rho_{\bar{k}[\epsilon]}(g) &= \begin{bmatrix} \bar{a}_0 + \sum_{i=1}^n \bar{a}_i\epsilon + \bar{a}'_0\epsilon, & \bar{b}_0 + \sum_{i=1}^n \bar{b}_i\epsilon + \bar{b}'_0\epsilon \\ \bar{c}_0 + \sum_{i=1}^n \bar{c}_i\epsilon + \bar{c}'_0\epsilon & \bar{d}_0 + \sum_{i=1}^n \bar{d}_i\epsilon + \bar{d}'_0\epsilon \end{bmatrix} \\ &= \begin{bmatrix} \bar{a}_0 + \bar{a}'_0\epsilon, & \bar{b}_0 + \bar{b}'_0\epsilon \\ \bar{c}_0 + \bar{c}'_0\epsilon & \bar{d}_0 + \bar{d}'_0\epsilon \end{bmatrix}\end{aligned}$$

In other words, $V_{\bar{k}[\epsilon]} \cong V_R \otimes S/\mathfrak{m}_S$, thus $V_{\bar{k}[\epsilon]} \in \mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$ by the definition of Ext^1_{cr} (by letting $\mathcal{O}_k = S$ in the definition of Ext^1_{cr} if necessary).

The *second case* is probably more illustrative and indicative of the general direction. Again, recall $V_{\bar{k}[\epsilon]} \in \mathcal{D}(\bar{k}[\epsilon])$, R that lifts $\bar{k}[\epsilon]$, and V_R. Now we suppose $R = R_1[\epsilon_1] \times_C R_2[\epsilon_2]$ where $R_1 = R_2 = W$ and $C \in \mathcal{C}_{\bar{k}}$. By Definition 3.3, (without loss of generality) we may assume $\varphi(\epsilon_1) = \epsilon$ where ϵ_1 denotes $(\epsilon_1, 0) \in R$. Let v be the valuation of W so that $v(\pi) = 1$.

Recall that $(\epsilon_1, 0)$ being a fiber product in $R = R_1[\epsilon_1] \times_C R_2[\epsilon_2]$ implies $(r\epsilon_1, 0) \in R$ for all $r \in R_1$.

By Definition 3.3, V_R induces $V_{R_1[\epsilon_1]}, V_{R_2[\epsilon_2]}$ by $R \to R_1[\epsilon_1]$, $R \to R_2[\epsilon_2]$. We let

$$V_{\bar{k}[\epsilon_i]} := V_{R_i[\epsilon_i]} \otimes_W W/(\pi), \quad i = 1, 2.$$

Proposition 3.6. *Suppose* $V_{\bar{k}[\epsilon_2]} \neq 0$ *as an element of* $\mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$. *Suppose* $v(p^N) \geq 2$. *Then,* $V_{\bar{k}[\epsilon]} \in \mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$.

Proof. Where $\rho_R : G \to \mathrm{GL}_2(R)$ is given by V_R and a chosen basis, for any $g \in G$ we can write

$$\rho_R(g) = \begin{bmatrix} (a_1 + a'_1\epsilon_1, a_2 + a'_2\epsilon_2) & (b_1 + b'_1\epsilon_1, b_2 + b'_2\epsilon_2) \\ (c_1 + c'_1\epsilon_1, c_2 + c'_2\epsilon_2) & (d_1 + d'_1\epsilon_1, d_2 + d'_2\epsilon_2) \end{bmatrix}.$$

Then, we have $\rho_{R_2[\epsilon_2]}(g) = \begin{bmatrix} a_2 + a'_2\epsilon_2 & b_2 + b'_2\epsilon_2 \\ c_2 + c'_2\epsilon_2 & d_2 + d'_2\epsilon_2 \end{bmatrix}$. By our assumption, there is some g so that at least one of a'_2, b'_2, c'_2, d'_2 is $\not\equiv 0 \pmod{\pi}$, which means there is some $\mathbf{x} = (r + r'\epsilon_1, s + s'\epsilon_2) \in R$ with $s' \in W^\times$. By multiplying s'^{-1} and (since $\bar{r} = \bar{s}$) subtracting some $(w, w) \in W \times_W W \subset R$, we can assume

$$\mathbf{x} = (r + r'\epsilon_1, s + 1 \cdot \epsilon_2) \in R$$

with $r, s \in (\pi)$. Let

$$\varphi(\mathbf{x}) = u_{\mathbf{x}}\epsilon, \quad u_{\mathbf{x}} \in \bar{k}. \tag{3.1}$$

Again recall $\rho_R(g) = \begin{bmatrix} (a_1+a_1'\epsilon_1,a_2+a_2'\epsilon_2) & (b_1+b_1'\epsilon_1,b_2+b_2'\epsilon_2) \\ (c_1+c_1'\epsilon_1,c_2+c_2'\epsilon_2) & (d_1+d_1'\epsilon_1,d_2+d_2'\epsilon_2) \end{bmatrix}$, and note

$$(a_1 + a_1'\epsilon_1, a_2 + a_2'\epsilon_2) = a_2'\mathbf{x} + (a_1' - a_2'r')\epsilon_1 + (a_1 - a_2'r, a_2 - a_2's). \tag{3.2}$$

Now, write

$$\varphi(0,\pi) = u\epsilon, \quad u \in \bar{k}. \tag{3.3}$$

(u is possibly 0.) Note

$$(a_1 - a_2'r, a_2 - a_2's) = (a_1 - a_2'r)(1,1) + (0, a_2 - a_1 + a_2'(r - s)). \tag{3.4}$$

By Definition 3.3,

$$V_{R_i[\epsilon_i]} \otimes R_i \cong T_E \pmod{p^N}, \quad i = 1, 2.$$

So, $a_1 \equiv a_2 \pmod{p^N}$, and by our assumption, $\pi^2 | a_1 - a_2$. Combine them with (3.3), then we have

$$\varphi(0, a_2 - a_1 + a_2'(r-s)) = \frac{a_2 - a_1 + a_2'(r-s)}{\pi} u\epsilon = \bar{a}_2' \cdot \overline{\left(\frac{r-s}{\pi}\right)} \cdot u\epsilon \tag{3.5}$$

Combine this with (3.1), (3.2), (3.4), then we get

$$\begin{aligned}
&\varphi(a_1 + a_1'\epsilon_1, a_2 + a_2'\epsilon_2) \\
&\qquad = \overline{(a_1 - a_2'r)} + \bar{a}_2' u_{\mathbf{x}} \epsilon + (\bar{a}_1' - \bar{a}_2'\bar{r}')\epsilon + \bar{a}_2' \cdot \overline{\left(\frac{r-s}{\pi}\right)} \cdot u\epsilon \\
&\qquad = \bar{a}_1 + \bar{a}_1'\epsilon + \left(u_{\mathbf{x}} - \bar{r}' + \overline{\left(\frac{r-s}{\pi}\right)} \cdot u\right) \bar{a}_2'\epsilon
\end{aligned}$$

This is true for other coefficients, also. Thus, in $\mathrm{Ext}^1(\overline{T}_E, \overline{T}_E)$,

$$V_{\bar{k}[\epsilon]} = V_{\bar{k}[\epsilon_1]} + \left(u_{\mathbf{x}} - \bar{r}' + \overline{\left(\frac{r-s}{\pi}\right)} \cdot u\right) V_{\bar{k}[\epsilon_2]},$$

which is in $\mathrm{Ext}^1_{cr}(\overline{T}_E, \overline{T}_E)$. □

Suppose we want to prove Proposition 3.6 for any $R_{\bar{k}[\epsilon]}$. There are three possible issues.

First, we need to consider a fiber product R of more than two factors. The proof will certainly be more complicated, but it is tempting to say it will still be similar to Proposition 3.6.

Second, Proposition 3.6 only considers $R = W[\epsilon_1] \times_C W[\epsilon_2]$, so we may guess that the fiber products of W's and $W[\epsilon]$'s work better than the fiber products in $\mathcal{S}$. So, we may consider changing Definition 3.2 accordingly.

Third, Proposition 3.6 assumes $V_{\bar{k}[\epsilon_2]} \neq 0$. Probably this is a relatively small technical issue.

The author is hopeful about all three issues, but the (admittedly vague) ideas hinted above are yet to be tested, and likely there is much work to be done. I leave them for future work.

Now, we consider the *second issue*, which is about the representations over Hecke algebras. The author and Choi ([1]) considered various types of Hecke algebras, but a good case to consider is $\mathbf{T} := \mathbf{T}_l(\Gamma_1(M))$, the W-algebra generated by the Hecke operators T_q and $\langle q\rangle$ for all primes $q \nmid M$, and U_q for primes $q|M$ as endomorphisms of $S_l(\Gamma_1(M))$.

Recall f of level $\Gamma_1(M)$ and weight l (see the discussion before Definition 3.3). In particular, recall $T_f \equiv T_E \pmod{p^N}$.

Let

$$\mathfrak{m} = \ker(\mathbf{T} \longrightarrow \bar{k})$$

given by $t(\in \mathbf{T}) \mapsto a_t \pmod{\pi}$ where $tf = a_t f$.

(Assuming M is square-free if necessary) evaluating Hecke operators for each eigenform gives $\mathbf{T} \hookrightarrow \prod_g \mathcal{O}_g$ (which runs over all eigenforms g of the given level and weight) where $\mathcal{O}_g$ is given by adjoining all coefficients of g to W.

By expanding W if necessary, we may assume $\mathcal{O}_g \cong W$ for all g (or all g with $g \equiv f \pmod{\pi}$). Then, we have

$$\mathbf{T}_\mathfrak{m} \hookrightarrow \prod_g W,$$

where g runs over all eigenforms g of level $\Gamma_1(M)$ and weight l with $g \equiv f \pmod{\pi}$. By this or other means, we have $V_{\mathbf{T}_\mathfrak{m}} = \mathbf{T}_\mathfrak{m}^2 \in F_2(\mathbf{T}_\mathfrak{m}, G)$, which is crystalline of weights $[0, l-1]$. *The issue at hand* is that where $\overline{V}_{\mathbf{T}_\mathfrak{m}} = V_{\mathbf{T}_\mathfrak{m}} \otimes W/(\pi)$, we want to show $\overline{V}_{\mathbf{T}_\mathfrak{m}} \in \mathcal{D}(\mathbf{T}_\mathfrak{m} \otimes W/(\pi))$.

First, we need to show $\mathbf{T}_\mathfrak{m} \in \mathcal{S}$. Again, as an illustrative example, we suppose there are only two eigenforms g_1, g_2 of level $\Gamma_1(M)$ and weight l with $g \equiv f \pmod{\pi}$ so that $\mathbf{T}_\mathfrak{m} \hookrightarrow W \times W$. By this, we consider $\mathbf{T}_\mathfrak{m}$ as a W-subalgebra of $W \times W$. Then, $1 \in \mathbf{T}_\mathfrak{m}$ is identified with $(1,1) \in W \times W$.

Since $\mathbf{T}_\mathfrak{m}$ has rank 2 over W, $\mathbf{T}_\mathfrak{m} \supset \pi^s(W \times W)$ if s is big enough. Suppose $\pi^r W \times 0 \subset \mathbf{T}_\mathfrak{m}$. Then, for any $w \in W$,

$$(0, \pi^r w) = \pi^r w \cdot (1,1) - (\pi^r w, 0) \in \mathbf{T}_\mathfrak{m}.$$

Hence, $0 \times \pi^r W \subset \mathbf{T}_\mathfrak{m}$. Hence, there is some r so that $\pi^r(W \times W) \subset \mathbf{T}_\mathfrak{m}$ maximally, i.e., if s or t is smaller than r, then $\pi^s W \times \pi^t W \not\subset \mathbf{T}_\mathfrak{m}$. Since $\mathbf{T}_\mathfrak{m}$ is local, $r > 0$.

Suppose there is $(a,b) \in \mathbf{T}_\mathfrak{m}$ and $a \not\equiv b \pmod{\pi^r}$. Similar to the above, $(a-b, 0) \in \mathbf{T}_\mathfrak{m}$. In other words, $(\pi^{r'} c, 0) \in \mathbf{T}_\mathfrak{m}$ for some $r' < r$, $c \in W^\times$. Then, $\pi^{r'} W \times 0 \subset \mathbf{T}_\mathfrak{m}$, which contradicts the above.

Thus, $a \equiv b \pmod{\pi^r}$. In other words, $(a,b) \in \mathbf{T}_\mathfrak{m}$ if and only if $(a,b) \in W \times_{W/(\pi^r)} W$, i.e.,

$$\mathbf{T}_\mathfrak{m} \cong W \times_{W/(\pi^r)} W.$$

$W \times_{W/(\pi^r)} W$ itself is not in $\mathcal{S}$ unless $r = 1$, but it is quite close. We may be able to resolve this by changing the definition of $\mathcal{S}$ slightly.

Of course assuming there are only two eigenforms congruent to f is extreme, and one can imagine $\mathbf{T}_\mathfrak{m}$ takes a more complicate form of fiber product. But, that itself may not be a big problem. Rather, in the above, we expand W to include all coefficients of g's. But, for patching, we consider $\mathbf{T}_Q$ for the set of auxiliary primes Q, and Q varies. Clearly we cannot fix W for all Q's. Will it pose a much bigger challenge? The author finds this question more vexing than most other issues.

Last, $g \equiv f \pmod{\pi}$ only implies $T_g \equiv T_f \pmod{\pi}$, so $V_{\mathbf{T}_\mathfrak{m}}$ (as $R = \mathbf{T}_\mathfrak{m}$) does not fit Definition 3.3 (d) unless $g_1 \equiv g_2 \equiv f \pmod{p^N}$. To remedy this, instead we may use $\mathrm{Im}(\mathbf{T}_\mathfrak{m} \to \prod_{g \equiv f \pmod{p^N}} \mathcal{O}_g = \prod_{g \equiv f \pmod{p^N}} W)$ and its associated representation. There are some reasons to believe it can work well, but how will it impact patching?

To sum up, we have resolved some issues, but leave some others for future work for now. We hope that we will be able to resolve them similar to the above, perhaps with some adjustments, in not-too-distant future. Nonetheless, we hope that readers will find the work in this paper convincing.

References

[1] S. H. Choi & B. D. Kim, "Congruences of two-variable p-adic L-functions of congruent modular forms of different weights", *Ramanujan J.* **43** (2017), no. 1, p. 163-195.

[2] B. De Smit & H. W. Lenstra, Jr, "Explicit construction of universal deformation rings", in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, Springer, 1997, p. 313-326.

[3] F. Diamond, "The Taylor–Wiles construction and multiplicity one", *Invent. Math.* **128** (1997), no. 2, p. 379-391.

[4] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque, vol. 47-48, Société Mathématique de France, 1977, 262 pages.

[5] J.-M. Fontaine & G. Laffaille, "Construction de representations p-adiques", *Ann. Sci. Éc. Norm. Supér. (4)* **15** (1982), no. 4, p. 547-608.

[6] J.-M. Fontaine & Y. Ouyang, "Theory of p-adic Galois Representations", lecture notes.

[7] B. D. Kim, "Congruences of algebraic p-adic L-functions and the Main Conjecture of Iwasawa Theory", *J. Number Theory* **226** (2021), p. 168-212.

[8] M. Kisin, "Geometric deformations of modular Galois representations", *Invent. Math.* **157** (2004), no. 2, p. 275-328.

[9] B. Mazur, "Deforming Galois representations", in *Galois groups over* $\mathbb{Q}$, Mathematical Sciences Research Institute Publications, vol. 15, Springer, 1989, p. 385-437.

[10] ———, "An introduction to the deformation theory of Galois representations", in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, Springer, 1997, p. 243-311.

[11] B. Perrin-Riou, "Theorie d'Iwasawa p-adique locale et globale", *Invent. Math.* **99** (1990), no. 2, p. 247-292.

[12] ———, "Theorie d'Iwasawa des representations p-adiques sur un corps local", *Invent. Math.* **115** (1994), no. 1, p. 81-149.

[13] R. Ramakrishna, "On a variation of Mazur's deformation functor", *Compos. Math.* **87** (1993), no. 3, p. 269-286.

[14] M. Schlessinger, "Functors of Artin rings", *Trans. Am. Math. Soc.* **130** (1968), p. 208-222.

[15] E. de Shalit, "On certain Galois representations related to the modular curve $X_1(p)$", *Compos. Math.* **95** (1995), no. 1, p. 69-100.

[16] ———, "Hecke rings, and universal deformation rings", in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, Springer, 1997, p. 421-445.

[17] R. Taylor & A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. Math. (2)* **141** (1995), no. 3, p. 553-572.

[18] A. Wiles, "Modular elliptic curves and Fermat's Last Theorem", *Ann. Math. (2)* **141** (1995), no. 3, p. 443-551.

Byoung Du (BD) Kim
School of Mathematics and Statistics
Victoria University of Wellington
Wellington, New Zealand
E-mail: byoungdu.kim@vuw.ac.nz
URL: https://people.wgtn.ac.nz/byoungdu.kim