JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Abhik GANGULI et Suneel KUMAR

Determination of certain mod p Galois representations using local constancy

Tome 38, n° 1 (2026), p. 111-161.

https://doi.org/10.5802/jtnb.1357

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 **38** (2026), 111–161

Determination of certain mod p Galois representations using local constancy

par Abhik GANGULI et Suneel KUMAR

Résumé. Soit $p \geq 5$ un nombre premier et k un entier dans $[2p+2, p^2-p+3]$. Soit b dans $[2,p]$ tel que $k-2 \equiv b \bmod p-1$ et $c := \frac{k-2-b}{p-1}$. Nous donnons un rayon explicite de constance locale dans l'espace des poids de la réduction modulo p des représentations cristallines de dimension deux V_{k,a_p} de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, où la pente $\nu(a_p)$ est supposée dans $(1,c)$ et non entière. Nous utilisons la correspondance de Langlands locale modulo p pour $\mathrm{GL}_2(\mathbb{Q}_p)$ afin de calculer explicitement les réductions modulo p sous des conditions additionnelles sur la pente. Nous montrons que la réduction dans le disque dépend uniquement de k et $\lfloor \nu(a_p) \rfloor$. En application, nous obtenons des réductions modulo p explicites pour de nombreuses nouvelles valeurs de k et a_p. Nous obtenons également un rayon explicite de constance locale dans l'espace a_p (pour un k fixé comme ci-dessus) qui est plus grand que le rayon explicite donné dans un résultat de Berger.

Abstract. Let $p \geq 5$ be a prime and k be an integer in $[2p+2, p^2-p+3]$. Let b be in $[2,p]$ such that $k-2 \equiv b \bmod p-1$ and $c := \frac{k-2-b}{p-1}$. We give an explicit radius of local constancy in the weight space of the mod p reduction of the two dimensional crystalline representations V_{k,a_p} of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, where the slope $\nu(a_p)$ is constrained to be in $(1,c)$ and non-integral. We use the mod p local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ to compute the mod p reductions explicitly under additional conditions on the slope. We show that the reduction in the disk depends only on k and $\lfloor \nu(a_p) \rfloor$. As an application, we obtain explicit mod p reductions at many new values of k and a_p. We also obtain an explicit radius of local constancy in the a_p space (for a fixed k as above) which is bigger than the explicit radius given in a result of Berger.

1. Introduction

Let p be an odd prime and $\nu : \overline{\mathbb{Q}}_p^* \to \mathbb{Q}$ be the normalized p-adic valuation such that $\nu(p) = 1$. For an integer $k \geq 2$ and $0 \neq a_p \in \overline{\mathbb{Q}}_p$ with slope $\nu(a_p) > 0$, let D_{k,a_p} be the weakly admissible filtered φ-module given in [11] with the characteristic polynomial of Frobenius φ given by $X^2 - a_p X + p^{k-1}$

Manuscrit reçu le 30 octobre 2024, révisé le 7 avril 2025, accepté le 30 mai 2025.
2020 *Mathematics Subject Classification.* 11F80, 11F70, 11F33.
Mots-clefs. Reduction of crystalline representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, Local constancy, mod p local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$.

with jumps in the filtration at 0 and $k-1$. By the theorem of Colmez–Fontaine ([25, Theorem A]) there exists a unique irreducible 2-dimensional crystalline representation V_{k,a_p} of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with Hodge–Tate weights $(0, k-1)$ such that $D_{cris}(V^*_{k,a_p}) \cong D_{k,a_p}$. Here D_{cris} is Fontaine's functor defined in [28] and V^*_{k,a_p} is the dual representation of V_{k,a_p}. Let $\overline{V}_{k,a_p}$ be the reduction of a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-stable lattice of V_{k,a_p} up to semisimplification. The problem of explicit computation of the mod p reduction $\overline{V}_{k,a_p}$ is quite intricate, and substantial work has been done using local techniques that involve p-adic Hodge theory and more recently the mod p local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ due to Breuil and Berger ([7, 9, 16, 17]).

We see that V_{k,a_p} is completely determined by a_p and the weight k and thus, so is $\overline{V}_{k,a_p}$. In this article, fixing a_p we study the question of local constancy of $\overline{V}_{k,a_p}$ as a function of k in the weight space. From Berger's local constancy Theorem B of [8] (see Theorem 2.3 below) we expect local constancy to hold if k and k' are p-adically close enough and are in the same class modulo $p-1$. Let $m(k, a_p)$ be the smallest integer m such that $\overline{V}_{k',a_p} \cong \overline{V}_{k,a_p}$ for all $k' \in k + p^{m-1}(p-1)\mathbb{Z}_{\geq 0}$.

Local constancy of the mod p reduction (up to semisimplification) of p-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ holds in general if the representations are specializations of a family of p-adic representations parametrized by an affinoid space (see [21, Section 3.16] and [37, Proposition 5.11] for the version for adic spaces locally of finite type). Colmez in [24, Proposition 5.2] and Chenevier in [21, Propositions 3.9, 3.17] show that such families exist locally in an affinoid open neighborhood of étale points of the Colmez–Chenevier rigid analytic spaces parametrizing trianguline (φ, Γ)-modules. Together with local constancy of the reduction map, existence of such local families provide a crucial input in the proof of Berger's local constancy theorem above. Berger and Colmez ([10, Theorem A]) attach a family of étale (φ, Γ)-modules on an affinoid space, associated to a family of p-adic representations. In the other direction, Kedlaya and Liu in [38] observe that local constancy of the residual representations is a key obstruction to attaching a family of p-adic representations to a given family of étale (φ, Γ)-modules on an affinoid space over $\mathbb{Q}_p$. Furthermore in [38, Theorem 0.2], Kedlaya and Liu give the existence of families of p-adic representations locally in a neighborhood of an étale point of such an affinoid space over $\mathbb{Q}_p$. We refer to the recent work of Conti and Torti ([26, Theorem 1.5, Remark 5.20]) giving neighborhoods of constancy modulo π_L^n (for all $n \gg 0$) for sheaves of p-adic representations on rigid analytic spaces over an extension L of $\mathbb{Q}_p$, admitting affine formal models (see also [42, Proposition 1.3] and [41, Theorem 1.1]).

In the above context, one may ask for the precise reduction in the neighborhoods of local constancy. Results like Theorem 1.1 (and Corollary 1.3)

determine the precise reduction apart from giving an explicit disk of constancy for crystalline representations. We refer to the end of Section 1.2 for a discussion on potential applications of giving explicit radii of local constancy for crystalline representations in the above context of families of trianguline (φ, Γ)-modules.

We write k as $b + c(p-1) + 2$, where we take $b \in [2, p]$ and $c \geq 0$. The first result giving an explicit upper bound for Berger's constant $m(k, a_p)$ is in Bhattacharya [12], and [31] extends the result significantly to cover more values of k and allowing higher slope. Thus, [12] and [31] give an explicit radius of local constancy. In both [12] and [31] the slope $\nu(a_p) > c$, and the precise reduction $\overline{V}_{k',a_p}$ is also given in the disk of constancy.

1.1. Main result. In this article, we consider the problem of local constancy in the situation when $\nu(a_p) < c$ and also non-integral. The approach in [12, 31] and our results here is to compute explicitly and show that $\overline{V}_{k',a_p}$ is constant for all k' in the punctured disk $k + p^t(p-1)\mathbb{Z}_{>0}$ for $t \geq t_0$, where t_0 is given explicitly. In order to compute $\overline{V}_{k',a_p}$, we use the mod p local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$. In [12] and [31], [6, Theorem 1.1.1] together with Berger's local constancy theorem ([8, Theorem B]) are applied to further determine the reduction $\overline{V}_{k,a_p}$ at the center to finally establish local constancy in the disc around the weight k. In our present situation, the condition for Berger's local constancy is already satisfied since $\nu(a_p) < c$, proving the existence of local constancy for these smaller slopes. We use Berger's theorem to infer that since the reduction $\overline{V}_{k',a_p}$ computed in a sufficiently small punctured disk is the same as $\overline{V}_{k,a_p}$ at the center, local constancy must hold in the disk $k + p^t(p-1)\mathbb{Z}_{\geq 0}$ for $t \geq t_0$ around the weight k.

In this smaller slope range the lower bound $\nu(a_p) > \lfloor \frac{k-1}{p} \rfloor$ in Bergdall–Levin, [6] (and also the larger bound from Berger–Li–Zhu, [11]) is not satisfied. Therefore, unlike the generic situation in [12] and [31], we are not able to compute in general the reduction at the center separately, making it difficult to predict the precise reduction in a punctured disk around k. Furthermore, as an important application of local constancy in this slope regime, we instead deduce the precise reduction $\overline{V}_{k,a_p}$ at the center in previously unknown cases of weights and slopes (see Corollary 1.2). Let ν denote $\lfloor \nu(a_p) \rfloor$. Our main result is as follows:

Theorem 1.1. *Let $k = b + c(p-1) + 2$ with $2 \leq c \leq p-1$, $2 \leq b \leq p$ and $p \geq 5$. Fix a_p such that $\nu(a_p)$ is non-integral, $1 < \nu(a_p) < c - \epsilon$, where $\epsilon \in \{0, 1, 2\}$ as defined in (1.2), and let $t > \nu(a_p) + c$.*

(1) *If $b \geq c + \nu - 1$ such that $b \neq 2\nu + 1$ and $(b, \nu) \neq (p, 1)$, then $\overline{V}_{k',a_p} \cong \mathrm{ind}\left(\omega_2^{b+1+\nu(p-1)}\right)$ for all $k' \in k + p^t(p-1)\mathbb{Z}_{\geq 0}$.*

(2) *Further, assume Conjecture 5.2 is true. Suppose* $2 \leq b \leq c-2$ *and* $1 \leq \nu \leq \min\{c-2, p+b-c\}$. *Also assume that* $b \neq 2\nu+2-p$ *if* $b \leq 2c-2-p$. *Then for all* $k' \in k + p^t(p-1)\mathbb{Z}_{\geq 0}$, $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+(\nu+1)(p-1)}\Big)$ *if* $b \leq \nu$, *and* $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1}\Big)$ *if* $b = \nu+1$.

Moreover, in the above cases the Berger's constant $m(k, a_p)$ *exists and* $m(k, a_p) \leq \lceil \nu(a_p) \rceil + c + 1$.

We note that ϵ depends only on k at the centre of the disk of constancy. We refer to Theorem 7.2 where we show more cases of local constancy. We note that in Theorem 1.1 (and Theorem 7.2), we treat only the cases where $\overline{V}_{k',a_p}$ is necessarily irreducible. The omitted values of b in the theorems are precisely the possibly reducible cases that arise from the mod p local Langlands correspondence (see Lemma 2.5). The condition $b \leq c + \nu - 2$ holds in Theorem 1.1 (2). The constraints on b, c and ν in Theorem 1.1 arise quite naturally from our method. This is discussed in detail in Section 1.4 below.

We make an important note that when $\nu(a_p) < c$, the computation on the $\mathrm{GL}_2(\mathbb{Q}_p)$ side becomes substantially more complicated when compared to the situation of $\nu(a_p) > c$. This is because the matrices A (see Conjecture 5.1) in the former case, which have essentially $\alpha(i, l)$ (see (3.1)) as entries, turn out to be much more difficult to analyze. The matrices A arise naturally in a key step to show that certain monomials $q(j)$ are effectively in the kernel of a map P coming from the mod p local Langlands machinery (see Section 1.4 for details). This is precisely Conjecture 5.2 which is also a consequence of Conjecture 5.1. We have been able to show that these matrices have the required property (as given in Conjecture 5.1) only in the cases where we are able to obtain a drastic simplification for the expression $\alpha(i, l)$. This simplification is obtained in a series of steps in Lemma 3.2 and Lemmas 3.5–3.9. We refer to Section 1.4 for more details on the other aspects of our approach.

Although it is Conjecture 5.2 that is needed directly for our main theorem, it is the cases of Conjecture 5.1 that we actually prove. In Theorem 8.1, we prove a substantial portion of Conjecture 5.1. In the cases proved in Theorem 8.1, the matrices A turn out to be non-invertible. We have verified Conjecture 5.1 using SageMath code for all values of b, c, m and primes up to 97. These SageMath computations further reveal that the matrices A in the remaining cases not covered by Theorem 8.1 are all invertible.

1.2. Applications and further considerations. For slope $0 < \nu(a_p) < 2$, the mod p reduction $\overline{V}_{k,a_p}$ is completely known for all the weights (see Section 1.3). Our contribution in computing new cases of $\overline{V}_{k,a_p}$ is therefore when the slope $\nu(a_p) > 2$. Recall that b is the unique integer in $[2, p]$ such that $k-2 \equiv b \bmod p-1$ and $c := \frac{k-2-b}{p-1}$. As a consequence of Theorem 7.2,

we have the following corollary that gives the reduction $\overline{V}_{k,a_p}$ at new values of k and a_p. We note that the first case of reductions given below are coming from Theorem 1.1 (1), and hence unconditional on Conjecture 5.2.

Corollary 1.2. *Fix a_p such that $\nu(a_p)$ is non-integral and $1 < \nu(a_p) < p-1$. Let $p \geq 13$ and assume Conjecture 5.2 is true. Suppose that $k \notin \{2\nu+3+c(p-1), 2\nu+4-p+c(p-1)\}$, where c is given below.*

If $2 \leq \nu \leq \frac{p-1}{2}$, then $\overline{V}_{k,a_p}$ is isomorphic to

$$\begin{cases} \mathrm{ind}\left(\omega_2^{b+1+\nu(p-1)}\right) & \text{if } k \in \bigcup_{c=\nu+1+\epsilon}^{p+1-\nu}[c+\nu+1+c(p-1), p+2+c(p-1)] \\ \mathrm{ind}\left(\omega_2^{b+1+(b-c+1)(p-1)}\right) & \text{if } k \in [2+(\nu+2)p, \nu+(\nu+2)p] \\ \mathrm{ind}\left(\omega_2^{b+1}\right) & \text{if } k \in \{\nu+3+c(p-1) \,|\, \nu+2 \leq c \leq p-1\} \\ \mathrm{ind}\left(\omega_2^{b+1+(\nu+1)(p-1)}\right) & \text{if } k \in I, \end{cases}$$

where $I = \bigcup_{c=\nu+2}^{c_1}[4+c(p-1), \nu+2+c(p-1)] \cup \bigcup_{c=p-\nu+3}^{p-1}[c+\nu+1-p+c(p-1), \nu+2+c(p-1)]$ and $c_1 = \min\{p-\nu+2, p-1\}$.

For a given range of slope, the gaps in the intervals for the weight k in the above corollary are precisely the weights not covered in Theorem 7.2. Corollary 1.2 can be extended to slope $\nu \leq p-3$ with k as given in Corollary 7.4. We have taken the prime $p \geq 13$ in order to give a more uniform and simplified statement.

Next, we will discuss constant ν (recall $\nu = \lfloor \nu(a_p) \rfloor$) local constancy in the weight space. We observe that in Theorem 1.1, the reduction $\overline{V}_{k,a_p}$ at the center k depends only on ν and k. Let $V(k_1, k_2, \alpha_p) := V_{k_2-k_1, p^{k_1}\alpha_p}(-k_1)$ be the $-k_1^{th}$ Tate twist of $V_{k_2-k_1, p^{k_1}\alpha_p}$. Theorem 1.1 gives the following corollary:

Corollary 1.3.

(1) *Assume all the hypotheses of Theorem 1.1 on k and $\nu(a_p)$. Then we have $\overline{V}_{k',a'_p} \cong \overline{V}_{k,a_p}$ for all a'_p of non-integral slope $\nu(a'_p)$ with $\lfloor \nu(a'_p) \rfloor = \nu$, and for all $k' \in k + p^t(p-1)\mathbb{Z}_{\geq 0}$, where $t \geq \lceil \nu(a_p) \rceil + c$.*

(2) *Assume all the hypotheses of Theorem 1.1 on $k := k_2 - k_1$ and $\nu(a_p)$, where $a_p := p^{k_1}\alpha_p$. Then we have $\overline{V}(k'_1, k'_2, \alpha'_p) \cong \overline{V}(k_1, k_2, \alpha_p)$ for all $\alpha'_p \in \overline{\mathbb{Q}}_p$ of non-integral slope with $k'_1 + \lfloor \nu(\alpha'_p) \rfloor = k_1 + \lfloor \nu(\alpha_p) \rfloor$, and for all $k'_1 \in k_1 + p^{t_1}(p-1)\mathbb{Z}$, $k'_2 \in k_2 + p^{t_2}(p-1)\mathbb{Z}$ with $k'_2 - k'_1 \geq k_2 - k_1$, where $\min\{t_1, t_2\} \geq \lceil \nu(\alpha_p) \rceil + k_1 + c$.*

Here we implicitly assume that $k_1, k_2 \in \mathbb{Z}$ such that $k_2 - k_1 \geq 2$, and $\alpha_p \in \overline{\mathbb{Q}}_p$ such that $\nu(\alpha_p) + k_1 > 0$. By using Proposition 3.1.1 of [17], we note that $V(k_1, k_2, \alpha_p)$ are mutually non-isomorphic. The Hodge–Tate weights of $V(k_1, k_2, \alpha_p)$ are $(k_1, k_2 - 1)$ and the trace of the crystalline Frobenius is

α_p. In Corollary 1.3(2), we are forced to take $k_1' = k_1$ if one insists α_p' to be sufficiently close to α_p (e.g. $\alpha_p' \in \alpha_p + p^{\nu(\alpha_p)}\mathfrak{m}_{\overline{\mathbb{Z}}_p}$).

For a fixed weight k, the reduction $\overline{V}_{k,a_p'}$ is a function of a_p'. Theorem A of Berger in [8] proves that for a fixed weight k, the reduction $\overline{V}_{k,a_p'}$ is constant on the disk $a_p + p^{\lambda(k,a_p)}\mathfrak{m}_{\overline{\mathbb{Z}}_p}$ around a_p, where $\lambda(k,a_p) = 2\nu(a_p) + \sum_{n\geq 1}\lfloor\frac{(k-1)}{p^n(p-1)}\rfloor$ and $\mathfrak{m}_{\overline{\mathbb{Z}}_p}$ is the maximal ideal of the ring of integers $\overline{\mathbb{Z}}_p$ of $\overline{\mathbb{Q}}_p$. Under the hypotheses of Theorem 1.1, Corollary 1.3(1) improves the above radius of local constancy in the a_p space. More precisely, taking $k' = k$ in Corollary 1.3(1), we have the following result:

Corollary 1.4. *Assume all the hypotheses of Theorem 1.1 on k and $\nu(a_p)$. Then we have $\overline{V}_{k,a_p'} \cong \overline{V}_{k,a_p}$ for all a_p' with $a_p' \in a_p + p^{\nu(a_p)}\mathfrak{m}_{\overline{\mathbb{Z}}_p}$.*

Let $\Gamma = \Gamma_0(p) \cap \Gamma_1(N)$, where $p \nmid N$. We consider the Coleman–Mazur eigencurve $\mathcal{C}_N$ of tame level N ([18, 23]) with the associated weight map $\kappa : \mathcal{C}_N \to \mathcal{W}$ into the weight space $\mathcal{W}$. Recall that each connected component $\mathcal{W}_\epsilon$ of $\mathcal{W} = \bigcup_\epsilon \mathcal{W}_\epsilon$ can be viewed as the open p-adic unit disk $\mathbf{B}_0 = \{w : \nu(w) > 0\}$ via the map $w_\kappa : \mathcal{W}_\epsilon \to \mathbf{B}_0$, where $w_\kappa = \kappa(1+p) - 1$ for all continuous characters $\kappa : 1 + p\mathbb{Z}_p \to \mathbb{C}_p^*$. We let V_τ denote the semisimple and continuous p-adic representation of $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to $\tau \in \mathcal{C}_N$. Let I_p be the inertia subgroup of $G_\mathbb{Q}$ at p, and let $t_0 = \lceil \nu(a_p)\rceil + c$ be as in Corollary 1.3. We let $\mathcal{U}$ denote an open affinoid (subdomain) of an affinoid neighborhood of a point in $\mathcal{C}_N$. For $u \in \mathcal{C}_N$, let $a_p(u)$ denote the U_p-eigenvalue of the overconvergent eigenform at u.

Corollary 1.5. *Let $\mathcal{U}$ be an affinoid open containing a classical point x_f in $\mathcal{C}_N$. Assume that the weight k and the slope $h = \nu(a_p(x_f)) > 0$ of x_f satisfy the hypotheses of Theorem 1.1. Suppose further that $\mathcal{U}$ has constant slope h (i.e., the map $u \mapsto \nu(a_p(u))$ is constant h on $\mathcal{U}$).*

Then for any $\tau \in \mathcal{U}$ such that

(1) *both $\kappa(\tau), \kappa(x_f)$ are in the same component $\mathcal{W}_\epsilon$ with $w_\kappa(\kappa(\tau)) \in \mathbb{Z}_p$,*
(2) *$\nu(w_\kappa(\kappa(\tau)) - w_\kappa(\kappa(x_f))) \geq t_0 + 1$,*

we have that $\overline{V}_\tau|_{I_p} \cong \overline{V}_{x_f}|_{I_p}$ (and $\overline{V}_\tau$ is irreducible as a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$).

The proof of above applies Corollary 1.3(1), and uses crucially the fact that $h < \frac{k-2}{2}$ (as seen implicitly in Theorem 1.1), and so the point $x_f \in \mathcal{C}_N$ corresponds to the p-stabilization of a cuspidal eigenform of level $\Gamma_1(N)$. Corollary 1.5 is really meaningful only when the affinoid open $\mathcal{U}$ is not contained in a unique connected component of $\mathcal{C}_N$ (for otherwise, the map $\tau \mapsto \overline{V}_\tau^{ss}$ will necessarily be locally constant on $\mathcal{U}$). Also, the weight map need not be a rigid analytic isomorphism on $\mathcal{U}$. It would be interesting

to see if t_{min} giving the exact radius in Corollary 1.3(1) (or the possibly larger t_0) is related to the constant $\mathrm{CS}^k(f)$ defined by Bergdall in [5]. For example, for (k,h) such that $t_{min} \leq \mathrm{CS}^k(f)$, one obtains an upper bound to the maximum possible radius of a disk centered at $\kappa(x_f)$ contained in a p-adic family of constant slope passing through x_f (see [5, Theorems 3.4 and 7.4, and Section 9]).

Let $\mathcal{T}$ be the rigid analytic space over $\mathbb{Q}_p$ that represents the functor $\mathcal{T}(\mathcal{A}) := \{\text{continuous characters } \delta : \mathbb{Q}_p^* \to \mathcal{A}^*\}$ on affinoid $\mathbb{Q}_p$-algebras $\mathcal{A}$ (see [21, Section 1.8]). The condition on k_1' and α_p' in Corollary 1.3(2) suggests that we could also formulate local constancy in terms of variations in the trianguline parameters in $\mathcal{T}^2$. Local constancy of crystalline representations with respect to parameters in $\mathcal{T}^2$ may have interesting consequences for rigid analytic spaces that parameterize families of trianguline (φ,Γ)-modules with sufficient crystalline points like Chenevier's $S_2^{\square}$ (see [21, Theorems 3.3 and 3.14]). Results giving the affinoid open neighborhoods of local constancy in $\mathcal{T}^2$ could help understand better[1] the affinoid open neighborhoods $\mathcal{U}$ in $S_2^{\square}$ of a point x in the étale part $S_2^{\square,0}$ of $S_2^{\square}$ (see [21, Section 3.16]) with algebraic parameters $(\delta_{1,x},\delta_{2,x}) \in \mathcal{T}^2$, where these neighborhoods $\mathcal{U}$ parameterize families of p-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ given by free $\mathcal{O}_{\mathcal{U}}$-modules $V_{\mathcal{U}}$ of rank 2 with continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (see [21, Proposition 3.17]). We are currently pursuing this line of investigation.

1.3. Existing results on the reduction $\overline{V}_{k,a_p}$. We discuss the overlap of our theorem above with known results computing $\overline{V}_{k,a_p}$. Firstly, the reductions $\overline{V}_{k,a_p}$ coming from Theorem 1.1 have no overlap with the (k,a_p) covered in [6, 11, 17]. Theorem 1.1 has a significant number of cases when the slope is in $(1,2)$, and the $\overline{V}_{k,a_p}$ from Theorem 1.1 above match with those from Theorem 1.1 of [14]. Theorem 1.1 also overlaps with Corollary 1.12 of [35], precisely when $b \in [2,c-2]$ and $\nu(a_p) \in (b-1,b)\cup(b,b+1)$ or when $b = c-1$ and $\nu(a_p) = (b-1,b)$. The reductions from Theorem 1.1 match with the ones coming from [35].

We next discuss results that compute $\overline{V}_{k,a_p}$. Breuil in [17] computes $\overline{V}_{k,a_p}$ for weights up to $2p+1$ and for all a_p (see [7, Theorem 3.2.1]). Berger–Li–Zhu in [11] and Bergdall–Levin in [6] treat this problem for sufficiently large slopes $\nu(a_p) > \lfloor \frac{k-2}{p-1} \rfloor$ and $\nu(a_p) > \lfloor \frac{k-1}{p} \rfloor$ respectively. Buzzard–Gee in [19] and [20] determine $\overline{V}_{k,a_p}$ for slope in $(0,1)$ and for all weights. For slope in $(1,2)$, Ganguli–Ghate in [30] compute $\overline{V}_{k,a_p}$ up to weights p^2-p, and Bhattacharya–Ghate in [14] give the reduction for all weights and slope in $(1,2)$ with an additional assumption at $\nu(a_p) = \frac{3}{2}$. Bhattacharya–Ghate–Rozensztajn in [15] treat the case $\nu(a_p) = 1$ for all weights. We refer to

[1] For instance, giving explicit affinoid subdomains of $\mathcal{U}$.

the work of Ghate–Rai in [34] which treats the case of slope $\nu(a_p) = \frac{3}{2}$. More recently, Nagel–Pande in [39] have determined most of the reductions for slope in $(2, 3)$. Furthermore, Rozensztajn in [40] gives an algorithm to compute $\overline{V}_{k,a_p}$ which is efficient for small slopes and weights. We also refer to the recent work of Arsovski [1, 2] in connection to the slope conjecture of Breuil, Buzzard and Emerton. The zig-zag conjecture of Ghate in [32] (see also [33, Conjecture 1.1]) gives an explicit description of $\overline{V}_{k',a_p}$ for all half-integral slopes $1/2 \leq \nu(a_p) \leq \frac{p-1}{2}$ and $k' \geq k$ (and k' sufficiently close to k p-adically), where $3 \leq k \leq p+1$ is such that $k = 2\nu(a_p) + 2$. This conjecture provides important counterexamples to local constancy in the weight space for certain a_p and k (see [32, Theorem 2.2]). We remark that in fact $k > 2\nu(a_p) + 2$ in our theorem above. We refer to the work of Chitrao–Ghate–Yasuda in [22] which explains to a large extent the reason behind these important counterexamples to local constancy.

For results with alternate approaches using global methods which assume the modularity of the Galois representations, we refer to the work of Deligne, Deligne–Serre and Fontaine–Edixhoven (see [27] and also [19, Theorem 1.2]) for modular forms, and the work of Ganguli [29] and Bhattacharya–Ganguli [13] for certain Hilbert modular forms of small slope.

1.4. Outline of the proof. Breuil has constructed a locally algebraic representation Π_{k',a_p} of $\mathrm{GL}_2(\mathbb{Q}_p)$ and a $\mathrm{GL}_2(\mathbb{Q}_p)$-stable lattice Θ_{k',a_p} in Π_{k',a_p} such that $\overline{\Theta}^{ss}_{k',a_p} \cong LL(\overline{V}_{k',a_p})$, where LL is the mod p local Langlands correspondence (see Section 2.1 for more details). Let $r = k' - 2 \geq 0$ be a non-negative integer. Using the definition of Θ_{k',a_p}, we get a canonical surjection $P : \mathrm{ind}_{KZ}^{G}(V_r) \twoheadrightarrow \overline{\Theta}_{k',a_p}$ (see Section 2.3 for more details). For $m \in \mathbb{Z}_{\geq 1}$, we denote $V_r^{(m)} := \{f \in V_r \,|\, \theta^m \text{ divides } f \text{ in } \overline{\mathbb{F}}_p[x, y]\}$, where $\theta := x^p y - xy^p$. From Remark 4.4 of Buzzard–Gee in [19], we deduce that

$$P : \mathrm{ind}_{KZ}^{G}\left(\frac{V_r}{V_r^{(\nu+1)}}\right) \longrightarrow\!\!\!\!\!\rightarrow \overline{\Theta}_{k',a_p}$$

as $\nu(a_p) < \nu + 1$, where $\nu = \lfloor \nu(a_p) \rfloor$. We consider the following filtration

$$0 \subseteq \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(\nu)}}{V_r^{(\nu+1)}}\right) \subseteq \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(\nu-1)}}{V_r^{(\nu+1)}}\right) \subseteq \cdots \subseteq \mathrm{ind}_{KZ}^{G}\left(\frac{V_r}{V_r^{(\nu+1)}}\right).$$

For $0 \leq m \leq \nu$, observe that $\mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(m)}}{V_r^{(m+1)}}\right)$ are the successive quotients in the above filtration. By Lemma 2.4 the successive quotients $\mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(m)}}{V_r^{(m+1)}}\right)$ are generated by $[g, F_m(x, y)]$, where $F_m(x, y) = x^{r-m}y^m - x^{r-(s-m)}y^{s-m}$ and $s = k - 2$. By a contributing factor, we mean the successive quotient

$\mathrm{ind}_{KZ}^{G}\Big(\frac{V_r^{(n)}}{V_r^{(n+1)}}\Big)$ such that $P : \mathrm{ind}_{KZ}^{G}\Big(\frac{V_r^{(n)}}{V_r^{(n+1)}}\Big) \twoheadrightarrow \overline{\Theta}_{k',a_p}$ (we prove that there is always only one contributing factor for Theorem 1.1).

To determine $\overline{\Theta}^{ss}_{k',a_p}$ when $\overline{V}_{k',a_p}$ is irreducible, it is enough to determine the contributing factor (see Lemma 2.5). At first, Proposition 6.1 shows that the map P surjects via $\mathrm{ind}_{KZ}^{G}\Big(\frac{V_r^{(n_1+1)}}{V_r^{(n_2)}}\Big)$, where n_1 and n_2 are as given in the proposition. Next in Theorem 6.4, we prove that $\mathrm{ind}_{KZ}^{G}\Big(\frac{V_r^{(n_0)}}{V_r^{(n_0+1)}}\Big)$ is the contributing factor, where n_0 is defined in the same theorem. The hypotheses of Theorem 6.4 is such that $n_1 = n_0 - 1$ and $n_2 = n_0 + 1$, thus giving that contributing factor comes from n_0. In particular, the condition $b \geq c + \nu - 1$ in Theorem 1.1 (1) arises naturally to give us that $n_0 = \nu$.

We next apply Lemma 2.5 together with Theorem 6.4 to get the reduction $\overline{V}_{k',a_p}$ (in a puncture disk centered at k) in Proposition 7.1. Finally we apply Theorem 2.3 in Theorem 7.2 to determine $\overline{V}_{k,a_p}$ at the center, thereby giving us local constancy in the whole disk.

In Proposition 6.1, we show that $\mathrm{ind}_{KZ}^{G}\Big(\frac{V_r^{(m)}}{V_r^{(m+1)}}\Big)$ do not contribute to $\overline{\Theta}_{k',a_p}$ for all $m \in [0, n_1] \cup [n_2, \nu]$. Using Lemmas 2.1 and 2.2, it is enough to prove that $F_m(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $m \in [1, n_1] \cup [n_2, \nu]$. Next, we explain the steps to prove $F_m(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $m \in [1, n_1] \cup [n_2, \nu]$. By using Remark 4.4 of [19], observe that for each $m \leq \nu$, $F_m(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ if and only if $q(c) = x^{r-s+m}y^{s-m} \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ (as $\nu < \nu(a_p)$; see Section 1.5 for the definition of $q(i)$ in general).

Applying Proposition 4.3, we deduce that there exists $a_{j,l} \in \mathbb{Z}_p$ such that $\sum_j a_{j,l} q(j) \in \mathrm{Ker}(P)$, where $0 \leq j \leq c-1$ and $b-m+j(p-1) > 0$. Further in Lemma 4.1, we prove that for all $\epsilon_1 \leq j \leq c - m - 1$, $q(j)$ are integral linear combinations of $q(j)$ for $c - m \leq j \leq c$. Using this we have

$$\sum_{1 \leq i \leq m+1} \frac{\alpha(i, l)}{p^{\sigma_1(l)}} q(c - m - 1 + i) \in \mathrm{Ker}(P), \tag{1.1}$$

where $\alpha(i, l)$ are as given in (3.1) and $\sigma_1(l)$ in (3.4). This is done in Proposition 4.4. We note from the definition of $\sigma_1(l)$ and $\alpha(i, l)$ that $\alpha(i, l)/p^{\sigma_1(l)}$ is integral for all i, l. Therefore, in order to prove that $q(c) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $m \in [1, n_1] \cup [n_2, \nu]$, we need to show that for each m there exists some l such that the following holds:

(1) The sum $\sum_{1 \leq i \leq m} \frac{\alpha(i,l)}{p^{\sigma_1(l)}} q(c - m - 1 + i)$ vanishes modulo $(V_r^{(m+1)} + \mathrm{Ker}(P))$.
(2) The coefficient $\frac{\alpha(m+1,l)}{p^{\sigma_1(l)}}$ of $q(c)$ (i.e., the last term $i = m + 1$) in the above summation is non-zero mod p.

To prove the statement (1) above, we first check if $\frac{\alpha(i,l)}{p^{\sigma_1(l)}}$ vanish modulo p for all $1 \leq i \leq m$, but we get a negative answer to this in general. Therefore, we ask whether the monomials $q(c-m-1+i) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $1 \leq i \leq m$. To answer this question, we consider the matrix $A = (\alpha(i,l))_{\substack{1 \leq i \leq m+1 \\ 0 \leq l \leq m}}$ and check whether the linear systems $AX = e_i \pmod p$ has a solution for all $1 \leq i \leq m$. We note that $\alpha(i,l)$ has a complicated formula, and so proving that the linear system of equations $AX = e_i \pmod p$ has a solution in general turns out to be quite hard. However, we make the conjecture that the above linear system of equations has a solution (see Conjecture 5.1). We apply Proposition 4.4 to translate Conjecture 5.1 into Conjecture 5.2 which claims that the monomials $q(c-m-1+i) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $1 \leq i \leq m$.

Next, we consider the expression $\frac{\alpha(m+1,l)}{p^{\sigma_1(l)}}$ occurring in the statement (2) above. One can indeed check that $\frac{\alpha(m+1,l)}{p^{\sigma_1(l)}} = d_l$, where d_l is as defined in (3.5). Crucially in Lemma 3.3, we prove that for each m given in the lemma, there exists at least one l such that d_l is non-zero modulo p. We use this in Proposition 4.5 to recover the statement (2) above. Lemma 3.3 is not covering all the values of m in $[1, \nu]$. This is because for the remaining values of m, the coefficients d_l are zero modulo p for all l. This results in the gap between n_1 and n_2 as seen in the various subcases of Proposition 6.1, wherein $n_2 > n_1 + 1$ in general. In our approach, the vanishing of d_l is the key reason for the restrictions appearing on b, c and ν in Theorems 6.4 and 7.2, the other reason being to force $n_1 + 1$ and n_2 to be consecutive. The condition that $\nu(a_p)$ is non-integral appears first in Proposition 4.5, and is required so that one is able to apply Proposition 4.3 and Lemma 3.3.

We note importantly that Proposition 4.5 requires Conjecture 5.2 as a hypothesis, and thus Conjecture 5.2 is also needed crucially for Proposition 6.1. We also remark that Lemma 5.4 proves Conjecture 5.1 in the cases required to make Theorem 1.1 (1) (i.e., Theorem 7.2 (1)) unconditional on Conjecture 5.2 (see Remark 7.3 for more details).

1.5. Notations and Conventions. We fix the following conventions in the rest of this article unless stated otherwise:

(1) The integer p always denotes a prime number greater than or equal to 5. The integers b and c are from $\{2, 3, \ldots, p\}$ and $\{0, 1, \ldots, p-2\}$ respectively.
(2) We define ϵ as follows

$$\epsilon = \begin{cases} 0 & \text{if } 2c-1 \leq b \leq p \\ 1 & \text{if } 2(c-1) - p \leq b \leq 2(c-1) \\ 2 & \text{if } 2 \leq b \leq 2(c-1) - (p+1). \end{cases} \tag{1.2}$$

(3) We define ϵ_1 as follows

$$\epsilon_1 = \begin{cases} 0 & \text{if } 2m+1 \leq b \leq p \\ 1 & \text{if } 2m+1-(p-1) \leq b \leq 2m \\ 2 & \text{if } 2 \leq b \leq 2m-(p-1). \end{cases} \tag{1.3}$$

(4) We write $s = b + c(p-1)$ and $r = s + p^t(p-1)d$ with $p \nmid d$, and $t, d \in \mathbb{N}$ and so $s < r$.

(5) For $n \in \mathbb{Z}_{\geq 0}$ and $k \in \mathbb{Z}$, we define $\binom{n}{k} = 0$ if $k > n$ or $k < 0$ and the usual binomial coefficient otherwise.

(6) For $A \equiv B$, where $A, B \in \mathrm{M}_n(\mathbb{Z}_p)$ we mean that $A \equiv B \bmod p$.

(7) Unless stated otherwise, for $A, B \in \mathrm{ind}_{KZ}^{G}(\mathrm{Sym}^r(\overline{\mathbb{Q}}_p^2))$, by $A \equiv B$ or $A \equiv B \bmod p$ we mean that $A - B$ is in $\mathbf{m}_{\overline{\mathbb{Z}}_p}\, \mathrm{ind}_{KZ}^{G}(\mathrm{Sym}^r(\overline{\mathbb{Z}}_p^2))$.

(8) By the vectors $\{e_j\}$ we mean the standard basis of $\mathbb{Z}_p^n$ for $n \in \mathbb{N}$.

(9) For $v \in \mathrm{Sym}^r(\overline{\mathbb{F}}_p^2)$, by $v \in \mathrm{Ker}(P)$ or $v \in V_r^{m+1} + \mathrm{Ker}(P)$ we mean that $[1,\ v] \in \mathrm{Ker}(P)$ or $[1,\ v] \in \mathrm{ind}_{KZ}^{G}(V_r^{m+1}) + \mathrm{Ker}(P)$ respectively.

(10) We define $q(i) = x^{r-b+m-i(p-1)}y^{b-m+i(p-1)}$ for all $n_0 \leq i \leq c$ and $1 \leq m \leq p-1$, where $n_0 = 0$ if $b \geq m$ and 1 otherwise.

2. Background

2.1. The mod p local Langlands correspondence. We begin by recalling some notations and definitions. We fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ with the ring of integers $\overline{\mathbb{Z}}_p$ and the residue field $\overline{\mathbb{F}}_p$. Let G_p and G_{p^2} be the absolute Galois groups of $\mathbb{Q}_p$ and $\mathbb{Q}_{p^2}$ respectively where $\mathbb{Q}_{p^2}$ is the unique unramified quadratic extension of $\mathbb{Q}_p$. Let $\omega_1 = \omega$ be the mod p cyclotomic character, and ω_2 be a fixed fundamental character of level 2. We view ω_1 as a character of $\mathbb{Q}_p^*$ via local class field theory, identifying uniformizers with geometric Frobenii. For $a \in \mathbb{Z}^{\geq 0}$ such that $(p+1) \nmid a$ let $\mathrm{ind}(\omega_2^a)$ denote the unique two dimensional irreducible representation of G_p with determinant ω^a and whose restriction to inertia is isomorphic to $\omega_2^a \oplus \omega_2^{ap}$.

We denote the group $\mathrm{GL}_2(\mathbb{Q}_p)$ by G, its maximal compact subgroup $\mathrm{GL}_2(\mathbb{Z}_p)$ by K and the center of G by $Z \cong \mathbb{Q}_p^*$. For $r \geq 0$ let $V_r := \mathrm{Sym}^r(\overline{\mathbb{F}}_p^2)$ be the symmetric power representation of $\mathrm{GL}_2(\mathbb{F}_p)$ of dimension $r+1$. We can also view V_r as representations of KZ by defining the action of K through the natural surjection $K \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_p)$, and by letting p act trivially. For $0 \leq r \leq p-1$, $\lambda \in \overline{\mathbb{F}}_p$ and a smooth character $\eta : \mathbb{Q}_p^* \to \overline{\mathbb{F}}_p^*$, the representation

$$\pi(r, \lambda, \eta) := \frac{\mathrm{ind}_{KZ}^{G}(V_r)}{T - \lambda} \otimes (\eta \circ \det)$$

is a smooth admissible representation of G where ind_{KZ}^{G} denotes compact induction (see [16, 19]). The operator T (see Section 2.2) is the Hecke

operator T_p generating the Hecke algebra $\mathrm{End}_G(\mathrm{ind}_{KZ}^G(V_r)) = \overline{\mathbb{F}}_p[T_p]$. The irreducible subquotients of these representations give all the irreducible smooth admissible representations of G ([3, 4, 16]). For $\lambda \in \overline{\mathbb{F}}_p^*$, let μ_λ be the unramified character of G_p that sends the geometric Frobenius to λ. Then Breuil 's semisimple mod p local Langlands correspondence LL (see [17]) is as follows:

- $\lambda = 0 : \mathrm{ind}(\omega_2^{r+1}) \otimes \eta \overset{LL}{\longleftrightarrow} \pi(r, 0, \eta)$
- $\lambda \neq 0 : (\mu_\lambda \omega^{r+1} \oplus \mu_{\lambda^{-1}}) \otimes \eta \overset{LL}{\longleftrightarrow} \pi(r, \lambda, \eta)^{ss} \oplus \pi([p-3-r], \lambda^{-1}, \omega^{r+1}\eta)^{ss}$ where $\{0, 1, \ldots, p-2\} \ni [p-3-r] \equiv p-3-r \bmod (p-1)$.

For integers $k \geq 2$ we define $\Pi_{k,a_p} := \frac{\mathrm{ind}_{KZ}^G(\mathrm{Sym}^r(\overline{\mathbb{Q}}_p^2))}{T-a_p}$ as representations of G where $r = k-2$ and T is the Hecke operator from Section 2.2. We consider the G-stable lattice Θ_{k,a_p} in the representation Π_{k,a_p} (see [9, 17]) given by

$$\begin{aligned}\Theta_{k,a_p} &:= \mathrm{image}\Big(\mathrm{ind}_{KZ}^G(\mathrm{Sym}^r(\overline{\mathbb{Z}}_p^2)) \longrightarrow \Pi_{k,a_p}\Big) \\ &\cong \frac{\mathrm{ind}_{KZ}^G(\mathrm{Sym}^r(\overline{\mathbb{Z}}_p^2))}{(T-a_p)\,\mathrm{ind}_{KZ}^G(\mathrm{Sym}^r(\overline{\mathbb{Q}}_p^2)) \cap \mathrm{ind}_{KZ}^G(\mathrm{Sym}^r(\overline{\mathbb{Z}}_p^2))}.\end{aligned}$$

By the compatibility of the p-adic and mod p local Langlands correspondences ([7, 9, 17]) we have

$$\overline{\Theta}_{k,a_p}^{ss} \cong LL(\overline{V}_{k,a_p}) \quad \text{where} \quad \overline{\Theta}_{k,a_p} := \Theta_{k,a_p} \otimes \overline{\mathbb{F}}_p.$$

Since the mod p local Langlands correspondence is injective, to determine $\overline{V}_{k,a_p}$ it is enough to compute $\overline{\Theta}_{k,a_p}^{ss}$.

2.2. Hecke Operator T. We give an explicit definition of the Hecke operator $T = T_p$ below (see [17] for more details). For $m = 0$, set $I_0 = \{0\}$ and for $m > 0$, let $I_m = \{[\lambda_0] + p[\lambda_1] + \cdots + p^m[\lambda_{m-1}] \mid \lambda_i \in \mathbb{F}_p\} \subset \mathbb{Z}_p$ where square brackets denote Teichmüller representatives. For $m \geq 1$ there is a truncation map $[\ ]_{m-1} : I_m \to I_{m-1}$ given by taking the first $m-1$ terms in the p-adic expansion above. For $m = 1$, $[\ ]_{m-1}$ is the zero map. For $m \geq 0$ and $\lambda \in I_m$, let

$$g_{m,\lambda}^0 = \begin{pmatrix} p^m & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad g_{m,\lambda}^1 = \begin{pmatrix} 1 & 0 \\ p\lambda & p^{m+1} \end{pmatrix}.$$

Then we have

$$G = \coprod_{\substack{m \geq 0, \lambda \in I_m \\ i \in \{0,1\}}} KZ(g_{m,\lambda}^i)^{-1}.$$

Let R be a $\mathbb{Z}_p$-algebra and $V = \mathrm{Sym}^r R^2$ be the symmetric power representation of KZ, modelled on homogeneous polynomials of degree r in the variables x and y over R. For $g \in G,\ v \in V$, let $[g,\ v]$ be the function

defined by: $[g,v](g') = g'g \cdot v$ for all $g' \in KZg^{-1}$ and zero otherwise. Since an element of $\mathrm{ind}_{KZ}^{G}(V)$ is a V-valued function on G that has compact support modulo KZ, one can see that every element of $\mathrm{ind}_{KZ}^{G}(V)$ can be written as a finite sum of $[g,v]$ with $g = g_{m\lambda}^{0}$ or $g = g_{m,\lambda}^{1}$, for some $\lambda \in I_m$ and $v \in V$. Then the action of T on $[g,v]$ can be given explicitly when $g = g_{n,\mu}^{0}$ with $n \geq 0$ and $\mu \in I$. Let $v = \sum_{j=0}^{r} c_j x^{r-j} y^j$, with $c_j \in R$. We write $T = T^+ + T^-$ where

$$T^+([g_{n,\mu}^{0}, v]) = \sum_{\lambda \in I_1} \left[g_{n+1,\mu+p^n\lambda}^{0}, \sum_{j=0}^{r} p^j \left(\sum_{i=j}^{r} c_i \binom{i}{j} (-\lambda)^{i-j} \right) x^{r-j} y^j \right]$$

$$T^-([g_{n,\mu}^{0}, v]) = \left[g_{n-1,[\mu]_{n-1}}^{0}, \sum_{j=0}^{r} \left(\sum_{i=j}^{r} p^{r-i} c_i \binom{i}{j} \left(\frac{\mu - [\mu]_{n-1}}{p^{n-1}} \right)^{i-j} \right) x^{r-j} y^j \right] \text{ for } n > 0$$

$$T^-([g_{n,\mu}^{0}, v]) = \left[\alpha, \sum_{j=0}^{r} p^{r-j} c_j x^{r-j} y^j \right] \quad \text{for } n = 0, \text{ where } \alpha := g_{0,0}^{1}.$$

2.3. The filtration. Let $k' = k + p^t(p-1)d$ satisfy the hypotheses of Theorem 1.1. Since $t \geq \lceil 2\nu(a_p) \rceil + \epsilon$, we have $r = k' - 2 \geq (\nu+1)(p+1)$, where $\nu = \lfloor \nu(a_p) \rfloor$. From the definition of V_r and $\overline{\Theta}_{k',a_p}$ it follows that there is a natural surjection

$$P : \mathrm{ind}_{KZ}^{G}(V_r) \longrightarrow\!\!\!\!\!\rightarrow \overline{\Theta}_{k',a_p}.$$

Now, let us consider the Dickson polynomial $\theta := x^p y - xy^p \in V_{p+1}$. Here we note that $\mathrm{GL}_2(\mathbb{F}_p)$ acts on θ by the determinant character. For $m \in \mathbb{N}$, let us denote

$$V_r^{(m)} = \left\{ f \in V_r \,\middle|\, \theta^m \text{ divides } f \text{ in } \overline{\mathbb{F}}_p[x,y] \right\}$$

which is a subrepresentation of V_r. By using Remark 4.4 of [19], one can see that the map P factors through $\mathrm{ind}_{KZ}^{G}\left(\frac{V_r}{V_r^{(\nu+1)}}\right)$, where $\nu := \lfloor \nu(a_p) \rfloor$. So let us consider the following chain of submodules

$$0 \subseteq \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(\nu)}}{V_r^{(\nu+1)}}\right) \subseteq \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(\nu-1)}}{V_r^{(\nu+1)}}\right) \subseteq \cdots \subseteq \mathrm{ind}_{KZ}^{G}\left(\frac{V_r}{V_r^{(\nu+1)}}\right). \tag{2.1}$$

For $0 \leq m \leq \nu$, observe that $\mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(m)}}{V_r^{(m+1)}}\right)$ are the successive quotients in the above filtration. In the following two lemmas we make precise the notion of a successive quotient not contributing to $\overline{\Theta}_{k',a_p}$ via the map P.

Lemma 2.1. *Let $1 \leq n \leq \nu$ and assume for all $0 \leq m \leq n-1$ that there exists $W_m \subset V_r^{(m)}$ such that $P\left(\mathrm{ind}_{KZ}^{G}(W_m)\right) = 0$ and $W_m \twoheadrightarrow \frac{V_r^{(m)}}{V_r^{(m+1)}}$ induced by the inclusion $W_m \subset V_r^{(m)}$. Then the map P restricted to $\mathrm{ind}_{kZ}^{G}\left(\frac{V_r^{(n)}}{V_r^{(\nu+1)}}\right)$ is a surjection.*

Lemma 2.2. *Let $1 \leq n \leq \nu$ and suppose for all $n \leq m \leq \nu$ that there exists $G_m(x,y) \in V_r$ such that $P([g,\ G_m(x,y)]) = 0$. If $G_m(x,y)$ generates $\frac{V_r^{(m)}}{V_r^{(m+1)}}$ then the map P factors through $\mathrm{ind}_{kZ}^{G}\left(\frac{V_r}{V_r^{(n)}}\right)$.*

2.4. JH factors of $V_r^{(n)}/V_r^{(n+1)}$. In this subsection, we assume simply that $r, n \in \mathbb{Z}_{\geq 0}$ such that $r \geq (n+2)(p+1) - 3$ so that we can apply Theorems (4.1) and (4.2) of [36] below. Next, we determine the Jordan–Holder factors of the successive quotients $\frac{V_r^{(n)}}{V_r^{(n+1)}}$. Let D denote the determinant character of $\mathrm{GL}_2(\mathbb{F}_p)$. Let us write $r - n(p+1) = r' + d'(p-1)$ such that $p \leq r' \leq 2p-2$ and for some $d' \in \mathbb{Z}^{\geq 0}$. Theorems (4.1) and (4.2) of [36] together with Lemma 5.1.3 of [17] gives:

(i) if $r' = p$ then

$$0 \longrightarrow V_1 \otimes D^n \longrightarrow \frac{V_r^{(n)}}{V_r^{(n+1)}} \longrightarrow V_{p-2} \otimes D^{n+1} \longrightarrow 0. \tag{2.2}$$

The first map sends $(x,\ y)$ to $(\theta^n x^{r-n(p+1)},\ \theta^n y^{r-n(p+1)})$ and the second map sends $\theta^n x^{r-n(p+1)-1} y$ to x^{p-2}.

(ii) if $r' \neq p$ then

$$0 \longrightarrow V_{r'-(p-1)} \otimes D^n \longrightarrow \frac{V_r^{(n)}}{V_r^{(n+1)}} \longrightarrow V_{2(p-1)-r'} \otimes D^{n+r'-(p-1)} \longrightarrow 0. \tag{2.3}$$

The first map sends $(x^{r'-(p-1)}, y^{r'-(p-1)})$ to $(\theta^n x^{r-n(p+1)}, \theta^n y^{r-n(p+1)})$ because $\binom{r'}{p-1} \equiv 0 \bmod p$ as $1 \leq r' - p \leq p-2$. For $r' - (p-1) \leq i \leq p-1$, the second map sends $\theta^n x^{r-n(p+1)-i} y^i$ to $\alpha_i\ x^{p-1-i} y^{p-1-r'+i}$ where $\alpha_i := (-1)^{r'-i}\binom{2(p-1)-r'}{p-1-r'+i} \not\equiv 0 \bmod p$ because $0 \leq 2(p-1) - r' \leq p-3$ and $0 \leq p-1-r'+i \leq 2(p-1) - r'$.

2.5. Some crucial results. In this section, we state Berger's local constancy theorem and some crucial lemmas required later.

Theorem 2.3 (Berger [8])**.** *Suppose $a_p \neq 0$ with $\nu(a_p) > 0$ and $k >^2 3\nu(a_p) + \frac{(k-1)p}{(p-1)^2} + 1$, then there exists $m = m(k, a_p)$ such that $\overline{V}_{k',a_p} \cong \overline{V}_{k,a_p}$, if $k' - k \in p^{m-1}(p-1)\mathbb{Z}_{\geq 0}$.*

For integers $0 \leq m \leq s$ let us define polynomials F_m in V_r as follows

$$F_m(x,y) := x^m y^{r-m} - x^{r-s+m} y^{s-m}$$

where $r > s$ and $r \equiv s \bmod (p-1)$.

[2]Theorem B of [8] is actually stronger, wherein the lower bound on k is $3\nu(a_p) + \alpha(k-1) + 1$. Here $\alpha(k-1) = \sum_{n \geq 1} \lfloor (k-1)/(p^{n-1}(p-1)) \rfloor$. We note that although $\frac{(k-1)p}{(p-1)^2} \geq \alpha(k-1)$, it is easier to use this bigger bound for calculations.

Lemma 2.4 (Bhattacharya [12, Lemma 3.2])**.** *Let $r \equiv s \bmod (p-1)$, and $t = \nu(r-s) \geq 1$ and $1 \leq m \leq p-1$.*

(1) *For $s \geq 2m$, the polynomial F_m is divisible by θ^m but not by θ^{m+1}.*
(2) *For $s > 2m$, the image of F_m generates the subquotient $\frac{V_r^{(m)}}{V_r^{(m+1)}}$ as a $\mathrm{GL}_2(\mathbb{F}_p)$-module.*

Lemma 2.5 ([31, Lemma 6.1])**.** *Let $p \geq 5$ and r, n be integers such that $0 \leq n \leq p-1$ and $r \geq (n+2)(p+1)-3$. Let $b \equiv r \bmod p-1$ such that $2 \leq b \leq p$. Suppose the map*

$$P : \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(n)}}{V_r^{(n+1)}}\right) \longrightarrow \overline{\Theta}_{r+2,a_p} \tag{2.4}$$

is a surjection. Further if $(b,n) \notin \{(p-2,\ 0), (p,0), (p,1)\}$ and also $b \notin \{2n \pm 1, 2(n+1)-p, 2n-p\}$ then

$$\overline{V}_{r+2,a_p} \cong \begin{cases} \mathrm{ind}\left(\omega_2^{b+n(p-1)+1}\right) & \text{if } 2n+1 \leq b \leq p \\ \mathrm{ind}\left(\omega_2^{b+(n+1)(p-1)+1}\right) & \text{if } 2n+1-(p-1) \leq b \leq 2n \\ \mathrm{ind}\left(\omega_2^{b+(n+2)(p-1)+1}\right) & \text{if } 2(n+1)-2(p-1) \leq b \leq 2n-(p-1). \end{cases}$$

3. Binomial Identities

In this section, we consider some technical lemmas that we use later.

Lemma 3.1. *For $0 \neq a, m \in \mathbb{Z}_{\geq 0}$ and $1 \leq i \leq m+1$, let*

$$\beta(a,i) := \begin{cases} \binom{m+1}{i} & \text{if } a = 1 \\ \sum_{1 \leq l \leq a-1} (-1)^{l+1} \binom{m+1}{l} \beta(a-l,i) + (-1)^{a-1} \binom{m+1}{i+a-1} & \text{if } a \geq 2 \end{cases}$$

then $\beta(a,i) = \binom{i+a-2}{a-1}\binom{m+a}{i+a-1}$.

Proof. We refer to Lemma A.1 for the proof. □

For $0 \leq l \leq p-1$ and $1 \leq i \leq m+1$, we define $\alpha(i,l)$ as follows

$$\alpha(i,l) := \begin{cases} \alpha_1(i,l) + \binom{r-l}{b-m+(i+c-m-1)(p-1)} & \text{if } 1 \leq i \leq m \\ \alpha_1(i,l) & \text{if } i = m+1 \end{cases} \tag{3.1}$$

where

$$\alpha_1(i,l) = (-1)^{i+1} \sum_{1 \leq a \leq c-m-\epsilon_1} \binom{r-l}{b-m+(c-m-a)(p-1)} \beta(a,i) \tag{3.2}$$

and $\beta(a,i)$ is defined as in Lemma 3.1. For $1 \le i \le m+1$, we define $\alpha'(i,l)$ as follows

(3.3)

$$\alpha'(i,l) := \begin{cases} 0 & \text{if } \ 0 \le l \le b-c \\ (-1)^{i+1} \sum_{c_0 \le a \le c_1} \binom{p+b-c-l}{b-c+a} \binom{c-1}{c-m-a} \beta(a,i) & \text{if } c_2 \le l \le p+b-c \\ (-1)^{i+1} \sum_{1 \le a \le c_1} \binom{2p+b-c-l}{p+b-c+a} \binom{c-2}{c-m-1-a} \beta(a,i) & \text{if } p+c_2 \le l \le m \end{cases}$$

where $c_0 = \max\{c-b, 1\}$, $c_1 = c-m-\epsilon_1$, $c_2 = b-c+1$.

Lemma 3.2. *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and $t \ge 2$. Assume that $2 \le b \le p$, $0 \le c \le p-1$, $1 \le m \le c-1$, $1 \le i \le m+1$ and $0 \le l \le m$. Let*

$$X(i,l) = \binom{r-l}{b-m+(i+c-m-1)(p-1)}.$$

Then $\alpha_1(i,l) \equiv \alpha'(i,l)$ and

$$X(i,l) \equiv \begin{cases} \binom{b-c-l}{b-c+1-i}\binom{c}{c-m-1+i} & \text{if } 0 \le l \le b-c,\ 1 \le i \le b-c+1 \\ \binom{p+b-c-l}{b-c+1-i}\binom{c-1}{c-m-1+i} & \text{if } b-c+1 \le l \le p+b-c,\ 1 \le i \le b-c+1 \\ 0 & \text{if } 0 \le l \le b-c,\ b-c+2 \le i \le p+b-c+1 \\ \binom{p+b-c-l}{p+b-c+1-i}\binom{c-1}{c-m-2+i} & \text{if } b-c+1 \le l \le p+b-c,\ b-c+2 \le i \le p+b-c+1 \\ \binom{2p+b-c-l}{p+b-c+1-i}\binom{c-2}{c-m-2+i} & \text{if } p+b-c+1 \le l \le p-1,\ b-c+2 \le i \le p+b-c+1 \\ 0 & \text{if } b-c+1 \le l \le p+b-c,\ p+b-c+2 \le i \le p-1 \\ \binom{2p+b-c-l}{2p+b-c+1-i}\binom{c-2}{c-m-3+i} & \text{if } p+b-c+1 \le l \le p-1,\ p+b-c+2 \le i \le p-1. \end{cases}$$

Proof. First, we note that

$$\begin{aligned} r-l &= b-c-l+cp+p^t(p-1)d \\ b-m+(c-m-a)(p-1) &= b-c+a+(c-m-a)p \\ b-m+(c-m-1+i)(p-1) &= b-c+1-i+(c-m-1+i)p \end{aligned}$$

If $0 \le l \le b-c$ and $1 \le i \le m+1$, then by Lucas Theorem we have

$$\begin{aligned} &(-1)^{i+1} \sum_{1 \le a \le c-m} \binom{r-l}{b-m+(c-m-a)(p-1)} \beta(a,i) \\ &\quad \equiv (-1)^{i+1} \sum_{1 \le a \le c-m} \binom{b-c-l}{b-c+a}\binom{c}{c-m-a}\binom{i+a-2}{a-1}\binom{m+a}{i+a-1} \\ &\quad \equiv 0 \bmod p. \end{aligned}$$

The last congruence follows since $\binom{b-c-l}{b-c+a} = 0$ as $b-c-l < b-c+a$. Thus, we obtain the result in this case by using the above calculation together

with

$$\binom{r-l}{b-m+(c-m-a+i)(p-1)} \equiv \binom{b-c-l}{b-c+1-i}\binom{c}{c-m-1+i}.$$

By a similar computation, one obtains results in all other cases also. □

Let $S = \{j \mid 0 \le j \le c-1 \text{ and } b-m+j(p-1) > 0\}$. For $0 \le l \le p-1$, we define

$$\begin{aligned} y(j,l) &= \binom{r-l}{b-m+j(p-1)} \quad \forall\, j \in S \\ \text{and } \sigma_1(l) &= \begin{cases} 1 & \text{if } y(j,l) \equiv 0 \bmod p \ \ \forall\, j \in S \\ 0 & \text{if } y(j,l) \not\equiv 0 \bmod p \ \text{ for at least one } j \in S. \end{cases} \end{aligned} \tag{3.4}$$

For any $1 \le \nu \le p-1$ and $0 \le l \le \nu - \sigma_1(l)$, we define d_l as follows

$$d_l := \frac{(-1)^m}{p^{\sigma_1(l)}} \sum_{\epsilon_1 \le j \le c-m-1} \binom{c-1-j}{m}\binom{r-l}{b-m+j(p-1)}. \tag{3.5}$$

Lemma 3.3. *Let $s = b + c(p-1)$ with $2 \le b \le p$, $1 \le c \le p-1$ and $r = s + p^t(p-1)d$, with $t \ge 2$, $p \nmid d$. Fix a ν in $[1, c-1-\epsilon]$. Assume that $1 \le m \le \nu$ and $l \in [0, \nu - \sigma_1(l)]$.*

1. *If $c-1 \le b \le p$, and $1 \le m \le \min\{\nu-1, b-c\}$, then for each m there exists at least one l such that $d_l \ne 0 \bmod p$.*
2. *If $c-1 \le b \le p$, and $b-\nu \le m \le \nu$, then for each such m there exists at least one l such that $d_l \ne 0 \bmod p$.*
3. *If $2c-2-p \le b \le c-2$, and $1 \le \nu \le c-2$, then for each $m \in ([b-\nu, \nu] \cap [1, b-1]) \cup [b, \nu-1]$, there exists at least one l such that $d_l \ne 0 \bmod p$.*
4. *If $2 \le b \le 2(c-1)-p-1$, and $1 \le \nu \le p+b-c$, then for each $m \in ([b-\nu, \nu] \cap [1, b-1]) \cup [b, \nu-1]$, there exists at least one l such that $d_l \ne 0 \bmod p$.*
5. *If $2 \le b \le 2(c-1)-p-1$ and $p+b-c+1 \le \nu \le c-3$, then for each $m \in [1, p+b-c] \cup [p+b-\nu-1, \nu]$, there exists at least one l such that $d_l \ne 0 \bmod p$.*

Remark 3.4. The range of l is $[0, \nu - \sigma_1(l)]$ in Lemma 3.3 since it is applied in Proposition 4.5 wherein l is in $[0, \nu]$ (or $[0, \nu-1]$). Further, in almost all cases of above lemma, the l for which $d_l \not\equiv 0 \bmod p$ is given in terms of m. As will be clear in the proof below, the range of m in the cases below is given primarily so that the desired l (such that $d_l \not\equiv 0 \bmod p$) lies in $[0, \nu - \sigma_1(l)]$.

Proof. For each b, c, m as in the statement, in the following cases, we prove that there exists at least one $l \in [0, \nu - \sigma_1(l)]$ such that $d_l \not\equiv 0 \bmod p$. For the range of $0 \leq l \leq \nu - \sigma_1(l)$ and $\epsilon_1 \leq j \leq c - m - 1$, we define

$$a_{j,l} = \frac{\binom{r-l}{b-m+j(p-1)}}{p^{\sigma_1(l)}}.$$

We now outline the main steps in general for all the cases. We provide the proof for the first part of the lemma as an illustration of these steps. In the first step, we compute $a_{j,l}$ modulo p by applying Lemma 3.4 and Lemma 3.5 of [31] depending on whether the value of $\sigma_1(l) = 0$ or $\sigma_1(l) = 1$. In the second step, we rearrange the binomial coefficients appearing in d_l in a way similar to equation (3.8) below. Pulling out the binomial coefficients that are independent of j from the sum, we apply Vandermonde's identity on the sum for d_l similar to (3.9) in each case to finally arrive at the required expression for d_l. We observe that d_l is non-zero modulo p for the following values of l.

(1) $l = m$ if $c - 1 \leq b \leq p$, and $1 \leq m \leq \min\{\nu - 1, b - c\}$.
(2) Let $c - 1 \leq b \leq p$ and $b - \nu \leq m \leq \nu$. Then $l = b - m$ if $b \geq 2m + 1$ and $l = b - m - 1$ if $b \leq 2m$.
(3) Let $2c - 2 - p \leq b \leq c - 2$, and $1 \leq \nu \leq c - 2$. Then

$$l = \begin{cases} b - m & \text{if } m \in [b - \nu, \nu] \cap [1, b - 1] \text{ and } b \geq 2m + 1 \\ b - m - 1 & \text{if } m \in [b - \nu, \nu] \cap [1, b - 1] \text{ and } b \leq 2m \\ m & \text{if } m \in [b, \nu - 1]. \end{cases}$$

(4) Let $2 \leq b \leq 2(c - 1) - p - 1$, and $1 \leq \nu \leq p + b - c$. Then the same l will work as given in (3) above.
(5) Let $2 \leq b \leq 2(c - 1) - p - 1$ and $p + b - c + 1 \leq \nu \leq c - 3$. Then

$$l = \begin{cases} b - m & \text{if } m \in [1, b - 1] \text{ and } b \geq 2m + 1 \\ 0 & \text{if } m \in [1, b - 1] \text{ and } b \leq 2m \\ p + b - c & \text{if } m \in [b, p + b - c] \text{ and } b \geq 2m + 1 - (p - 1) \\ p + b - c + 1 & \text{if } m \in [b, p + b - c] \text{ and } b \leq 2m - (p - 1) \\ p + b - m - 1 & \text{if } m \in [p + b - \nu - 1, \nu] \text{ and } b \geq 2m + 1 - (p - 1) \\ p + b - c + 1 & \text{if } m \in [p + b - \nu - 1, \nu] \text{ and } b \leq 2m - (p - 1). \end{cases}$$

Next, we will prove the first part of the lemma, that is when $c - 1 \leq b \leq p$ and $1 \leq m \leq \min\{\nu - 1, b - c\}$. Note that actually $b \geq c$ in this case. We prove that there exists at least one $l \in [m,\ \min\{\nu - 1, b - c\}]$ such that

$d_l \not\equiv 0 \pmod{p}$. By Lemma 3.4 of [31], we have

$$\begin{aligned}(3.6)\quad &\binom{r-l}{b-m+j(p-1)}\\ &\equiv \binom{b-c-l}{b-m-j}\binom{c}{j} \quad \text{if } 0\le l\le b-c \text{ and } 0\le j\le c-1 \text{ (as } c\le b-m)\\ &\equiv 0 \quad \text{if } m\le l\le b-c \text{ and } 0\le j\le c-1.\end{aligned}$$

Therefore, $\sigma_1(l)=1$ for all $m\le l\le \min\{\nu-1, b-c\}$. Using Lemma 3.5 of [31], we get

$$(3.7)\quad \frac{\binom{r-l}{b-m+j(p-1)}}{p} \equiv \frac{(-1)^{l-m}\binom{b-m}{j}\binom{p-1+m-l}{c-1-j}}{\binom{b-m-c}{l-m}\binom{b-m}{c}}$$
$$\text{if } 0\le j\le c-1 \text{ and } m\le l\le \min\{\nu-1, b-c\}.$$

Next, observe that $\epsilon_1 = 0$ as $b \ge m+c \ge 2m+1+\epsilon$. Hence, for $m\le l\le \min\{\nu-1, b-c\}$ we have

$$d_l \equiv (-1)^l \sum_{0\le j\le c-m-1} \frac{\binom{b-m}{j}\binom{p-1+m-l}{c-1-j}\binom{c-1-j}{m}}{\binom{b-m-c}{l-m}\binom{b-m}{c}}.$$

Note that

$$(3.8)\quad \binom{p-1+m-l}{c-1-j}\binom{c-1-j}{m} = \binom{p-1+m-l}{m}\binom{p-1-l}{c-m-1-j}.$$

Therefore, we have

$$(3.9)\qquad d_l \equiv \frac{(-1)^l\binom{p-1+l-m}{m}}{\binom{b-m-c}{l-m}\binom{b-m}{c}} \sum_{0\le j\le c-m-1} \binom{b-m}{j}\binom{p-1-l}{c-m-1-j}.$$

By applying Vandermonde's identity, we get

$$d_l \equiv \frac{(-1)^l\binom{p-1+m-l}{m}\binom{p+b-(m+1+l)}{c-m-1}}{\binom{b-m-c}{l-m}\binom{b-m}{c}}.$$

By taking $l=m$, we get

$$\begin{aligned} d_m &\equiv \frac{(-1)^m\binom{p-1}{m}\binom{p+b-(2m+1)}{c-m-1}}{\binom{b-m}{c}}\\ &\equiv \frac{(-1)^m\binom{p-1}{m}\binom{b-(2m+1)}{c-m-1}}{\binom{b-m}{c}} \quad (\text{as } b\ge 2m+1).\end{aligned}$$

Hence, we get $d_m \not\equiv 0 \bmod p$ as $b-2m-1-(c-m-1) = b-c-m \ge 0$ and $b-(2m+1)\le p-1$. □

The following identities will only be required in Section 8, where we prove more cases of Conjecture 5.1.

Lemma 3.5. *Let $2 \leq b \leq p$, $0 \leq c \leq p-1$ and $1 \leq m \leq c-1$. For $\max\{1, b-c+2\} \leq i \leq m+1$ and $\max\{0, b-c+1\} \leq l \leq \min\{m, p+b-c\}$*

$$\alpha'(i,l) \equiv u_l v_i \sum_{\epsilon_1 \leq k \leq c_1} (-1)^k (c-k) \binom{c-m-1+i}{k} \cdot \binom{i+c-m-2-k}{i-(b-c+2)} \binom{l+c-m-1-k}{l},$$

where $\alpha'(i,l)$ defined in (3.3), $c_1 = \min\{c-m-1, b-m\}$, $u_l = (-1)^l l!(p+b-c-l)!(c-1)!$ and

$$v_i = \frac{(-1)^{i+1+c-m}(i-(b-c+2))!}{(i-1)!(m+1-i)!(c-m-1+i)!}.$$

Proof. We refer to Lemma A.2 for the proof. □

Following similar steps as in the proof of Lemma 3.5, we obtain the following lemma.

Lemma 3.6. *Let $2 \leq b \leq p$, $0 \leq c \leq p-1$ and $1 \leq m \leq c-2$. For $p+b-c+2 \leq i \leq m+1$ and $p+b-c+1 \leq l \leq \min\{m, 2p+b-c\}$*

$$\alpha'(i,l) \equiv u_l v_i \sum_{\epsilon_1 - 1 \leq k \leq c_1} (-1)^k (c-1-k) \binom{c-m-2+i}{k} \cdot \binom{i+c-m-3-k}{i-(p+b-c+2)} \binom{l+c-m-2-k}{l},$$

where $\alpha'(i,l)$ defined in (3.3), $c_1 = c-m-2$, $u_l = (-1)^l l!(2p+b-c-l)!(c-2)!$ and

$$v_i = \frac{(-1)^{i+c-m}(i-(p+b-c+2))!}{(i-1)!(m+1-i)!(c-m-2+i)!}.$$

Lemma 3.7. *Let $b, i \in \mathbb{N}$ and suppose $c, l \in \mathbb{Z}_{\geq 0}$ such that $l \geq b-c+1$ and $i \geq b-c+2$. Also assume that $1 \leq m \leq c-1$ and $b \geq m$. Then*

$$\sum_{0 \leq k \leq c-m-1} (-1)^k (c-k) \binom{c-m-1+i}{k} \cdot \binom{c-m-2+i-k}{i-(b-c+2)} \binom{l+c-m-1-k}{l} = \begin{cases} C_1 + C_2 & \text{if } i \leq l \\ C_1 + C_2 + (-1)^{b-m+l}(m+1-i)\binom{i-1}{l} & \text{if } l \leq i-1. \end{cases}$$

where

$$C_1 = \sum_{0\le j\le m_1} (-1)^j c \binom{c-m-1+i}{i-(b-c+2+j)} \binom{l-(b-c+2+j)}{l-(b-m+1+j)}$$

$$C_2 = \sum_{0\le j\le m_2} (-1)^j (b-m+1+j) \binom{c-m-1+i}{i-(b-c+2+j)} \binom{l-(b-c+2+j)}{l-(b-m+j)}$$

where

$$m_1 = \min\{i-(b-c+2), l-(b-m+1)\}$$
$$\text{and} \quad m_2 = \min\{i-(b-c+2), l-(b-m)\}.$$

Further, $C_1 = 0$ *if* $l \le b-m$ *and* $C_2 = 0$ *if* $l \le b-m-1$.

Proof. We obtain the lemma from Lemma A.3, where we put $n = b-c+1$. □

Remark 3.8. If $b \ge 2m+1$ and $l \le m$, then the above lemma gives $C_1 = 0 = C_2$.

Lemma 3.9. *Let* $b, i \in \mathbb{N}$ *and suppose* $c, l \in \mathbb{Z}_{\ge 0}$ *such that* $l \ge p+b-c+1$ *and* $i \ge p+b-c+2$. *Also, assume that* $1 \le m \le c-2$ *and* $p+b-m-1 \ge 0$. *Then*

$$\sum_{0\le k\le c-m-2} (-1)^k (c-1-k) \binom{c-m-2+i}{k} \cdot \binom{i+c-m-3-k}{i-(p+b-c+2)} \binom{l+c-m-2-k}{l}$$
$$= \begin{cases} C_1 + C_2 & \text{if } l \ge i \\ C_1 + C_2 + (-1)^{p+b-m+1+l}(m+1-i)\binom{i-1}{l} & \text{if } l \le i-1. \end{cases}$$

where

$$C_1 = \sum_{0\le j\le m_1} (-1)^j (p+b-m+j) \binom{c-m-2+i}{i-(p+b-c+2+j)} \cdot \binom{l-(p+b-c+2+j)}{l-(p+b-m-1+j)},$$

$$C_2 = \sum_{0\le j\le m_2} (-1)^j (c-1) \binom{c-m-2+i}{i-(p+b-c+2+j)} \binom{l-(p+b-c+2+j)}{l-(p+b-m+j)}$$

and

$$m_1 = \min\{i-(p+b-c+2), l-(p+b-m-1)\}$$
$$\text{and} \quad m_2 = \min\{i-(p+b-c+2), l-(p+b-m)\}.$$

Further, $C_1 = 0$ *if* $l \le p+b-m-2$ *and* $C_2 = 0$ *if* $l \le p+b-m-1$.

Proof. The lemma follows from Lemma A.3 where we first replace c with $c-1$ and then put $n = p+b-c+1$ (in this order). Next, we observe that C_1 and C_2 of Lemma A.3 are C_2 and C_1 respectively of the lemma above. □

Remark 3.10. If $b \geq 2(m+1) - p$ and $l \leq m$ then above lemma gives $C_1 = 0 = C_2$.

4. Determination of monomials in Ker(P)

Lemma 4.1. *Let $r, b, c, m \in \mathbb{Z}_{\geq 0}$ such that $2 \leq b \leq p$ and $r \equiv b \bmod (p-1)$. Assume that $r \geq b + c(p-1) + 1$. If $0 \leq m \leq \min\{c-1-\epsilon_1, p-1\}$, then for all $1 \leq a \leq c-m-\epsilon_1$,*

$$q(c-m-a) \equiv \sum_{1 \leq i \leq m+1} (-1)^{i+1} \beta(a,i) q(c-m-1+i) \bmod (V_r^{(m+1)}).$$

Proof. Let $P_j = x^{r-(b+1)-(c-j+1)(p-1)} y^{b-2m-1+(c-m-j)(p-1)}$ for all $1 \leq j \leq c-m-\epsilon_1$, and recall $q(i) = x^{r-b+m-i(p-1)} y^{b-m+i(p-1)}$ for all $n_0 \leq i \leq c$, where $n_0 = 0$ if $b \geq m$ and 1 otherwise. Indeed $P_j \in V_{r-(m+1)(p+1)}$ as $b-2m-1+(c-m-j)(p-1) \geq b-(2m+1)+\epsilon_1(p-1) \geq 0$. Observe that

$$\theta^{m+1} P_j = \sum_{0 \leq i \leq m+1} (-1)^i \binom{m+1}{i} q(c-m-j+i). \tag{4.1}$$

We will prove the result by induction on a. Observe that for $a = 1$, the result is true, and can be seen by putting $j = 1$ in (4.1) as follows

$$\sum_{0 \leq i \leq m+1} (-1)^i \binom{m+1}{i} q(c-m-1+i) \equiv 0 \bmod (V_r^{(m+1)})$$

$$\implies q(c-m-1) \equiv \sum_{1 \leq i \leq m+1} (-1)^{i+1} \binom{m+1}{i} q(c-m-1+i) \bmod (V_r^{(m+1)}).$$

By induction step, assume the result is true for $1 \leq a \leq k-1$, and we prove it for $a = k \leq c-m-\epsilon_1$. By putting $j = k$ in (4.1) we have

$$\sum_{0 \leq i \leq m+1} (-1)^i \binom{m+1}{i} q(c-m-k+i) \equiv 0 \bmod (V_r^{(m+1)})$$

$$\implies q(c-m-k) \equiv \sum_{1 \leq i \leq k-1} (-1)^{i+1} \binom{m+1}{i} q(c-m-k+i) + \sum_{k \leq i \leq m+1} (-1)^{i+1} \binom{m+1}{i} q(c-m-k+i).$$

We note that if $k > m+1$, then the second sum above is zero and in the first sum i runs from 1 to $m+1$ as $\binom{m+1}{i} = 0$ for all $m+1 < i \leq k-1$.

We rename i by l in the first sum and replace $i-(k-1)$ by i in the second sum. Thus, we get

$$q(c-m-k) \equiv \sum_{1\le l\le k-1} (-1)^{l+1}\binom{m+1}{l} q(c-m-k+l) + \sum_{1\le i\le m+1-(k-1)} (-1)^{i+k}\binom{m+1}{i+k-1} q(c-m-1+i).$$

Observe that the second sum can be taken over $1 \le i \le m+1$ as $\binom{m+1}{i+k-1} = 0$ for all $i > m+1-(k-1)$. By induction, we have

$$\begin{aligned} & q(c-m-k) \\ & \equiv \sum_{1\le l\le k-1} (-1)^{l+1}\binom{m+1}{l}\left(\sum_{1\le i\le m+1} (-1)^{i+1}\beta(k-l,i) q(c-m-1+i)\right) \\ & \qquad + \sum_{1\le i\le m+1} (-1)^{i+k}\binom{m+1}{i+k-1} q(c-m-1+i) \end{aligned}$$

Now, we interchange the sums in the first sum and then combine them with the last sum, we get

$$q(c-m-a) \equiv \sum_{1\le i\le m+1} (-1)^{i+1}\beta(k,i) q(c-m-1+i)$$

where $\beta(k,i)$ is defined in Lemma 3.1. □

Corollary 4.2. *Let $r, b, c, m \in \mathbb{Z}_{\ge 0}$ such that $2 \le b \le p$ and $r \equiv b \bmod (p-1)$. Assume that $r \ge b + c(p-1) + 1$. Suppose $1 \le m \le \min\{c-1-\epsilon_1, p-1\}$, and $q(j) \in V_r^{(m+1)} + \mathrm{Ker}(P)$ for all $c-m \le j \le c-1$. Then for all $\epsilon_1 \le j \le c-m-1$,*

$$q(j) \equiv (-1)^m \binom{c-1-j}{m} q(c) (\bmod (\mathrm{Ker}(P) + V_r^{(m+1)})).$$

Proposition 4.3. *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and suppose also that $2 \le b \le p$, $1 \le c \le p-1$. Fix non zero slope $\nu(a_p)$ such that $0 \le m \le \nu(a_p) < p-1$, $(m,\nu) \ne (\nu, \nu(a_p))$, and also $s > 2\nu(a_p)$. Further we assume $t > \nu(a_p) + c - 1$ if $(b,c,m) \ne (p,1,0)$ and $t > \nu(a_p) + c$ if $(b,c,m) = (p,1,0)$. Then for all $g \in G$ and for $0 \le l \le \nu$ with $(l,\nu) \ne (\nu, \nu(a_p))$, there exists $f^l \in \mathrm{ind}_{KZ}^G\left(\mathrm{Sym}^r(\overline{\mathbb{Q}}_p^2)\right)$ such that*

$$(T - a_p) f^l \equiv \left[g, \sum_{\substack{0<j<s-m \\ j \equiv (s-m) \bmod (p-1)}} \binom{r-l}{j} x^{r-j} y^j \right]. \tag{4.2}$$

Further assume $(b,c,m) \neq (p,1,0)$, $t > \nu(a_p) + c$ *and* $0 \leq l, m \leq \nu - 1$. *If* $m = 0$, *then assume* l *further satisfies* $\nu\Big(\binom{r-l}{p-1-l}\Big) \geq 1$. *If* $l = \nu - 1$ *or* $m = \nu - 1$, *then assume* $\nu < \nu(a_p)$. *For all* $g \in G$ *and the above values of* l, m *there exists* $f^l \in \mathrm{ind}_{KZ}^G\Big(\mathrm{Sym}^r(\overline{\mathbb{Q}}_p^2)\Big)$ *such that*

$$(T - a_p)\left(\frac{f^l}{p}\right) \equiv \left[g, \sum_{\substack{0<j<s-m \\ j \equiv (s-m) \bmod (p-1)}} \frac{\binom{r-l}{j}}{p} x^{r-j}y^j\right]. \tag{4.3}$$

Proof. The proof is along similar lines to that of Proposition 4.1 of [31]. □

Proposition 4.4. *Let* $r = s + p^t(p-1)d$, *with* $p \nmid d$, $s = b + c(p-1)$ *and also suppose that* $2 \leq b \leq p$, $1 \leq c \leq p-1$. *Fix* a_p *such that* $1 < \nu(a_p) < p-1$ *and* $s > 2\nu(a_p)$. *Assume* $1 \leq m \leq \min\{\nu, c - 1 - \epsilon_1\}$ *and* $(m,\nu) \neq (\nu, \nu(a_p))$. *If* $t > \nu(a_p) + c - 1$, *then for all* $g \in G$ *and for* $0 \leq l \leq \nu$ *with* $(l,\nu) \neq (\nu, \nu(a_p))$, *there exists* $f^l \in \mathrm{ind}_{KZ}^G\Big(\mathrm{Sym}^r(\overline{\mathbb{Q}}_p^2)\Big)$ *such that*

$$(T - a_p)f^l \equiv \left[g, \sum_{1 \leq i \leq m+1} \alpha(i,l) q(i + c - m - 1)\right] \pmod{X} \tag{4.4}$$

where $\alpha(i,l)$ *is as in* (3.1) *and* $X := V_r^{(m+1)} + \mathrm{Ker}(P)$. *Further, suppose* $1 \leq m \leq \min\{\nu - 1, c - 1 - \epsilon_1\}$, $0 \leq l \leq \nu - 1$, *and* $t > \nu(a_p) + c$. *Assume* $\nu < \nu(a_p)$ *if* $l = \nu - 1$ *or* $m = \nu - 1$. *If for some* l *as above* $\binom{r-l}{b-m+j(p-1)} \equiv 0 \bmod p$ *for* $0 \leq j \leq c-1$ *such that* $b - m + j(p-1) > 0$, *then for all* $g \in G$ *there exists* $f^l \in \mathrm{ind}_{KZ}^G\Big(\mathrm{Sym}^r(\overline{\mathbb{Q}}_p^2)\Big)$ *such that*

$$(T - a_p)\left(\frac{f^l}{p}\right) \equiv \left[g, \sum_{1 \leq i \leq m+1} \frac{\alpha(i,l)}{p} q(i + c - m - 1)\right] \pmod{X}. \tag{4.5}$$

Proof. First, we note that

$$\begin{aligned} A &:= \sum_{\substack{0<j<s-m \\ j \equiv (s-m) \bmod (p-1)}} \binom{r-l}{j} x^{r-j}y^j \\ &= \sum_{\substack{0 \leq j' \leq c-1 \\ b-m+j'(p-1) > 0}} \binom{r-l}{b-m+j'(p-1)} q(j'). \end{aligned}$$

Now, we write the last sum into three parts: $0 \leq j < \epsilon_1$, $\epsilon_1 \leq j' \leq c-m-1$, and $c - m \leq j' \leq c-1$. Here we note that Remark 4.4 of [19] gives the first sum belongs to $\mathrm{Ker}(P)$ as $m < \nu(a_p)$. In the second range of sum, we put

$a = c - m - j'$ and in the third range of sum we put $i' = j' - (c - m - 1)$. Therefore, we have

$$A \equiv \sum_{1 \le a \le c-m-\epsilon_1} \binom{r-l}{b-m+(c-m-a)(p-1)} q(c-m-a) + \sum_{1 \le i' \le m} \binom{r-l}{b-m+(c-m-1+i')(p-1)} q(c-m-1+i') \mod (\mathrm{Ker}(P)).$$

By Lemma 4.1, for $1 \le a \le c - m - \epsilon_1$ we have

$$q(c-m-a) \equiv \sum_{1 \le i \le m+1} (-1)^{i+1} \beta(a,i) q(c-m-1+i) \mod (V_r^{(m+1)}).$$

Therefore, we get

$$A \equiv \sum_{1 \le i' \le m} \binom{r-l}{b-m+(c-m-1+i')(p-1)} q(c-m-1+i') + \sum_{1 \le a \le c-m-\epsilon_1} \binom{r-l}{b-m+(c-m-a)(p-1)} \cdot \left(\sum_{1 \le i \le m+1} (-1)^{i+1} \beta(a,i) q(c-m-1+i) \right).$$

The above congruence is over $\mod (V_r^{(m+1)} + \mathrm{Ker}(P))$. Now, we interchange the sums in the last sum and combine them with the first sum (replace i' by i); we get

$$A \equiv \sum_{1 \le i \le m+1} \alpha(i,l) q(c-m-1+i) \mod (V_r^{m+1} + \mathrm{Ker}(P))$$

where $\alpha(i,l)$ is as in (3.1). Hence, we obtained the first part of our result just by using Proposition 4.2. For the second part, we rerun the proof with

$$A := \sum_{\substack{0 < j < s-m \\ j \equiv (s-m) \bmod (p-1)}} \frac{\binom{r-l}{j}}{p} x^{r-j} y^j$$

by noting that $\frac{\binom{r-l}{j}}{p}$ is integral. □

Proposition 4.5. *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and also suppose that $2 \le b \le p$, $1 \le c \le p-1$. Fix a_p such that $\nu(a_p)$ is non-integral, $s > 2\nu(a_p)$, and let $1 \le m \le \nu \le c - 1 - \epsilon$. Also assume $t > \nu(a_p) + c$, and $q(j) \in (V_r^{(m+1)} + \mathrm{Ker}(P)$ for all $c - m \le j \le c - 1$.*

Then $F_m(x,y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ *in each of the following cases (with the additional conditions on* m *given below):*

(1) $1 \le m \le \min\{\nu - 1, b - c\}$ *if* $c - 1 \le b \le p$.
(2) $b - \nu \le m \le \nu$ *if* $c - 1 \le b \le p$.
(3) $m \in ([b-\nu, \nu] \cap [1, b-1]) \cup [b, \nu - 1]$ *if* $2 \le b \le c-2$ *and* $1 \le \nu \le \min\{c-2, p+b-c\}$.
(4) $m \in [1, p+b-c] \cup [p+b-\nu-1, \nu]$ *if* $2 \le b \le 2(c-1) - p - 2$ *and* $p + b - c + 1 \le \nu \le c - 3$.

Remark 4.6.

(1) We note that the hypothesis $q(j) \in (V_r^{(m+1)} + \mathrm{Ker}(P)$ for all $c - m \le j \le c - 1$ (see Conjecture 5.2) in Proposition 4.5 is crucial for applying Corollary 4.2.
(2) The statement (3) of the proposition above is obtained by combining (3) and (4) of Lemma 3.3.
(3) Corollary 4.2 is applicable since $c - 1 - \epsilon \le c - 1 - \epsilon_1$ if $1 \le m \le c - 1 - \epsilon$.

Proof. Recall the definition of $\sigma_1(l)$ from (3.4) and observe that $\frac{\binom{r-l}{b-m+j(p-1)}}{p^{\sigma_1(l)}}$ is integral. By Remark 4.4 of [19], we have $q(j) \in \mathrm{Ker}(P)$ for all $j \in [0, \epsilon_1 - 1]$ such that $b - m + j(p-1) > 0$. Therefore, for each $l \in [0, \nu - \sigma_1(l)]$, Proposition 4.3 gives

$$(T - a_p)\left(\frac{f^l}{p^{\sigma_1(l)}}\right) \equiv \left[g, \sum_{\epsilon_1 \le j \le c-m-1} \frac{\binom{r-l}{b-m+j(p-1)}}{p^{\sigma_1(l)}} q(j)\right] \mod (V_r^{(m+1)} + \mathrm{Ker}(P))$$

as $q(j) \in (V_r^{(m+1)} + \mathrm{Ker}(P)$ for all $j \in [c-m, c-1]$ (by the hypothesis). Since $\nu(a_p)$ is non-integral, we can also apply Proposition 4.3 in the case when $l = \nu$ in (4.2) or when $l, m = \nu - 1$ in (4.3). By Corollary 4.2, we have

$$(T - a_p)\left(\frac{f^l}{p^{\sigma_1(l)}}\right) \equiv [g,\ d_l\ q(c)] \bmod (\mathrm{Ker}(P) + V_r^{(m+1)}),$$

where d_l is as in (3.5). For each b, c, ν and m as in the statement, Lemma 3.3 gives that there exists at least one $l \in [0, \nu - \sigma_1(l)]$ such that $d_l \not\equiv 0 \bmod p$. Hence, we get $q(c) \in (\mathrm{Ker}(P) + V_r^{(m+1)})$. Further, note that Remark 4.4 of [19] gives $x^m y^{r-m} \in \mathrm{Ker}(P)$ as $m < \nu(a_p)$. Consequently, $F_m(x,y) \equiv q(c) \bmod (\mathrm{Ker}(P) + V_r^{(m+1)})$, thereby giving our proposition. □

5. Conjecture

We consider the following matrix

$$A = (\alpha(i,l))_{\substack{1\le i\le m+1,\\ 0\le l\le m}} \tag{5.1}$$

where $\alpha(i,l)$ are defined in (3.1). We note that $\alpha(i,l)$ has a complicated formula, so proving that the linear system of equations $AX = e_i \pmod p$ has a solution is generally hard. However, we make the following conjecture about the solutions to the above linear systems based on SageMath programs.

Conjecture 5.1 (Matrix form)**.** *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and suppose that $2 \le b \le p$, $1 \le c \le p-1$, and $t \ge 2$. Suppose also that $1 \le m \le c-1-\epsilon$. Then the linear systems $AX = e_i \pmod p$ has a solution for all $1 \le i \le m$.*

We note that if $AX = e_{i'} \pmod p$ has a solution, then under the hypotheses of Proposition 4.4, we get $q(c-m-1+i') \in (V_r^{(m+1)} + \mathrm{Ker}(P))$. One can see this as follows, if $X^t = (d_0, d_1, \ldots, d_m) \in \mathbb{Z}_p^{m+1}$ is a solution of $AX = e_{i'} \pmod p$, then take $f := \sum_{0\le l\le m} d_l f^l$, where f^l are defined in Proposition 4.4. Observe that

$$\begin{aligned}
&(T-a_p)f \\
&\equiv \left[g, \sum_{1\le i\le m+1}\left(\sum_{0\le l\le m} d_l\alpha(i,l)\right)q(c-m-1+i)\right] \bmod (V_r^{(m+1)} + \mathrm{Ker}(P)) \\
&\equiv \left[g,\ q(c-m-1+i')\right] \bmod (V_r^{(m+1)} + \mathrm{Ker}(P)).
\end{aligned}$$

Therefore, as a consequence of the above conjecture, we get the following conjecture for monomials $q(j)$.

Conjecture 5.2 (Monomial form)**.** *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and suppose that $2 \le b \le p$, $1 \le c \le p-1$. Fix a_p such that $1 < \nu(a_p) < p-1$ and $t > \nu(a_p) + c$. Suppose also that $s > 2\nu(a_p)$. Further we assume that $1 \le m \le \min\{\nu, c-1-\epsilon\}$ and $(m,\nu) \ne (\nu, \nu(a_p))$. Then the monomials $q(j) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $c-m \le j \le c-1$.*

Remark 5.3. Note that the crucial hypothesis in Proposition 4.5 on $q(j)$ is precisely the claim of Conjecture 5.2.

In the following lemma, we prove enough cases of Conjecture 5.1 so that Proposition 4.5(1) holds unconditionally. In the last section, we discuss evidence for the remaining cases (and also provide proof in many cases) of Conjecture 5.1.

Lemma 5.4. *If $c-1 \le b \le p$ and $1 \le m \le \min\{b-c, c-1-\epsilon\}$, then Conjecture 5.1 is true.*

Proof. First, we note that the range of m is non-empty only when $b \geq c+1$, so we will prove our lemma only for $b \geq c+1$. Now, let's express A in (5.1) as follows

$$A = \begin{pmatrix} A' & B' \\ A'' & B'' \end{pmatrix}, \tag{5.2}$$

where the ranges of i and l are divided into non-empty intervals $[1, m], [m+1, m+1]$ and $[0, m-1]$, $[m, m]$, determining the order of the blocks. For $0 \leq l \leq m$ and $1 \leq i \leq m+1$, Lemma 3.2 gives $\alpha_1(i,l) \equiv 0 \bmod p$ (as $m \leq b-c$), and also that the additional term of $\alpha(i,l)$ (for $i \leq m$) is given by

$$\begin{aligned} X(i,l) &= \begin{pmatrix} r-l \\ b-m+(i+c-m-1)(p-1) \end{pmatrix} \\ &\equiv \begin{pmatrix} b-c-l \\ b-c+1-i \end{pmatrix} \begin{pmatrix} c \\ i+c-m-1 \end{pmatrix}. \end{aligned}$$

Hence, we get

$$\alpha(i,l) \equiv \begin{cases} \binom{b-c-l}{b-c+1-i}\binom{c}{c-m-1+i} & \text{if } 0 \leq l \leq m, 1 \leq i \leq m \\ 0 & \text{if } 0 \leq l \leq m, i = m+1. \end{cases}$$

The above congruence implies that modulo p, A' is an invertible lower triangular matrix (with all the diagonal entries non-zero modulo p, given by $i = l+1$), and A'', B'' are zero modulo p. Hence, for every $1 \leq i \leq m$, modulo p the row rank of $[A : e_{i'}]$ is same as the row rank of A. Thus, the linear systems $AX \equiv e_{i'} \pmod p$ has a solution for all $1 \leq i' \leq m$. □

6. Elimination of JH factor

Proposition 6.1. *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and suppose also that $2 \leq b \leq p$, $2 \leq c \leq p-1$. Fix a_p such that $\nu(a_p)$ is non-integral, $1 < \nu(a_p) < c - \epsilon$ and $t > \nu(a_p) + c$. Further, assume Conjecture 5.2 is true. Then the map P surjects from $\operatorname{ind}_{KZ}^{G}\left(\frac{V_r^{(n_1+1)}}{V_r^{(n_2)}}\right)$, where n_1 and n_2 are defined as follows:*

1. *If $c-1 \leq b \leq p$, then $n_1 = \min\{b-c, \nu-1\}$ and $n_2 = \min\{b-\nu, \nu+1\}$.*
2. *Suppose $2 \leq b \leq c-2$ and $1 \leq \nu \leq \min\{c-2, p+b-c\}$. Then*

$$n_1 = \begin{cases} \nu - 1 & \text{if } b \leq \nu \\ -1 & \text{otherwise} \end{cases} \quad \text{and} \quad n_2 = \begin{cases} \nu + 1 & \text{if } b \leq \nu \\ \min\{b-\nu,\ \nu+1\} & \text{otherwise.} \end{cases}$$

3. *If $2 \leq b \leq 2c-4-p$ and $p+b-c+1 \leq \nu \leq c-3$, then $n_1 = p+b-c$ and $n_2 = \min\{p+b-\nu-1,\ \nu+1\}$.*

Remark 6.2. In the proposition above, Conjecture 5.2 is needed to apply Proposition 4.5. Note that the statement (1) above is obtained by combining the statements (1) and (2) of Proposition 4.5. If $b \geq c + \nu - 1$, then the range of m in Proposition 4.5 (2) is empty. Therefore, the case $b \geq c+\nu-1$ (appearing later) is covered entirely by the statement of Proposition 4.5 (1).

Proof. In all three parts of the proposition, we need to show that the map P factors through $\mathrm{ind}_{KZ}^{G}\Big(\frac{V_r^{(n_1+1)}}{V_r^{(n_2)}}\Big)$. In order to do that we apply Lemmas 2.1 and 2.2 to the intervals $[0, n_1]$ and $[n_2, \nu]$ respectively, whenever they are non-empty. To apply Lemma 2.2 in each cases, we show that $F_m(x, y) \in \mathrm{Ker}(P)$ for all $m \in [n_2, \nu]$. In fact, it suffices to show that $F_m(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $m \in [n_2, \nu]$. We show this by reverse induction on m after observing that $F_\nu(x, y) \in \mathrm{Ker}(P)$ because $F_\nu(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ and $\mathrm{ind}_{KZ}^{G}(V_r^{(\nu+1)}) \subset \mathrm{Ker}(P)$.

Next, we explain the steps to apply Lemma 2.1 for $[0, n_1]$. If $F_m(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for $m \geq 1$, then there exists $v_{m+1} \in V_r^{(m+1)}$ such that $F_m(x, y) - v_{m+1} \in \mathrm{Ker}(P)$. Let W_m be the submodule of $V_r^{(m)}$ generated by $F_m(x, y) - v_{m+1}$. By using Lemma 2.4, and given that $F_m(x, y) - v_{m+1} \in \mathrm{Ker}(P)$, we observe that W_m satisfies the required conditions of Lemma 2.1. Hence, to apply Lemma 2.1 for $[0, n_1]$, we show that $F_m(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $m \in [1, n_1]$ and construct the required W_0 separately. In each of the above cases, Proposition 4.5 gives $F_m(x, y) \in (V_r^{(m+1)} + \mathrm{Ker}(P))$ for all $m \in [1, n_1] \cup [n_2, \nu]$. Therefore, to complete the proof, we construct W_0 in Lemma 6.3 for cases (1) and (3) above, and only for $b \leq \nu$ in case (2) ($m = 0$ is not applicable when $b \geq \nu + 1$). □

Lemma 6.3. *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and suppose also that $2 \leq b \leq p$, $2 \leq c \leq p-1$. Fix a_p such that $\nu(a_p)$ is non-integral, $1 < \nu(a_p) < c - \epsilon$ and $t > \nu(a_p) + c$. Then the submodule W_0 of V_r generated by $x^{r-b}y^b$, x^r if $b \neq p$, and generated by $x^{r-1}y$, x^r if $b = p$ satisfy the condition of Lemma 2.1 in the following cases:*

(1) $c - 1 \leq b \leq p$.
(2) $2 \leq b \leq \min\{c-2, \nu\}$ *and* $1 \leq \nu \leq \min\{c-2, p+b-c\}$.
(3) $2 \leq b \leq 2c-4-p$ *and* $p+b-c+1 \leq \nu \leq c-3$.

Proof. We refer to Lemma A.5 for the proof. □

Theorem 6.4. *Let $r = s + p^t(p-1)d$, with $p \nmid d$, $s = b + c(p-1)$ and suppose also that $2 \leq b \leq p$, $2 \leq c \leq p-1$. Fix a_p such that $\nu(a_p)$ is non-integral, $1 < \nu(a_p) < c - \epsilon$ and $t > \nu(a_p) + c$. Assume Conjecture 5.2 is true. Then the map P surjects from $\mathrm{ind}_{KZ}^{G}\Big(\frac{V_r^{(n_0)}}{V_r^{(n_0+1)}}\Big)$, where n_0 is defined as follows:*

(1) *If* $b \geq c+\nu-1$, *then* $n_0 = \nu$.
(2) *If* $c-1 \leq b \leq c+\nu-2$ *and* $\nu = c-2$, *then* $n_0 = b-c+1$.
(3) *Suppose* $2 \leq b \leq c-2$ *and* $1 \leq \nu \leq \min\{c-2, p+b-c\}$. *Then* $n_0 = \nu$ *if* $b \leq \nu$ *and* $n_0 = 0$ *if* $b = \nu+1$.
(4) *If* $2 \leq b \leq 2c-4-p$ *and* $\nu \in \{p+b-c+1, c-3\}$, *then* $n_0 = p+b-c+1$.

7. Main theorem

In the following proposition, we determine $\overline{V}_{k',a_p}$ for all $k' > k$, where $k' = r+2$, $k = s+2$ and r, s are as given in the statement below. We apply Lemma 2.5 in the proposition below to consider only those b, c, ν where the reduction is necessarily irreducible. In particular, we have removed the point $b = 2c-4-p$ coming from Theorem 6.4 (3) since it is a case with possibly reducible reduction $\overline{V}_{k',a_p}$.

Proposition 7.1. *Let* $p \geq 5$. *Let* $r = s+p^t(p-1)d$, *with* $p \nmid d$, $s = b+c(p-1)$ *and suppose also that* $2 \leq b \leq p$, $2 \leq c \leq p-1$. *Fix* a_p *such that* $\nu(a_p)$ *is non-integral,* $1 < \nu(a_p) < c-\epsilon$ *and* $t > \nu(a_p)+c$. *Assume Conjecture 5.2 is true and let* $k' = r+2$.

(1) *If* $b \geq c+\nu-1$ *such that* $b \neq 2\nu+1$ *and* $(b,\nu) \neq (p,1)$, *then*
$$\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+\nu(p-1)}\Big).$$
(2) *If* $c-1 \leq b \leq c+\nu-2$ *and* $\nu = c-2$, *then*
$$\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+(b-c+1)(p-1)}\Big).$$
(3) *Suppose* $2 \leq b \leq c-2$ *and* $1 \leq \nu \leq \min\{c-2, p+b-c\}$. *Also assume that* $b \neq 2\nu+2-p$ *if* $b \leq 2c-2-p$. *Then*
$$\overline{V}_{k',a_p} \cong \begin{cases} \mathrm{ind}\Big(\omega_2^{b+1+(\nu+1)(p-1)}\Big) & \text{if } b \leq \nu \\ \mathrm{ind}\Big(\omega_2^{b+1}\Big) & \text{if } b = \nu+1. \end{cases}$$
(4) *If* $2 \leq b \leq 2c-5-p$ *and* $\nu \in \{p+b-c+1, c-3\}$, *then*
$$\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{k_0}\Big),$$
where $k_0 = b+1+(p+b-c+2)(p-1)$.

Proof. We prove the corollary in the following parts.

Case (1): $c+\nu-1 \leq b \leq p$. By Theorem 6.4, we have
$$P : \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(\nu)}}{V_r^{(\nu+1)}}\right) \longrightarrow\!\!\!\!\!\rightarrow \overline{\Theta}_{k',a_p}.$$
Observe that $b \geq 2\nu$ as by assumption $b \geq \nu+c-1$, and $\nu \leq c-1$. We also observe that the equality $b = 2\nu$ occurs only for $\nu = c-1$. But $b = 2c-2$ gives $\epsilon = 1$, and so we must have by hypothesis that $\nu \leq c-2$. Thus, as

such we must have $b \geq 2\nu + 1$. Therefore, if $b \neq 2\nu + 1$ and $(b, \nu) \neq (p, 1)$, then by Lemma 2.5 (with $n = \nu$), we have

$$\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+\nu(p-1)}\Big) \text{ as } 2\nu + 2 \leq b \leq p.$$

Case (2): $c - 1 \leq b \leq c + \nu - 2$ and $\nu = c - 2$ (so $b \leq 2c - 4$). By Theorem 6.4, we have

$$P : \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(b-c+1)}}{V_r^{(b-c+2)}}\right) \twoheadrightarrow \overline{\Theta}_{k',a_p}.$$

Subcase (i): $b = c - 1$. If $b \neq p - 2$, then Lemma 2.5 (with $n = 0$) gives $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1}\Big)$. If $b = p - 2$, then by (2.3) (with $n = 0$ and $r' = 2p - 3$), we see that the image of $\mathrm{ind}_{KZ}^{G}(V_{p-2})$ in $\mathrm{ind}_{KZ}^{G}\Big(\frac{V_r}{V_r^{(1)}}\Big)$ is generated by $[1,\ x^r]$ and the latter belongs to $\mathrm{Ker}(P)$ by Remark 4.4 of [19]. Hence, P factors through $\mathrm{ind}_{KZ}^{G}\big(V_1 \otimes D^{p-2}\big)$. Therefore, Proposition 3.3 of [19] gives $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{2+(p-2)(p+1)}\Big)$. We conclude by observing that $\omega_2^{2+(p-2)(p+1)}$ is conjugate to ω_2^{b+1} as $b = p - 2$ and $2 + (p - 2)(p + 1) = p(b + 1)$.

Subcase (ii): $c \leq b \leq 2c - 4$. In this case, we note that $b \geq 2n + 2$ with $n = b - c + 1$ as $b \leq 2c - 4$, and also note that $(b, n) \neq (p, 1)$ as $c \leq p - 1$. Hence, Lemma 2.5 (with $n = b - c + 1$) gives $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+(b-c+1)(p-1)}\Big)$.

Case (3): $2 \leq b \leq c - 2$ and $1 \leq v \leq \min\{c - 2, p + b - c\}$.

Subcase (i): $b \leq \nu \leq \min\{c - 2, p + b - c\}$. By Theorem 6.4, we get

$$P : \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(\nu)}}{V_r^{(\nu+1)}}\right) \twoheadrightarrow \overline{\Theta}_{k',a_p}.$$

Observe that $2\nu + 1 - (p - 1) \leq b \leq 2\nu$ as $b \leq \nu \leq \min\{c - 2, p + b - c\}$. The equality $b = 2\nu + 2 - p$ occurs only if $b \leq 2c - 2 - p$, and these are possibly reducible cases. Therefore, by Lemma 2.5, we have $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+(\nu+1)(p-1)}\Big)$ as $2\nu + 1 - (p - 1) < b \leq 2\nu$.

Subcase (ii): $b = \nu + 1$ and $1 \leq \nu \leq \min\{c - 2, p + b - c\}$. By Theorem 6.4 we get

$$P : \mathrm{ind}_{KZ}^{G}\left(\frac{V_r}{V_r^{(1)}}\right) \twoheadrightarrow \overline{\Theta}_{k',a_p}.$$

If $b \neq p - 2$, then Lemma 2.5 gives $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1}\Big)$. Observe that $b = p - 2$ occurs only if $(\nu, c) = (c - 2, p - 1)$, and in this case, we proceed exactly the same as in the proof of part (1) above to get the required result.

Case (4): $2 \leq b \leq 2c-5-p$ *and* $\nu \in \{p+b-c+1, c-3\}$. In this case, Theorem 6.4 gives

$$P : \mathrm{ind}_{KZ}^{G}\left(\frac{V_r^{(p+b-c+1)}}{V_r^{(p+b-c+2)}}\right) \twoheadrightarrow \overline{\Theta}_{k',a_p}.$$

Observe that if $n = p+b-c+1$, then $2n+1-(p-1) < b < 2n$ as $b \leq 2c-5-p$. Hence, using Lemma 2.5, we obtain $\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+(p+b-c+2)(p-1)}\Big)$. $\square$

The following theorem is the main result of this section, where we prove local constancy by assuming Conjecture 5.2.

Theorem 7.2. *Let* $k = b + c(p-1) + 2$ *with* $2 \leq c \leq p-1$, $2 \leq b \leq p$ *and* $p \geq 5$. *Fix* a_p *such that* $\nu(a_p)$ *is non-integral,* $1 < \nu(a_p) < c - \epsilon$, *and let* $t > \nu(a_p) + c$. *Assume Conjecture 5.2 is true.*

(1) *If* $b \geq c + \nu - 1$ *such that* $b \neq 2\nu + 1$ *and* $(b, \nu) \neq (p, 1)$, *then*

$$\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+\nu(p-1)}\Big)$$

for all $k' \in k + p^t(p-1)\mathbb{Z}_{\geq 0}$.

(2) *If* $c-1 \leq b \leq 2c-4$ *and* $\nu = c-2$, *then*

$$\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{b+1+(b-c+1)(p-1)}\Big)$$

for all $k' \in k + p^t(p-1)\mathbb{Z}_{\geq 0}$.

(3) *Suppose* $2 \leq b \leq c-2$ *and* $1 \leq \nu \leq \min\{c-2, p+b-c\}$. *Also assume that* $b \neq 2\nu+2-p$ *if* $b \leq 2c-2-p$. *Then for all* $k' \in k+p^t(p-1)\mathbb{Z}_{\geq 0}$,

$$\overline{V}_{k',a_p} \cong \begin{cases} \mathrm{ind}\Big(\omega_2^{b+1+(\nu+1)(p-1)}\Big) & \text{if } b \leq \nu, \\ \mathrm{ind}\Big(\omega_2^{b+1}\Big) & \text{if } b = \nu+1. \end{cases}$$

(4) *If* $2 \leq b \leq 2c-5-p$ *and* $\nu \in \{p+b-c+1, c-3\}$, *then*

$$\overline{V}_{k',a_p} \cong \mathrm{ind}\Big(\omega_2^{k_0}\Big)$$

for all $k' \in k+p^t(p-1)\mathbb{Z}_{\geq 0}$, *where* $k_0 = b+1+(p+b-c+2)(p-1)$.

In the above cases the Berger's constant $m(k, a_p)$ *exists and* $m(k, a_p) \leq \lceil \nu(a_p) \rceil + c + 1$.

Remark 7.3. Here, we make an important remark that statement (1) is unconditional on Conjecture 5.2. This is because Conjecture 5.2 is a consequence of Conjecture 5.1, and the latter is proved in Lemma 5.4 for the cases required in statement (1) above (see also Remark 6.2 above).

Proof. Observe that since $\nu(a_p) < c - \epsilon$ we have

$$3\nu(a_p) + \frac{(k-1)p}{(p-1)^2} + 1 < 4c + 1 - 3\epsilon + \frac{(b+1)p}{(p-1)^2} + \frac{c}{(p-1)} < b + c(p-1) + 2 = k \qquad \forall\ p \geq 5.$$

The last inequality follows as $(b+1)(p^2-3p+1) + c(p^2-6p+4)(p-1) + 3\epsilon(p-1)^2 > 0$. Therefore, we get $k > 3\nu(a_p) + \frac{(k-1)p}{(p-1)^2} + 1$ so, by Theorem 2.3 there exists a constant $m = m(k, a_p)$ such that for all $k'' \in k + p^{m-1}(p-1)\mathbb{Z}_{\geq 0}$, we have $\overline{V}_{k'',a_p} \cong \overline{V}_{k,a_p}$. Observe that Proposition 7.1 determines $\overline{V}_{k',a_p}$ for all $k' \in k + p^t(p-1)\mathbb{Z}_{>0}$ (punctured disk around $k = s+2$) with $t > \nu(a_p) + c$ and shows that $\overline{V}_{k',a_p}$ is constant function of k' for each k. Note that both the disks $k + p^{m-1}(p-1)\mathbb{Z}_{\geq 0}$ and $k + p^t(p-1)\mathbb{Z}_{>0}$ have the same center. Therefore, we have $\overline{V}_{k',a_p} \cong \overline{V}_{k,a_p}$ for all $k' \in k + p^t(p-1)\mathbb{Z}_{\geq 0}$. Hence, we get $m(k, a_p) \geq t+1$ and also determine $\overline{V}_{k,a_p}$ in each case of the theorem. Thus, we have the desired result. □

Corollary 7.4. *Fix a_p such that $\nu(a_p)$ is non-integral and $1 < \nu(a_p) < p-1$. Let $p \geq 13$ and assume Conjecture 5.2 is true. Suppose that $k \notin \{2\nu + 3 + c(p-1), 2\nu + 4 - p + c(p-1)\}$ and $(k, \nu) \neq (p+2+c(p-1), 1)$, where c is given below. Theorem 7.2 computes $\overline{V}_{k,a_p}$ in the following cases:*

(1) *If $\nu = 1$, then for all*

$$k \in \bigcup_{c=2+\epsilon}^{p-1} [c+2+c(p-1), p+2+c(p-1)] \cup \bigcup_{c=3}^{p-1} \{4 + c(p-1)\}.$$

(2) *If $\nu = 2$, then for all*

$$k \in \bigcup_{c=3+\epsilon}^{p-1} [c+3+c(p-1), p+2+c(p-1)] \cup \bigcup_{c=4}^{p-1} [4+c(p-1), 5+c(p-1)] \cup \{4p+2\}.$$

(3) *If $\nu = 3$, then for all*

$$k \in \bigcup_{c=4+\epsilon}^{p-2} [c+4+c(p-1), p+2+c(p-1)] \cup \bigcup_{c=5}^{p-1} [4+c(p-1), 6+c(p-1)] \cup \{5p+2, 5p+3\}.$$

(4) *If* $4 \leq \nu \leq \frac{p-1}{2}$, *then for all*

$$\begin{aligned} k \in & \bigcup_{c=\nu+1+\epsilon}^{p+1-\nu} [c+\nu+1+c(p-1), p+2+c(p-1)] \\ & \cup \bigcup_{c=\nu+2}^{p-\nu+2} [4+c(p-1), \nu+3+c(p-1)] \\ & \cup \bigcup_{c=p-\nu+3}^{p-1} [c+\nu+1-p+c(p-1), \nu+3+c(p-1)] \\ & \cup [2+(\nu+2)p, \nu+(\nu+2)p]. \end{aligned}$$

(5) *If* $\frac{p+1}{2} \leq \nu \leq p-7$, *then for all*

$$\begin{aligned} k \in & \bigcup_{c=\nu+3}^{p-1} [c+\nu+1-p+c(p-1), \nu+3+c(p-1)] \\ & \cup [(\nu+1)p+\nu+2, (\nu+1)p+\nu+p]. \end{aligned}$$

(6) *If* $p-6 \leq \nu \leq p-5$, *then for all*

$$\begin{aligned} k \in & \bigcup_{c=\nu+2}^{\frac{p+\nu+3}{2}} [2c-p+c(p-1), \nu+3+c(p-1)] \\ & \cup \bigcup_{c=\nu+4}^{p-1} [c+\nu+1-p+c(p-1), 2c-1-p+c(p-1)] \\ & \cup [\nu+4+(\nu+2)(p-1), 2\nu+2+(\nu+2)(p-1)] \\ & \cup \{2\nu+4+(\nu+2)(p-1)\}. \end{aligned}$$

(7) *If* $\nu = p-4$, *then for all*

$$\begin{aligned} k \in & \bigcup_{c=p-2}^{p-1} [2c-p+c(p-1), p-1+c(p-1)] \\ & \cup [1+(p-1)^2, p-5+(p-1)^2] \cup \{p-3+(p-1)^2\}. \end{aligned}$$

(8) *If* $\nu = p-3$, *then for all* $k \in [p-2+(p-1)^2, p+2+(p-1)^2]$

Remark 7.5. We note that $\nu = p-2$ cannot occur. This is because we must also have $\nu = p-2 \leq c-1-\epsilon$, and so $\epsilon = 0$. Thus, $\nu = p-2$ could come only from Theorem 7.2(1) wherein $p \geq b \geq c+\nu-1$, forcing $p \leq 4$.

8. Proof of more cases of Conjecture 5.1

Recall that $m \in [1, c-1-\epsilon]$ in Conjecture 5.1.

Theorem 8.1. *Conjecture 5.1 is true in the following cases (with the additional conditions on m given below):*

(1) $m \in [1, b-c]$ *if* $b \geq c+1$.
(2) $m \in [1, \frac{b-1}{2}] \cap [b-c+1, c-1-\epsilon]$ *if* $b \geq c$.
(3) $m \in \Big([1, \frac{b-1}{2}] \cup [b, c-2]\Big) \cap [1, p+b-c]$ *if* $2 \leq b \leq c-1$.
(4) $m \in [p+b-c+1, \frac{p+b-2}{2}] \cap [p+b-c+1, c-3]$ *if* $2 \leq b \leq 2c-3-p$.

We give an equivalent version of the theorem above:

Corollary 8.2. *Conjecture 5.1 is true in the following cases (with the additional conditions on m given below):*

(1) *For all m if* $b \geq 2c-3$.
(2) $m \in [1, \frac{b-1}{2}] \cup [b, c-2]$ *if* $2c-2-p \leq b \leq 2c-4$.
(3) $m \in [1, \frac{b-1}{2}] \cup [b, c-3]$ *if* $2c-4-p \leq b \leq 2c-3-p$.
(4) $m \in [1, \frac{b-1}{2}] \cup [b, \frac{p+b-2}{2}]$ *if* $2 \leq b \leq 2c-5-p$.

Proof. When $b \geq 2c-2$, the full range of m i.e, $[1, c-1-\epsilon]$ is contained in $[1, b-c]$ as $c-1-\epsilon \leq b-c$, and so Theorem 8.1 (1) gives Corollary 8.2 (1) in this case. For $b = 2c-3$ we use Theorem 8.1 (1) and (2) for $1 \leq m \leq c-3$ and $m = c-2$ respectively to prove Corollary 8.2 (1).

Next, when $c \leq b \leq 2c-4$, observe that $[b, c-2]$ is empty and $[1, \frac{b-1}{2}] = [1, b-c] \cup ([1, \frac{b-1}{2}] \cap [b-c+1, c-1-\epsilon])$ as $b-c < \frac{b-1}{2}$ (since $b \leq 2c-4$). Therefore, the statement (2) of Corollary 8.2 is obtained by Theorem 8.1 (1) and (2) when $c \leq b \leq 2c-4$ and only by Theorem 8.1 (3) when $2c-2-p \leq b \leq c-1$.

Lastly, note that $\Big([1, \frac{b-1}{2}] \cup [b, c-2]\Big) \cap [1, p+b-c] = [1, \frac{b-1}{2}] \cup [b, p+b-c]$ if $b \leq 2c-3-p$. Thus, the last two statements of the corollary follow by Theorem 8.1 (3) and (4) as $[p+b-c+1, \frac{p+b-2}{2}] \cap [p+b-c+1, c-3]$ is equal to $[p+b-c+1, c-3]$ if $b \geq 2c-4-p$ and equal to $[p+b-c+1, \frac{p+b-2}{2}]$ if $b \leq 2c-5-p$. □

Remark 8.3. From the above corollary, we see that Conjecture 5.1 remains to be proven in the following cases:

(1) $m \in [\frac{b}{2}, b-1] \cap [1, c-2]$ if $2c-2-p \leq b \leq 2c-4$.
(2) $m \in [\frac{b}{2}, b-1]$ if $2c-4-p \leq b \leq 2c-3-p$.
(3) $m \in [\frac{b}{2}, b-1] \cup [\frac{p+b-1}{2}, c-3]$ if $2 \leq b \leq 2c-5-p$.

Using SageMath, we have verified that the matrix A defined in (5.1) is invertible for the above ranges of b, c, m and primes p up to 97.

We now prove Theorem 8.1.

Proof. Recall from Section 5 that we have the matrix

$$A = (\alpha(i,l))_{\substack{1\le i\le m+1\\ 0\le l\le m}}$$

where $\alpha(i,l)$ is as defined in (3.1). In proving the theorem, the main observation is to obtain some simple expression for $\alpha(i,l)$, which is essentially equivalent to giving a simple expression for $\alpha_1(i,l)$ (see (3.1)). Lemma 3.2 gives that $\alpha_1(i,l) \equiv \alpha'(i,l)$ (for definition of $\alpha'(i,l)$ see (3.3)). To prove cases (2) and (3) of the theorem, we show using Lemmas 3.5 and 3.7 that modulo p we have $\alpha'(i,l) = 0$ if $l \ge i$ and $\alpha'(i,l) = (-1)^{b-m+l}u_l v_i(m+1-i)\binom{i-1}{l}$ if $l \le i-1$. To prove the last part of the theorem, we use Lemmas 3.9 and 3.6 to do a similar analysis. We make an important comment that in all the cases, we will show that the last row of A is zero modulo p, and the remaining sub-matrix is of full rank. Hence for every $1 \le i' \le m$, modulo p the row rank of $[A : e_{i'}]$ is the same as the row rank of A. Thus, the linear systems $AX = e_{i'} \pmod p$ has a solution for all $1 \le i' \le m$.

Case (1): $b \ge c+1$ and $m \in [1, b-c]$. This is proved in Lemma 5.4.

Case (2): $b \ge c$ and $m \in [1, \frac{b-1}{2}] \cap [b-c+1, c-1-\epsilon]$. In this case, we write A as follows

$$A = \begin{pmatrix} A' & B' \\ A'' & B'' \end{pmatrix} \tag{8.1}$$

where the ranges of i and l are divided into non-empty intervals $[1, b-c+1]$, $[b-c+2, m+1]$ and $[0, b-c]$, $[b-c+1, m]$ respectively, determining the order of blocks.

Subcase (i): Analysis of A' and A'' (i.e., $0 \le l \le b-c$ and $1 \le i \le m+1$). For above range of l and for $1 \le i \le b-c+1$, Lemma 3.2 gives $\alpha_1(i,l) \equiv 0 \bmod p$ and

$$\binom{r-l}{b-m+(i+c-m-1)(p-1)} \equiv \binom{b-c-l}{b-c+1-i}\binom{c}{i+c-m-1}.$$

Hence, we have

$$\begin{aligned}\alpha(i,l) &\equiv \binom{b-c-l}{b-c+1-i}\binom{c}{c-m-1+i} \\ &\equiv 0 \bmod p \iff i < l+1.\end{aligned}$$

According to the calculation above, modulo p the matrix A' is an invertible lower triangular matrix. We also note that by Lemma 3.2 the matrix $A'' \equiv 0 \bmod p$ since both $\alpha'(i,l)$ and $X(i,l)$ are zero $\bmod\ p$ when $b-c+2 \le i \le m+1$ and $0 \le l \le b-c$.

Subcase (ii): Analysis of B'' (i.e., $b-c+1 \le l \le m$ and $b-c+2 \le i \le m+1$). In this case, we note that $m \le p+b-c$ as $b \ge c$ and $m \le c-1-\epsilon \le p-1$. Using Lemma 3.2, we get

$$\alpha(i,l) \equiv \begin{cases} \alpha'(i,l) + \binom{p+b-c-l}{p+b-c+1-i}\binom{c-1}{c-m-2+i} & \\ \qquad\qquad \text{if } b-c+1 \le l \le m,\ b-c+2 \le i \le m & \\ \alpha'(i,l) \qquad \text{if } b-c+1 \le l \le m, i = m+1 & \end{cases}$$

where $\alpha'(i,l)$ is as defined in (3.3). By Lemma 3.5, we have

$$\alpha'(i,l) \equiv u_l v_i \sum_{\epsilon_1 \le k \le c_1} (-1)^k (c-k)\binom{c-m-1+i}{k} \cdot \binom{i+c-m-2-k}{i-(b-c+2)}\binom{l+c-m-1-k}{l} \tag{8.2}$$

where $c_1 = \min\{c-m-1, b-m\}$, $u_l = (-1)^l l!(p+b-c-l)!(c-1)!$ and

$$v_i = \frac{(-1)^{i+1+c-m}(i-(b-c+2))!}{(i-1)!(m+1-i)!(c-m-1+i)!}$$

We note that $b \ge 2m+1$. Using the above calculations and Lemma 3.7 along with Remark 3.8, we obtain

$$\alpha'(i,l) \equiv \begin{cases} 0 & \text{if } i \le l \\ (-1)^{b-m+l} u_l v_i (m+1-i)\binom{i-1}{l} & \text{if } l \le i-1. \end{cases} \tag{8.3}$$

Hence, we get for $b-c+1 \le l \le m$

$$\alpha(i,l) \equiv \begin{cases} \binom{p+b-c-l}{p+b-c+1-i}\binom{c-1}{c-m-2+i} & \text{if } b-c+2 \le i \le m,\ i \le l \\ (-1)^{b-m+l} u_l v_i (m+1-i)\binom{i-1}{l} & \\ \quad + \binom{p+b-c-l}{p+b-c+1-i}\binom{c-1}{c-m-2+i} & \text{if } c_1' \le i \le m,\ l \le i-1 \\ 0 & \text{if } i = m+1 \end{cases}$$

where $c_1' = b-c+2$. The last case is clear as $(-1)^{b-m+l}u_l v_i(m+1-i)\binom{i-1}{l} = 0$ for $i = m+1$. For $i \le m$, we note that

$$\binom{p+b-c-l}{p+b-c+1-i}\binom{c-1}{c-m-2+i} = \frac{(-1)^{b+c+1+i}l!(p+b-c-l)!(c-1)!(i-(b-c+2))!\binom{i-1}{l}}{(i-1)!(m+1-i)!(c-m-2+i)!}.$$

Thus, we have for $b-c+1 \le l \le m$

$$\alpha(i,l) \equiv \begin{cases} \dfrac{(-1)^{b+c+1+i}l!(p+b-c-l)!(c-1)!(i-(b-c+2))!}{(i-1)!(m+1-i)!(c-m-2+i)!}\binom{i-1}{l} \\ \qquad\qquad \text{if } b-c+2 \le i \le m,\ i \le l \\ \dfrac{(-1)^{b+c+i+1}c\ l!(p+b-c-l)!(c-1)!(i-(b-c+2))!}{(i-1)!(m+1-i)!(c-m-1+i)!}\binom{i-1}{l} \\ \qquad\qquad \text{if } b-c+2 \le i \le m,\ l \le i-1 \\ 0 \qquad\qquad \text{if } i = m+1 \end{cases}$$

$$\equiv \begin{cases} u_l' v_i' \binom{i-1}{l} & \text{if } b-c+2 \le i \le m,\ b-c+1 \le l \le m \\ 0 & \text{if } i = m+1 \end{cases}$$

where $u_l' = l!(p+b-c-l)!$ and

$$v_i' = \begin{cases} \dfrac{(-1)^{b+c+1+i}(c-1)!(i-(b-c+2))!}{(i-1)!(m+1-i)!(c-m-2+i)!} & \text{if } b-c+2 \le i \le m,\ i \le l \\ \dfrac{(-1)^{b+c+i+1}c\ (c-1)!(i-(b-c+2))!}{(i-1)!(m+1-i)!(c-m-1+i)!} & \text{if } b-c+2 \le i \le m,\ l \le i-1. \end{cases}$$

From the above congruence on $\alpha(i,l)$, we have

$$B'' \equiv \begin{pmatrix} B''' & 0 \\ 0 & 0 \end{pmatrix} \bmod p, \quad \text{where } B''' = \left(u_l' v_i' \binom{i-1}{l}\right)_{\substack{b-c+2 \le i \le m \\ b-c+1 \le l \le m-1}} \tag{8.4}$$

and 0 denotes the zero matrix of the required size. We note that B''' is invertible (lower triangular with non-zero diagonal entries).

Therefore,

$$A \equiv \begin{pmatrix} A' & B' \\ 0 & B'' \end{pmatrix}$$

where A' is invertible mod p, and B'' is as above.

Case (3): $2 \le b \le c-1$ *and* $m \in \left([1, \frac{b-1}{2}] \cup [b, c-2]\right) \cap [1, p+b-c]$. If $m \in [1, \frac{b-1}{2}]$, then all the computations of Subcase (ii) of Case (2) for $\alpha(i,l)$ carry over here to give that the matrix A is of the form B'' as given in (8.4). If $m \in [b, c-2]$, then using Lemma 3.2, we observe that $\alpha_1(i,l) \equiv 0 \bmod p$. Using

this crucially, we write A as a block matrix of the form given in (5.2), where similar calculations as in Lemma 5.4 give modulo p that A' is invertible, and A'', B'' are zero.

Case (4): $2 \leq b \leq 2c-3-p$ *and* $m \in [p+b-c+1, \frac{p+b-2}{2}] \cap [p+b-c+1, c-3]$. In this case, we note that $\epsilon_1 = 1$ or 2 as $b \leq m$. If $m \geq p+b-c+2$, then we write A as follows

$$A = \begin{pmatrix} A' & B' \\ A'' & B'' \\ A''' & B''' \end{pmatrix}$$

where the ranges of i and l are divided into non-empty intervals $[1,\ p+b-c+1]$, $[p+b-c+2,\ m]$, $[m+1, m+1]$ and $[0, p+b-c]$, $[p+b-c+1,\ m]$ respectively, determining the order of blocks. If $m = p+b-c+1$, then we write A as follows

$$A = \begin{pmatrix} A' & B' \\ A''' & B''' \end{pmatrix}$$

where the ranges of i and l are divided into non-empty intervals $[1,\ m]$, $[m+1, m+1]$ and $[0, m-1]$, $[m,\ m]$ respectively, determining the order of blocks.

Next, one obtains that modulo p, A' is invertible and A'', A''' are zero using Lemma 3.2 and similar calculations as in Subcase (i) of Case (2). The analysis of blocks B'' and B''' is analogous to the calculation in Subcase (ii) of Case (2). For this, we use Lemmas 3.6 and 3.9 to obtain identities analogous to (8.2) and (8.3). By following similar steps we obtain modulo p that B''' is zero, and B'' is of full rank since

$$B'' \equiv (B_1'' \quad 0) \bmod p, \quad \text{where } B_1'' = \left(u_l' v_i' \binom{i-1}{l} \right)_{\substack{p+b-c+2 \leq i \leq m \\ p+b-c+1 \leq l \leq m-1}}. \quad \square$$

Appendix A.

Lemma A.1. *Proof of Lemma 3.1.*

Proof. We prove the above result by induction on a. Observe that it is trivially true for $a = 1$ and for all i. By induction, assume the above result is true for all $1 \leq a \leq k-1$ and we prove it for $a = k \geq 2$. Therefore, we need to prove

$$\binom{i+k-2}{k-1}\binom{m+k}{i+k-1} = \sum_{1 \leq l \leq k-1} (-1)^{l+1} \binom{m+1}{l} \beta(k-l, i) + (-1)^{k-1} \binom{m+1}{i+k-1}.$$

Using induction, we get

$$\sum_{0\le l\le k-1}(-1)^l\binom{m+1}{l}\binom{i+k-l-2}{i-1}\binom{m+k-l}{m+1-i} = (-1)^{k-1}\binom{m+1}{i+k-1}. \tag{A.1}$$

Hence, we need to prove the above equation to prove our lemma. Now,

$$(x-1)^{m+1} = \sum_{0\le l\le m+1}(-1)^l\binom{m+1}{l}x^{m+1-l}.$$

Multiply the above equation by x^{k-1} $(k\ge 2)$, we get

$$(x-1)^{m+1}x^{k-1} = \sum_{0\le l\le m+1}(-1)^l\binom{m+1}{l}x^{m+k-l}.$$

By differentiating the above equation with respect to x, $(m+1-i)$ times and multiplying by $\frac{x^{-1}}{(m+1-i)!}$, we get

$$\sum_{0\le j\le m+1-i}\binom{m+1}{m+1-i-j}\binom{k-1}{j}(x-1)^{i+j}x^{k-2-j} = \sum_{0\le l\le m+1}(-1)^l\binom{m+1}{l}\binom{m+k-l}{m+1-i}x^{i+k-l-2}.$$

Note that in the first sum, j can be taken over the range $0\le j\le n_1$ where $n_1 := \min\{m+1-i,\ k-1\}$. The last sum can be taken over the range $0\le l\le i+k-1$, since $\binom{m+k-l}{m+1-i}=0$ if $i+k-1<l\le m+1$ and $\binom{m+1}{l}=0$ if $m+1<l\le i+k-1$. Thus, we have

$$\sum_{0\le j\le n_1}\binom{m+1}{m+1-i-j}\binom{k-1}{j}(x-1)^{i+j}x^{k-2-j} = \sum_{0\le l\le i+k-1}(-1)^l\binom{m+1}{l}\binom{m+k-l}{m+1-i}x^{i+k-l-2}.$$

Again, by differentiating the above equation with respect to x, $(i-1)$ times and dividing by $(i-1)!$, we get

$$\sum_{0\le j\le n_1}\binom{m+1}{i+j}\binom{k-1}{j}\left(\sum_{0\le j'\le i-1}\binom{i+j}{i-1-j'}(x-1)^{j+j'+1}\frac{1}{j'!}d^{j'}(x^{k-2-j})\right)$$
$$=\sum_{0\le l\le i+k-2}(-1)^l\binom{m+1}{l}\binom{m+k-l}{m+1-i}\binom{i+k-l-2}{i-1}x^{k-l-1}$$
$$+(-1)^k\binom{m+1}{i+k-1}x^{-i}.$$

By putting $x=1$ in the above equation, we get

$$\sum_{0\le l\le i+k-2}(-1)^l\binom{m+1}{l}\binom{m+k-l}{m+1-i}\binom{i+k-l-2}{i-1}$$
$$+(-1)^k\binom{m+1}{i+k-1}=0$$

as $(x-1)^{j+j'+1}=0$ at $x=1$ (since $j,j'\ge 0$). Observe that the above summation can be taken over the range $0\le l\le k-1$ as $\binom{i+k-l-2}{i-1}=0$ if $k-1<l\le i+k-2$. Thus, we obtained the required equation (A.1) above. □

Lemma A.2. *Proof of Lemma 3.5*

Proof. Recall from the definition of $\alpha'(i,l)$ in (3.3), we have

$$\alpha'(i,l)=(-1)^{i+1}\sum_{\max\{c-b,1\}\le a\le c-m-\epsilon_1}\binom{p+b-c-l}{b-c+a}\binom{c-1}{c-m-a}\beta(a,i)$$

as $b-c+1\le l\le p+b-c$. Using Lemma A.1, we get

$$\alpha'(i,l)=(-1)^{i+1}\sum_{\max\{c-b,1\}\le a\le c-m-\epsilon_1}\binom{p+b-c-l}{b-c+a}$$
$$\cdot\binom{c-1}{c-m-a}\binom{i+a-2}{a-1}\binom{m+a}{i+a-1}.$$

Next,

$$\begin{aligned}
&\binom{p+b-c-l}{b-c+a}\binom{c-1}{c-m-a}\binom{i+a-2}{a-1}\binom{m+a}{i+a-1}\\
&\quad=\frac{(p+b-c-l)!(c-1)!(i+a-2)!(m+a)!}{(b-c+a)!(p-(l+a))!(c-m-a)!(m+a-1)!}\\
&\qquad\times\frac{1}{(a-1)!(i-1)!(i+a-1)!(m+1-i)!}\\
&\quad\equiv\frac{(p+b-c-l)!(c-1)!(i+a-2)!(l+a-1)!(m+a)(-1)^{l+a}}{(b-c+a)!(c-m-a)!(a-1)!(i-1)!(i+a-1)!(m+1-i)!}
\end{aligned}$$

The last congruence follows by noting that $(p-(l+a))!\equiv\frac{(-1)^{l+a}}{(l+a-1)!}\pmod p$. On multiplying and dividing by $l!(i+c-m-1)!(i-(b-c+2))!$ on the right-hand side of the above equation, we get

$$\begin{aligned}
&\binom{p+b-c-l}{b-c+a}\binom{c-1}{c-m-a}\binom{i+a-2}{a-1}\binom{m+a}{i+a-1}\\
&\equiv(-1)^{i+1+c-m+a}u_lv_i(m+a)\binom{i+c-m-1}{c-m-a}\binom{i+a-2}{i-(b-c+2)}\binom{l+a-1}{l}.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
\alpha'(i,l)&\equiv u_lv_i\sum_{\max\{c-b,1\}\le a\le c-m-\epsilon_1}(-1)^{c-m+a}(m+a)\binom{i+c-m-1}{c-m-a}\\
&\qquad\cdot\binom{i+a-2}{i-(b-c+2)}\binom{l+a-1}{l}\\
&=u_lv_i\sum_{\epsilon_1\le k\le c_1}(-1)^k(c-k)\binom{i+c-m-1}{k}\\
&\qquad\cdot\binom{i+c-m-2-k}{i-(b-c+2)}\binom{l+c-m-1-k}{l}.
\end{aligned}$$

The last equality follows by putting $k=c-m-a$. □

Lemma A.3. *Let $n, c, i, l \in \mathbb{Z}$ such that $l \geq \max\{0, n\}$ and $i \geq \max\{1, n+1\}$. Also assume that $1 \leq m \leq c-1$ and $n+c-m-1 \geq 0$. Then*

$$\sum_{0 \leq k \leq c-m-1} (-1)^k (c-k) \binom{c-m-1+i}{k} \cdot \binom{c-m-2+i-k}{i-(n+1)} \binom{l+c-m-1-k}{l} = \begin{cases} C_1 + C_2 & \text{if } i \leq l \\ C_1 + C_2 + (-1)^{n+c-m-1+l}(m+1-i)\binom{i-1}{l} & \text{if } l \leq i-1. \end{cases}$$

where

$$C_1 = \sum_{0 \leq j \leq m_1} (-1)^j c \binom{c-m-1+i}{i-(n+1+j)} \binom{l-(n+1+j)}{l-(n+c-m+j)}$$

$$C_2 = \sum_{0 \leq j \leq m_2} (-1)^j (n+c-m+j) \binom{c-m-1+i}{i-(n+1+j)} \binom{l-(n+1+j)}{l-(n+c-m-1+j)}$$

where $m_1 = \min\{i-(n+1), l-(n+c-m)\}$ and $m_2 = \min\{i-(n+1), l-(n+c-m-1)\}$. Further, $C_1 = 0$ if $l < n+c-m$ and $C_2 = 0$ if $l < n+c-m-1$.

Remark A.4. When $m = c-1$ and $j = l-(n+c-m-1)$ then the binomial coefficient $\binom{l-(n+1+j)}{l-(n+c-m-1+j)} = \binom{-1}{0} = 1$. This term appears in the last term of the sum in C_2 if $l-(n+c-m-1) \leq i-(n+1)$.

Proof. First, we consider the following binomial expansion

$$(x-1)^{c-m-1+i} x^{-1} = \sum_{0 \leq k \leq c-m-1+i} (-1)^k \binom{c-m-1+i}{k} x^{c-m-2+i-k}.$$

By differentiating $i-(n+1)$ times and dividing by $(i-n-1)!$, we get

$$\sum_{0 \leq j \leq i-(n+1)} (-1)^j \binom{c-m-1+i}{i-(n+1)-j} (x-1)^{n+c-m+j} x^{-(j+1)} = \sum_{0 \leq k \leq c-m-2+i} (-1)^k \binom{c-m-1+i}{k} \binom{c-m-2+i-k}{i-(n+1)} x^{n+c-m-1-k} + (-1)^{n+c-m-2} x^{n-i}.$$

Observe that $\binom{c-m-2+i-k}{i-(n+1)} = 0$ if $n+c-m-1 < k \leq c-m-2+i$. Therefore, we have

$$\begin{aligned}
&\sum_{0\leq j\leq i-(n+1)} (-1)^j \binom{c-m-1+i}{i-(n+1)-j} (x-1)^{n+c-m+j} x^{-(j+1)} \\
&= \sum_{0\leq k\leq n+c-m-1} (-1)^k \binom{c-m-1+i}{k} \binom{c-m-2+i-k}{i-(n+1)} x^{n+c-m-1-k} \\
&\quad + (-1)^{n+c-m-2} x^{n-i}.
\end{aligned}$$

In the above equation, we multiply by $\frac{x^{l-n}}{l!}$, and then differentiate l times. We get the following

$$\begin{aligned}
&\sum_{0\leq j\leq i-(n+1)} (-1)^j \binom{c-m-1+i}{i-(n+1)-j} \left(\frac{D^l}{l!}\right) \left((x-1)^{n+c-m+j} x^{l-(n+1+j)}\right) \\
&\quad = \sum_{0\leq k\leq n+c-m-1} (-1)^k \binom{c-m-1+i}{k} \binom{c-m-2+i-k}{i-(n+1)} \\
&\qquad \cdot \binom{l+c-m-1-k}{l} x^{c-m-1-k} + \frac{(-1)^{n+c-m-2}}{l!} D^l(x^{l-i})
\end{aligned}$$

where $D := \frac{\mathrm{d}}{\mathrm{d}x}$ differential operator. Observe that $\binom{l+c-m-1-k}{l} = 0$ if $c-m-1 < k \leq n+c-m-1$ and $\binom{c-m-2+i-k}{i-(n+1)} = 0$ if $n+c-m-1 < k \leq c-m-1$. Therefore, even if $n < 0$, we can extend the sum above to $k \leq c-m-1$, giving us

$$\begin{aligned}
&\sum_{0\leq j\leq i-(n+1)} (-1)^j \binom{c-m-1+i}{i-(n+1)-j} \left(\frac{D^l}{l!}\right) \left((x-1)^{n+c-m+j} x^{l-(n+1+j)}\right) \\
&\quad = \sum_{0\leq k\leq c-m-1} (-1)^k \binom{c-m-1+i}{k} \binom{c-m-2+i-k}{i-(n+1)} \\
&\qquad \cdot \binom{l+c-m-1-k}{l} x^{c-m-1-k} + \frac{(-1)^{n+c-m-2}}{l!} D^l(x^{l-i}).
\end{aligned}$$

Again, we multiply by x^{m+1} and after we that differentiate one time the above equation to obtain the following

$$\begin{aligned}
&\sum_{0\le j\le i-(n+1)} (-1)^j \binom{c-m-1+i}{i-(n+1)-j} \\
&\qquad\qquad \cdot D\left(x^{m+1}\left(\frac{D^l}{l!}\right)\left((x-1)^{n+c-m+j}x^{l-(n+1+j)}\right)\right) \\
&= \sum_{0\le k\le c-m-1} (-1)^k (c-k)\binom{c-m-1+i}{k}\binom{c-m-2+i-k}{i-(n+1)} \\
&\qquad \cdot \binom{l+c-m-1-k}{l} x^{c-1-k} + \frac{(-1)^{n+c-m-2}}{l!} D(x^{m+1}D^l(x^{l-i})).
\end{aligned}$$

By putting $x = 1$ in the above equation, we get

$$\begin{aligned}
(\text{A.2}) \quad &\sum_{0\le k\le c-m-1} (-1)^k (c-k)\binom{c-m-1+i}{k} \\
&\qquad\qquad \cdot \binom{c-m-2+i-k}{i-(n+1)}\binom{l+c-m-1-k}{l} \\
&= \sum_{0\le j\le i-(n+1)} (-1)^j \binom{c-m-1+i}{i-(n+1)-j} \\
&\qquad \cdot D\left(x^{m+1}\left(\frac{D^l}{l!}\right)\left((x-1)^{n+c-m+j}x^{l-(n+1+j)}\right)\right)\Big|_{x=1} \\
&\qquad\qquad + \frac{(-1)^{n+c-m-1}}{l!} D(x^{m+1}D^l(x^{l-i}))|_{x=1}.
\end{aligned}$$

Now,

$$\begin{aligned}
&D\left(\frac{x^{m+1}D^l}{l!}\left((x-1)^{n+c-m+j}x^{l-(n+1+j)}\right)\right) \\
&\qquad = \sum_{0\le a\le l} \binom{n+c-m+j}{a} \\
&\qquad\qquad \cdot D\left((x-1)^{n+c-m+j-a}x^{m+1}\left(\frac{D^{l-a}}{(l-a)!}\right)(x^{l-(n+1+j)})\right).
\end{aligned}$$

Observe that $\binom{n+c-m+j}{a} = 0$ if $n+c-m+j < a$. Hence, we have

$$D\left(\frac{x^{m+1}D^l}{l!}\Big((x-1)^{n+c-m+j}x^{l-(n+1+j)}\Big)\right)$$
$$= \sum_{0\le a\le n_1}\binom{n+c-m+j}{a}$$
$$\cdot D\left((x-1)^{n+c-m+j-a}x^{m+1}\left(\frac{D^{l-a}}{(l-a)!}\right)(x^{l-(n+1+j)})\right),$$

where $n_1 = \min\{l, n+c-m+j\}$. Therefore, we get

$$D\left(\frac{x^{m+1}D^l}{l!}\Big((x-1)^{n+c-m+j}x^{l-(n+1+j)}\Big)\right)$$
$$= \sum_{0\le a\le n_1}\binom{n+c-m+j}{a}(n+c-m+j-a)$$
$$\cdot\left((x-1)^{n+c-m-1+j-a}x^{m+1}\left(\frac{D^{l-a}}{(l-a)!}\right)(x^{l-(n+1+j)})\right)$$
$$+\sum_{0\le a\le n_1}\binom{n+c-m+j}{a}$$
$$\cdot\left((x-1)^{n+c-m+j-a}D\left(x^{m+1}\left(\frac{D^{l-a}}{(l-a)!}\right)(x^{l-(n+1+j)})\right)\right).$$

Note that at $x=1$ the former sum is zero if $l < n+c-m-1$ and the latter sum is zero if $l < n+c-m$ (i.e., if $m_2 < 0$ and if $m_1 < 0$ respectively). We have

$$\sum_{0\le j\le i-(n+1)}(-1)^j\binom{c-m-1+i}{i-(n+1)-j}$$
$$\cdot D\left(x^{m+1}\left(\frac{D^l}{l!}\right)\Big((x-1)^{n+c-m+j}x^{l-(n+1+j)}\Big)\right)\Bigg|_{x=1}$$
$$= \sum_{0\le j\le m_2}(-1)^j(n+c-m+j)\binom{c-m-1+i}{i-(n+1+j)}\binom{l-(n+1+j)}{l-(n+c-m-1+j)}$$
$$+\sum_{0\le j\le m_1}(-1)^j c\binom{c-m-1+i}{i-(n+1+j)}\binom{l-(n+1+j)}{l-(n+c-m+j)}.$$

Hence, from (A.2), we get

$$\sum_{0\le k\le c-m-1}(-1)^k(c-k)\binom{c-m-1+i}{k}\cdot\binom{c-m-2+i-k}{i-(n+1)}\binom{l+c-m-1-k}{l}$$
$$=C_2+C_1+\frac{(-1)^{n+c-m-1}}{l!}D\Big(x^{m+1}D^l(x^{l-i})\Big)\Big|_{x=1}.$$

If $l\ge i$, then $D^l(x^{l-i})=0$ since $l\ge i\ge 1$, giving us we the required identity in this case. If $l\le i-1$, then

$$\frac{(-1)^{n+c-m-1}}{l!}D\Big(x^{m+1}D^l(x^{l-i})\Big)\Big|_{x=1}=(-1)^{n+c-m-1+l}(m+1-i)\binom{i-1}{l}.$$

Hence, we obtain our identity in this case too. □

Lemma A.5. *Proof of Lemma 6.3*

Proof. We will prove our lemma in the following three cases.

Case (1): $c-1\le b\le p$ (and $\nu\le c-1-\epsilon$). We begin by observing that we need to construct W_0 only when $b\ge c$ as $[0,n_1]$ is empty for $b=c-1$.

Subcase (i): $c\le b\le p-1$. We observe that $\nu\big(\binom{r}{p-1}\big)\ge 1$ (as $c\ge 2$) and also $\binom{r}{b+j(p-1)}\equiv 0 \bmod p$ for all $0\le j\le c-1$. Therefore, by Proposition 4.3 (for $l=0$ and $m=0$) we have

$$(T-a_p)\begin{pmatrix}f^0\\ p\end{pmatrix}\equiv\left[g,\sum_{\substack{0<j<s\\ j\equiv b \bmod (p-1)}}\frac{\binom{r}{j}}{p}x^{r-j}y^j\right].$$

But $x^{r-j}y^j\equiv x^{r-\bar{j}}y^{\bar{j}} \bmod \left(V_r^{(1)}\right)$ where $\bar{j}\equiv j \bmod (p-1)$ and $2\le\bar{j}\le p$. Observe that $\frac{\binom{r}{j}}{p}\in\mathbb{Z}$ for all $0<j<s$ such that $j\equiv r \bmod (p-1)$. Hence, we have

$$\sum_{\substack{0<j<s\\ j\equiv r \bmod p-1}}\frac{\binom{r}{j}}{p}x^{r-j}y^j\equiv\eta x^{r-b}y^b \mod \left(V_r^{(1)}\right)$$

where

$$\eta=\sum_{\substack{0<j<s\\ j\equiv s \bmod (p-1)}}\frac{\binom{r}{j}}{p}\equiv\sum_{\substack{0<j<s\\ j\equiv s \bmod (p-1)}}\frac{\binom{s}{j}}{p}\equiv\frac{b-s}{b}\not\equiv 0 \mod p.$$

Here the first congruence follows as $\frac{\binom{r}{j}}{p} \equiv \frac{\binom{s}{j}}{p} \mod p^{t-1-\nu(j!)}$ and $t-1-\nu(j!) > \nu(a_p) > 1$ (since $t > \nu(a_p)+c$, $\nu(j!) \leq \nu((s-(p-1))!) \leq c-1$). The second last congruence follows from Lemma 2.5 of [14]. Hence, we have

$$(T-a_p)\left(\frac{f^0}{\eta p}\right) \equiv \left[g,\ x^{r-b}y^b\right] \bmod (V_r^{(1)})$$

as η is p-adic unit. Therefore, there exists a $v_1 \in V_r^{(1)}$ such that

$$(T-a_p)\left(\frac{f^0}{\eta p}\right) \equiv \left[g,\ x^{r-b}y^b - v_1\right]$$

Using equation (2.3) (with $r' = p-1+b$), we observe that the monomial $x^{r-b}y^b$ and x^r generates the quotient $V_{p-1-b} \otimes D^b$ and submodule V_b of $\frac{V_r}{V_r^{(1)}}$ respectively. But x^r belongs to $\mathrm{Ker}(P)$ by Remark 4.4 of [19]. Let W_0 is the sub module generated by x^r, $x^{r-b}y^b - v_1$ if $b \geq c$. Observe that W_0 satisfies all the required conditions.

Subcase (ii): $b = p$. In this case by using (2.2) we have the following

$$0 \longrightarrow V_1 \longrightarrow \frac{V_r}{V_r^{(1)}} \longrightarrow V_{p-2} \otimes D \longrightarrow 0.$$

In the above exact sequence, the first map sends x to x^r and the second map sends $x^{r-1}y$ to x^{p-2}. By the Remark 4.4 of [19], we have $x^r,\ x^{r-1}y \in \mathrm{Ker}(P)$ as $1 < \nu(a_p)$. We define W_0 in this case as the submodule generated by x^r and $x^{r-1}y$, and observe that W_0 satisfies the required conditions of Lemma 2.1.

Case (2): $2 \leq b \leq c-2$ *and* $1 \leq \nu \leq \min\{c-2, p+b-c\}$. In this case, we need to construct W_0 only when $b \leq \nu$ as it is clear from the statement of Proposition 6.1. By Proposition 4.3 (for $m = 0$ and $0 \leq l \leq \min\{\nu, p+b-c\}$), we have

$$\begin{aligned}(T-a_p)\left(f^l\right) &\equiv \left[g,\ \sum_{0\leq j\leq c-1} \binom{r-l}{b+j(p-1)} x^{r-(b+j(p-1))}y^{(b+j(p-1))}\right] \\ &\equiv \left[g,\ \left(\sum_{0\leq j\leq c-1} \binom{r-l}{b+j(p-1)}\right) x^{r-b}y^b\right] \bmod (V_r^{(1)}).\end{aligned}$$

The last congruence follows from the same observation as in Case (1) above. By applying Lemma 3.4 of [31] for $m = 0$ (see the second and fifth case),

we get

$$\binom{r-l}{b+j(p-1)} \equiv \begin{cases} \binom{p+b-c-l}{b-j}\binom{c-1}{j} & \text{if } 0 \le l \le p+b-c,\ 0 \le j \le b \\ 0 & \text{if } 0 \le l \le p+b-c,\ b+1 \le j \le c-1. \end{cases}$$

Therefore, we have

$$\begin{aligned}(T-a_p)\big(f^l\big) &\equiv \left[g,\ \left(\sum_{0\le j\le b}\binom{p+b-c-l}{b-j}\binom{c-1}{j}\right)x^{r-b}y^b\right] \bmod (V_r^{(1)}) \\ &\equiv \left[g,\ \binom{p+b-1-l}{b}x^{r-b}y^b\right] \bmod (V_r^{(1)}).\end{aligned}$$

The latter congruence is followed by Vandermonde's identity. Since $b \le \nu$, one can take $l = b$ in Proposition 4.3, in which case $\binom{p+b-1-l}{b} \not\equiv 0 \pmod p$. Thus,

$$[g, x^{r-b}y^b] \in V_r^{(1)} + \mathrm{Ker}(P).$$

Using (2.3) (with $r' = p-1+b$), we observe that the monomial $x^{r-b}y^b$ and x^r generates the quotient $V_{p-1-b}\otimes D^b$ and submodule V_b of $\frac{V_r}{V_r^{(1)}}$ respectively. But x^r belongs to $\mathrm{Ker}(P)$ by Remark 4.4 of [19]. Therefore, taking W_0 to be the submodule generated by x^r and $x^{r-b}y^b$ has the required properties.

Case (3): $2 \le b \le 2c-4-p$ *and* $p+b-c+1 \le \nu \le c-3$. Observe that $b \le \nu$ in this case, thus applying Proposition 4.3 with same ranges $m = 0$ and $0 \le l \le \min\{\nu, p+b-c\}$ as in Case (2) giving required W_0. □

Acknowledgments. We owe a great debt to the work in [12] and [8] critical to our work. The authors would like to express sincere gratitude to Shalini Bhattacharya for giving useful suggestions regarding this problem. We thank the anonymous referee for helpful comments and suggestions. The second author acknowledges the valuable support from IISER Tirupati during his postdoctoral research fellowship at the institute.

References

[1] B. Arsovski, "On the reductions of certain two-dimensional crystabelline representations", *Res. Math. Sci.* **8** (2021), no. 1, article no. 12 (50 pages).

[2] ———, "On the reductions of certain two-dimensional crystalline representations", *Doc. Math.* **26** (2021), p. 1929-1979.

[3] L. Barthel & R. Livné, "Irreducible modular representations of GL_2 of a local field", *Duke Math. J.* **75** (1994), no. 2, p. 261-292.

[4] ———, "Modular representations of GL_2 of a local field: the ordinary, unramified case", *J. Number Theory* **55** (1995), no. 1, p. 1-27.

[5] J. Bergdall, "Upper bounds for constant slope p-adic families of modular forms", *Sel. Math., New Ser.* **25** (2019), no. 4, article no. 59 (24 pages).

[6] J. Bergdall & B. Levin, "Reductions of some two-dimensional crystalline representations via Kisin modules", *Int. Math. Res. Not.* **2022** (2022), no. 4, p. 3170-3197.

[7] L. Berger, "Représentations modulaires de $\mathrm{GL}_2(\mathbb{Q}_p)$ et représentations galoisiennes de dimension 2", in *Représentations p-adiques de groupes p-adiques II: Représentations de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et* (ϕ,Γ)*-modules*, Astérisque, vol. 330, Société Mathématique de France, 2010, p. 263-279.

[8] ———, "Local constancy for the reduction mod p of 2-dimensional crystalline representations", *Bull. Lond. Math. Soc.* **44** (2012), no. 3, p. 451-459.

[9] L. Berger & C. Breuil, "Sur quelques représentations potentiellement cristallines de $\mathrm{GL}_2(\mathbb{Q}_p)$", in *Représentations p-adiques de groupes p-adiques II: Représentations de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et* (ϕ,Γ)*-modules*, Astérisque, vol. 330, Société Mathématique de France, 2010, p. 155-211.

[10] L. Berger & P. Colmez, "Familles de représentations de de Rham et monodromie p-adique", in *p-adic representations of p-adic groups I. Galois representations and* (ϕ,Γ)*-modules*, Astérisque, vol. 319, Société Mathématique de France, 2008, p. 303-337.

[11] L. Berger, H. Li & H. J. Zhu, "Construction of some families of 2-dimensional crystalline representations", *Math. Ann.* **329** (2004), no. 2, p. 365-377.

[12] S. Bhattacharya, "Reduction of certain crystalline representations and local constancy in the weight space", *J. Théor. Nombres Bordeaux* **32** (2020), no. 1, p. 25-47.

[13] S. Bhattacharya & A. Ganguli, "Weights for mod p quaternionic forms in the unramified case", *J. Algebra Appl.* (2025), Online Ready, https://doi.org/10.1142/S0219498826502701.

[14] S. Bhattacharya & E. Ghate, "Reductions of Galois representations for slopes in $(1,2)$", *Doc. Math.* **20** (2015), p. 943-987.

[15] S. Bhattacharya, E. Ghate & S. Rozensztajn, "Reductions of Galois representations of slope 1", *J. Algebra* **508** (2018), p. 98-156.

[16] C. Breuil, "Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbb{Q}_p)$. I", *Compos. Math.* **138** (2003), no. 2, p. 165-188.

[17] ———, "Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbb{Q}_p)$. II", *J. Inst. Math. Jussieu* **2** (2003), no. 1, p. 23-58.

[18] K. Buzzard, "Eigenvarieties", in *L-functions and Galois Representations*, London Mathematical Society Lecture Note Series, vol. 320, Cambridge University Press, 2007, p. 59-120.

[19] K. Buzzard & T. Gee, "Explicit reduction modulo p of certain two-dimensional crystalline representations", *Int. Math. Res. Not.* **2009** (2009), no. 12, p. 2303-2317.

[20] ———, "Explicit reduction modulo p of certain 2-dimensional crystalline representations, II", *Bull. Lond. Math. Soc.* **45** (2013), no. 4, p. 779-788.

[21] G. Chenevier, "Sur la densité des représentations cristallines de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$", *Math. Ann.* **355** (2013), no. 4, p. 1469-1525.

[22] A. Chitrao, E. Ghate & S. Yasuda, "Semi-stable representations as limits of crystalline representations", *Algebra Number Theory* **19** (2025), no. 6, p. 1049-1097.

[23] R. Coleman & B. Mazur, "The eigencurve", in *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, London Mathematical Society Lecture Note Series, vol. 254, Cambridge University Press, 1998, p. 1-114.

[24] P. Colmez, "Représentations triangulines de dimension 2", in *p-adic representations of p-adic groups I. Galois representations and* (ϕ,Γ)*-modules*, Astérisque, vol. 319, Société Mathématique de France, 2008, p. 213-258.

[25] P. Colmez & J.-M. Fontaine, "Construction des représentations p-adiques semi-stables", *Invent. Math.* **140** (2000), no. 1, p. 1-43.

[26] A. Conti & E. Torti, "Lattices in rigid analytic representations", 2024, https://arxiv.org/abs/2403.20232.

[27] B. Edixhoven, "The weight in Serre's conjectures on modular forms", *Invent. Math.* **109** (1992), no. 3, p. 563-594.

[28] J.-M. Fontaine & Y. Ouyang, "Theory of p-adic Galois representations", http://staff.ustc.edu.cn/~yiouyang/galoisrep.pdf.

[29] A. Ganguli, "On the reduction modulo p of certain modular p-adic Galois representations", *J. Number Theory* **172** (2017), p. 392-412.

[30] A. Ganguli & E. Ghate, "Reductions of Galois representations via the mod p local Langlands correspondence", *J. Number Theory* **147** (2015), p. 250-286.
[31] A. Ganguli & S. Kumar, "On the local constancy of certain mod p Galois representations", *Res. Number Theory* **10** (2024), no. 2, article no. 52 (43 pages).
[32] E. Ghate, "A zig-zag conjecture and local constancy for Galois representations", *RIMS Kôkyûroku Bessatsu* **B86** (2021), p. 249-268, Algebraic Number Theory and Related Topics 2018.
[33] ———, "Zig-zag for Galois Representations", 2023, `https://arxiv.org/abs/2211.12114v2`.
[34] E. Ghate & V. Rai, "Reductions of Galois representations of Slope $\frac{3}{2}$", *Kyoto J. Math.* **65** (2025), no. 3, p. 595-636.
[35] E. Ghate & R. Vangala, "The monomial lattice in modular symmetric power representations", *Algebr. Represent. Theory* **25** (2022), no. 1, p. 121-185.
[36] D. J. Glover, "A study of certain modular representations", *J. Algebra* **51** (1978), no. 2, p. 425-475.
[37] E. Hellmann, "Families of p-adic Galois representations and (φ, Γ)-modules", *Comment. Math. Helv.* **91** (2016), no. 4, p. 721-749.
[38] K. Kedlaya & R. Liu, "On families of ϕ, Γ-modules", *Algebra Number Theory* **4** (2010), no. 7, p. 943-967.
[39] E. Nagel & A. Pande, "Reductions of modular Galois representations of slope (2,3)", *Ramanujan J.* **67** (2025), no. 3, article no. 70 (62 pages).
[40] S. Rozensztajn, "An algorithm for computing the reduction of 2-dimensional crystalline representations of $\mathrm{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p\right)$", *Int. J. Number Theory* **14** (2018), no. 07, p. 1857-1894.
[41] E. Torti, "Local constancy for reductions of two-dimensional crystalline representations", *J. Théor. Nombres Bordeaux* **34** (2022), no. 2, p. 345-370.
[42] ———, "On the existence of analytic families of G-stable lattices and their reductions", 2024, `https://arxiv.org/abs/2401.00462`.

Abhik Ganguli
Department of Mathematical Sciences
Indian Institute of Science Education and Research Mohali
SAS Nagar, Punjab - 140306, India
E-mail: `aganguli@iisermohali.ac.in`

Suneel Kumar
Department of Mathematics and Statistics
Indian Institute of Technology Kanpur
Uttar Pradesh - 208016, India
E-mail: `suneelm145@gmail.com`