# On the Reductions of Certain Two-Dimensional Crystalline Representations

Bodan Arsovski

Received: November 10, 2017
Revised: September 7, 2021

Communicated by Don Blasius

Abstract. The question of computing the reductions modulo $p$ of two-dimensional crystalline $p$-adic Galois representations has been studied extensively, and partial progress has been made for representations that have small weights, very small slopes, or very large slopes. It was conjectured by Breuil, Buzzard, and Emerton that these reductions are irreducible if they have even weight and non-integer slope. We prove some instances of this conjecture for slopes up to $\frac{p-1}{2}$.

2020 Mathematics Subject Classification: 11S20

Keywords and Phrases: Crystalline, residual, irreducible, Langlands, slopes

## 1 Introduction

Throughout this article we assume that $p$ is an odd prime number. The main objects we study are irreducible two-dimensional crystalline representations of the absolute Galois group of $\mathbb{Q}_p$. These are up to a twist parametrized by an integer $k \geqslant 2$ and an element $a \in \overline{\mathbb{Z}}_p$ such that $v_p(a) > 0$, and we denote by $V_{k,a}$ the representation corresponding to the parameters $(k, a)$[1]. In Section 2 we outline a construction of $V_{k,a}$ and reference proofs of some of its basic properties. Thus in the remainder of this article we assume that $k \in \mathbb{Z}$ and $a \in \overline{\mathbb{Z}}_p$ are parameters satisfying the properties $k \geqslant 2$ and $v_p(a) > 0$. We also define the modulo $p$ representation $\overline{V}_{k,a}$ as the semi-simplification of the reduction

[1] Thus all two-dimensional crystalline representations of $G_{\mathbb{Q}_p}$ are of the form $V_{k,a} \otimes \eta$ for some character $\eta$ of $G_{\mathbb{Q}_p}$ that is the product of an unramified character and a power of the cyclotomic character.

modulo the maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{Z}}_p$ of a Galois stable $\overline{\mathbb{Z}}_p$-lattice in $V_{k,a}$. The most interesting property of $V_{k,a}$ is that the representation associated with a non-ordinary finite slope classical eigenform

$$f = \sum_{n=1}^{\infty} a_n q^n$$

—which is normalized so that $a_1 = 1$ and has weight $k \geqslant 2$, level $\Gamma_0(N)$ such that $(N, p) = 1$, and character $\chi$—is crystalline and equal to $V_{k,a_p\sqrt{\chi}(p)} \otimes \sqrt{\chi}$, where $\sqrt{\chi}$ is an unramified character of $G_{\mathbb{Q}_p}$ whose square is $\chi$.

### 1.1 The conjecture

The motivation behind the conjecture considered in this article comes from an observation made by Buzzard and Gouvêa in [Buz05] and [Gou01] (based on computational data) that, if $p$ belongs to a certain class of "$\Gamma_0(N)$-regular"-primes, the slope $v_p(a_p)$ of $f$ appears to always be an integer. A definition of $\Gamma_0(N)$-regularity is given in [Buz05] (see also [BG16]), and its connection with Galois representations is that a prime $p > 2$ is $\Gamma_0(N)$-regular if and only if, for all weights $k \geqslant 2$ and all $f \in S_k(\Gamma_0(N))$, the modulo $p$ representation associated with $f$ is reducible. Note that, since the level of $f$ is $\Gamma_0(N)$, its weight $k$ must be even. This naturally leads to the general conjecture, made by Breuil, Buzzard, and Emerton, that if $k$ is even and $\overline{V}_{k,a}$ is reducible then $v_p(a)$ is an integer. We consider this conjecture in the following slightly rephrased form (see Conjecture 4.1.1 in [BG16]).

Conjecture A. *If $k$ is even and $v_p(a) \notin \mathbb{Z}$ then $\overline{V}_{k,a}$ is irreducible.*

### 1.2 Known results

The question of computing $\overline{V}_{k,a}$ has been studied extensively. A classification of $\overline{V}_{k,a}$ for $k \leqslant 2p+1$ follows from the work of Berger and Breuil in [Ber10], [Bre03a], and [Bre03b]. A classification of $\overline{V}_{k,a}$ when the slope $v_p(a)$ is greater than $\lfloor \frac{k-2}{p-1} \rfloor$ follows from the work of Berger, Li, and Zhu, in [BLZ04]. With some exceptions, $\overline{V}_{k,a}$ has been computed when $v_p(a) < 2$ in the work of Buzzard, Gee, Ganguli, Ghate, Bhattacharya, Rozensztajn, and Rai in [BG15], [BGR18], [BG09], [BG13], [GG15], and [GR]. Finally, Rozensztajn's work [Roz18] gives an algorithm that computes $\overline{V}_{k,a}$ for given $p, k, a$, and her work [Roz20] gives an algorithm that finds the locus of all $a$ such that $\overline{V}_{k,a} = \overline{\rho}$ for given $p, k$, and a modulo $p$ representation $\overline{\rho}$.

### 1.3 The main theorem in this article

We prove the following theorem.

Theorem 1. *If $v_p(a) \notin \mathbb{Z}$ and $\nu = \lceil v_p(a) \rceil$ is such that*

$$k \not\equiv 3, 4, \ldots, 2\nu, 2\nu + 1 \bmod p - 1,$$

*then $\overline{V}_{k,a}$ is irreducible. In particular, Conjecture A is true when*

$$k \not\equiv 4, \ldots, 2\nu \bmod p - 1.$$

Note that $\nu \in \{1, 2, 3, \ldots\}$ and the theorem is vacuous when $\nu > \frac{p-1}{2}$. The proof of Theorem 1 is based on the method (developed by Breuil, Buzzard, and Gee) of using the local Langlands correspondence and its compatibility with reduction modulo $p$ to compute the representations of $G_{\mathbb{Q}_p}$ by computing certain corresponding representations of $\mathrm{GL}_2(\mathbb{Q}_p)$. We give detailed outlines of the proof in Sections 3 and 10 after setting up the necessary framework.

Acknowledgements

I would like to thank professor Kevin Buzzard for his helpful remarks, suggestions, and support. This work was supported by Imperial College London and its President's PhD Scholarship.

## 2 Crystalline representations

Recall that we assume that $p$ is an odd prime number and $k \in \mathbb{Z}$ and $a \in \overline{\mathbb{Z}}_p$ are such that $k \geqslant 2$ and $v_p(a) > 0$. The representation $V_{k,a}$ is defined in Subsection 3.1 of [Bre03b] as the irreducible two-dimensional representation of $G_{\mathbb{Q}_p}$ that is crystalline on $\mathbb{Q}_p$ and such that

$$D_{cris}(V^*_{k,a}) = D_{k,a}$$

for the weakly admissible filtered $\varphi$-module $D_{k,a} = \overline{\mathbb{Q}}_p e_1 \oplus \overline{\mathbb{Q}}_p e_2$ which has Hodge–Tate weights $(0, k-1)$, a filtration

$$\mathrm{Fil}^i(D_{k,a}) = \begin{cases} D_{k,a} & \text{if } i \leqslant 0, \\ \overline{\mathbb{Q}}_p e_1 & \text{if } 0 < i < k, \\ 0 & \text{if } i \geqslant k, \end{cases}$$

and a Frobenius map $\varphi$ such that

$$\begin{cases} \varphi(e_1) = p^{k-1} e_2, \\ \varphi(e_2) = -e_1 + a e_2. \end{cases}$$

All irreducible two-dimensional crystalline representations of $G_{\mathbb{Q}_p}$ are of the form $V_{k,a} \otimes \eta$ for some character $\eta$ of $G_{\mathbb{Q}_p}$ that is the product of an unramified character and a power of the cyclotomic character (see Proposition 3.1

in [Bre03b]). We define $\overline{V}_{k,a}$ to be the semi-simplification of the reduction of a Galois stable $\overline{\mathbb{Z}}_p$-lattice in $V_{k,a}$ modulo the maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{Z}}_p$ (the resulting representation is independent of the choice of lattice).

In the remainder of this article we assume that $v_p(a) \notin \mathbb{Z}$ and we denote $\nu := \lceil v_p(a) \rceil$, so that $\nu \in \{1, 2, 3, \ldots\}$ and $\nu - 1 < v_p(a) < \nu$. Since Theorem 1 is vacuous when $v_p(a) > \frac{p-1}{2}$, we assume that $\nu \in \{1, \ldots, \frac{p-1}{2}\}$. Moreover, since $\overline{V}_{k,a}$ has been completely classified when $k \leqslant 2p+1$ (see for instance Theorem 3.2.1 in [Ber10]), we assume that $a^2 \neq 4p^{k-1}$ and $a \neq \pm(1+p^{-1})p^{k/2}$.

## 3 The $p$-adic and modulo $p$ local Langlands correspondences

Let $B$ be the Borel subgroup of $G = \mathrm{GL}_2(\mathbb{Q}_p)$ consisting of the upper triangular elements, let $K = \mathrm{GL}_2(\mathbb{Z}_p) \subset G$, and let $Z$ be the center of $G$. Let $W$ be a finite-dimensional representation of the closed subgroup $KZ$ of $G$. By a locally algebraic map $KZ \to W$ we mean a map which on an open subgroup of $KZ$ is the restriction of a rational map on (the algebraic group) $KZ$, and we say that $W$ is locally algebraic if the map $h \in KZ \mapsto hw \in W$ is locally algebraic for all $w \in W$. For a locally algebraic finite-dimensional representation $W$ of $KZ$ we define the compact induction of $W$ by

$$\mathrm{ind}^G W := \big\{\text{locally algebraic } G \to W \;\big|\; f(hg) = hf(g) \text{ for all } h \in KZ \;\&\; \mathrm{supp}\, f \text{ is compact in } KZ\backslash G\big\}.$$

Suppose that the representation $W$ is over the field $\mathbb{F} \in \{\overline{\mathbb{Q}}_p, \overline{\mathbb{F}}_p\}$. For elements $g \in G$ and $w \in W$ let $g \bullet_{\mathbb{F}} w$ be the unique element of $\mathrm{ind}^G W$ that is supported on $KZg^{-1}$ and maps $g^{-1}$ to $w$. Since $KZ\backslash G$ is discrete, every element of $\mathrm{ind}^G W$ can be written as a finite linear combination of functions of the type $g \bullet_{\mathbb{F}} w$. It is easy to check that

$$g_1(g_2 \bullet_{\mathbb{F}} (hw)) = (g_1 g_2 h) \bullet_{\mathbb{F}} w.$$

We define

$$\xi \bullet_{\mathbb{F}} w = \xi(\mathrm{id} \bullet_{\mathbb{F}} w)$$

for $\xi \in \mathbb{F}$. Let $\mu_x$ be the unramified character of the Weil group that sends the geometric Frobenius to $x$, and let $|\,| : \mathbb{Q}_p^\times \to \mathbb{Q}_p^\times \hookrightarrow \overline{\mathbb{Q}}_p^\times$ be the $p$-adic norm, so that $|x| = p^{-v_p(x)}$. We can view the symmetric power $\mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2)$ as the $G$-module of homogeneous polynomials in $x$ and $y$ of total degree $k-2$ with coefficients in $\overline{\mathbb{Q}}_p$, with $G$ acting by

$$\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \cdot v(x, y) = v(g_1 x + g_3 y, g_2 x + g_4 y)$$

for $\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in G$ and $v \in \mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2)$. Let

$$\widetilde{\Sigma}_{k-2} = \underline{\mathrm{Sym}}^{k-2}(\overline{\mathbb{Q}}_p^2) := \mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2) \otimes |\det|^{\frac{k-2}{2}}.$$

In particular, $\left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$ acts on $\mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2)$ as multiplication by $p^{k-2}$ and it acts on $\widetilde{\Sigma}_{k-2}$ trivially. If $R \in \{\overline{\mathbb{Z}}_p, \overline{\mathbb{F}}_p\}$, we can view the $KZ$-module $\underline{\mathrm{Sym}}^{k-2}(R^2)$ of homogeneous polynomials in $x$ and $y$ of total degree $k-2$ with coefficients in $R$, with $\left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$ acting trivially and $K$ acting by

$$\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \cdot v(x,y) = v(g_1x + g_3y, g_2x + g_4y)$$

for $\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in K$ and $v \in \underline{\mathrm{Sym}}^{k-2}(R^2)$. Let $\Sigma_{k-2}$ be the reduction of $\underline{\mathrm{Sym}}^{k-2}(\overline{\mathbb{Z}}_p^2)$ modulo $\mathfrak{m}$. Write $\lambda$ for one of the roots of $X^2 - aX + p^{k-1}$, so that the other root is $\lambda^{-1}p^{k-1}$. Let us consider the $\overline{\mathbb{Q}}_p$-representation

$$\pi = \mathrm{Ind}_B^G(\mu_{\lambda p^{1-k}} |\ |^{1/2} \times \mu_{\lambda^{-1}} |\ |^{-1/2}).$$

Here the Borel subgroup $B$ is seen as a parabolic subgroup of $G$ and $\mathrm{Ind}_B^G$ denotes parabolic induction (as opposed to $\mathrm{ind}^G$ which denotes compact induction). Let us fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. In Section 2.1 of [Bre03b], Breuil defines the Hecke operator $T \in \mathrm{End}_G(\mathrm{ind}^G \widetilde{\Sigma}_{k-2})$ corresponding to the double coset of $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and proves the explicit formula

$$T(\gamma \bullet_{\overline{\mathbb{Q}}_p} v) = \textstyle\sum_{\mu \in \mathbb{F}_p} \gamma\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1 \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \left(\left(\begin{smallmatrix} 1 & -[\mu] \\ 0 & p \end{smallmatrix}\right) \cdot v\right) + \gamma\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \left(\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot v\right),$$

where $[\xi]$ is the Teichmüller lift of $\xi \in \mathbb{F}_p$ to $\mathbb{Z}_p$. In Section 3.2 of the same article he defines the $\mathrm{GL}_2(\mathbb{Q}_p)$-representation

$$\Pi_{k,a} = \mathrm{ind}^G \widetilde{\Sigma}_{k-2}/(T-a),$$

proves that

$$\Pi_{k,a} \cong \mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2) \otimes |\det|^{-\frac{1}{2}} \otimes \pi, \tag{1}$$

and defines

$$\Theta_{k,a} = \mathrm{im}\left(\mathrm{ind}^G(\underline{\mathrm{Sym}}^{k-2}(\overline{\mathbb{Z}}_p^2)) \longrightarrow \Pi_{k,a}\right)$$

and

$$\overline{\Theta}_{k,a} = \Theta_{k,a} \otimes_{\overline{\mathbb{Z}}_p} \overline{\mathbb{F}}_p.$$

For $h \in \mathbb{Z}_{\geqslant 0}$ let us write $\sigma_h := \underline{\mathrm{Sym}}^h(\overline{\mathbb{F}}_p^2)$. For $t \in \{0, \dots, p-1\}$, $\lambda \in \overline{\mathbb{F}}_p$, and a character $\psi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$, let

$$\pi(t, \lambda, \psi) := (\mathrm{ind}^G \sigma_t/(T_\sigma - \lambda)) \otimes \psi,$$

where $T_\sigma \in \mathrm{End}_G(\mathrm{ind}^G \sigma_t)$ is the Hecke operator corresponding to the double coset of $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Let $\omega$ be the modulo $p$ reduction of the cyclotomic character. Let $\mathrm{ind}(\omega_2^{t+1})$ be the unique irreducible representation whose determinant is $\omega^{t+1}$ and that is equal to $\omega_2^{t+1} \oplus \omega_2^{p(t+1)}$ on inertia. Let $\overline{h} \in \{1, \dots, p-1\}$ and $\underline{h} \in \{0, \dots, p-2\}$ be the numbers in the corresponding sets that are congruent to $h$ modulo $p-1$.

In [Ber10], Berger proves the following correspondence between $\overline{V}_{k,a}$ and $\overline{\Theta}_{k,a}$, which was conjectured by Breuil (Conjecture 3.3.5 in [Bre03b]).[2]

Theorem 2. *There are $t \in \{0, \dots, p-1\}$ and $\psi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$ such that either*

$$\overline{\Theta}_{k,a} \cong \pi(t, 0, \psi)$$

*or*

$$\overline{\Theta}_{k,a}^{\mathrm{ss}} \cong \left(\pi(t, \lambda, \psi) \oplus \pi(\underline{p-3-t}, \lambda^{-1}, \omega^{t+1}\psi)\right)^{\mathrm{ss}}$$

*for some $\lambda \in \overline{\mathbb{F}}_p$. In the former case we have*

$$\overline{V}_{k,a} \cong \mathrm{ind}(\omega_2^{t+1}) \otimes \psi,$$

*and in the latter case we have*

$$\overline{V}_{k,a} \cong \left(\mu_\lambda \omega^{t+1} \oplus \mu_{\lambda^{-1}}\right) \otimes \psi.$$

Equation (1) implies that Berger's modulo $p$ correspondence is compatible with the $p$-adic local Langlands correspondence, which associates with $V_{k,a}$ a principal series representation. As $\overline{\Theta}_{k,a}$ has finite length as a $\overline{\mathbb{F}}_p[G]$-module, we have $\overline{\Theta}_{k,a}^{\mathrm{ss}} \cong \overline{\Pi}_{k,a}^{\mathrm{ss}}$ by Lemma 3.3.4 in [Bre03b], so we may replace $\Theta_{k,a}$ with $\Pi_{k,a}$ in Theorem 2. Theorem 2 implies that Theorem 1 can be rewritten in the following equivalent form.

Theorem 3. *If $v_p(a) \notin \mathbb{Z}$ and $\nu = \lceil v_p(a) \rceil$ is such that*

$$k \not\equiv 3, 4, \dots, 2\nu, 2\nu+1 \bmod p-1,$$

*then $\overline{\Theta}_{k,a}$ is irreducible.*

Thus the goal of the sections that follow is to prove Theorem 3.

## 4 Notation

For $\alpha \in \overline{\mathbb{Z}}_p$, let $\mathsf{O}(\alpha)$ denote the sub-$\overline{\mathbb{Z}}_p$-module

$$\alpha \,\mathrm{ind}^G\left(\underline{\mathrm{Sym}}^{k-2}(\overline{\mathbb{Z}}_p^2)\right) \subseteq \mathrm{ind}^G\left(\underline{\mathrm{Sym}}^{k-2}(\overline{\mathbb{Z}}_p^2)\right).$$

We abuse this notation and write $\mathsf{O}(\alpha)$ to represent a term $f \in \mathsf{O}(\alpha)$. Let

$$\mathscr{I}_a = \ker\left(\mathrm{ind}^G \Sigma_{k-2} \longrightarrow\!\!\!\!\!\rightarrow \overline{\Theta}_{k,a}\right).$$

[2] In fact, what Berger proves is a more general correspondence for so-called "trianguline" representations.

We use the shorthand "$\mathrm{im}(T-a)$" for the image of the map

$$T-a \in \mathrm{End}_G(\mathrm{ind}^G \widetilde{\Sigma}_{k-2}).$$

This image is a $G$-submodule of the $G$-module $\mathrm{ind}^G \widetilde{\Sigma}_{k-2}$. A crucial property of $\mathrm{im}(T-a)$ is that if an element of $\mathrm{ind}^G \Sigma_{k-2}$ is the reduction modulo $\mathfrak{m}$ of an integral element of $\mathrm{im}(T-a)$ then it is also in the "kernel" $\mathscr{I}_a$.

If $V$ is a $\overline{\mathbb{F}}_p[KZ]$-module, let $V(m)$ denote the twist $V \otimes \det^m$. For $h \in \mathbb{Z}$, let $I_h$ denote the $\overline{\mathbb{F}}_p[KZ]$-module of degree $h$ homogeneous functions $\mathbb{F}_p^2 \to \overline{\mathbb{F}}_p$ that vanish at the origin, with $\left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$ acting trivially and $K$ acting by

$$\left(\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) f\right)(x,y) = f(g_1 x + g_3 y, g_2 x + g_4 y)$$

for $\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in K$ and $f(x,y) \in I_h$. Note that if $h_1 \equiv h_2 \bmod p-1$ then $I_{h_1} \cong I_{h_2}$. Recall that, for $h \in \mathbb{Z}$,

$$\sigma_h = \underline{\mathrm{Sym}}^h(\overline{\mathbb{F}}_p^2).$$

Then $\sigma_{\overline{h}} \subset I_h$, since any element of $\sigma_{\overline{h}}$ is also a function $\mathbb{F}_p^2 \to \overline{\mathbb{F}}_p$ which is homogeneous of degree $h$ and vanishes at the origin, and the actions of $KZ$ on $\sigma_{\overline{h}}$ and $I_h$ match. Due to Lemma 3.2 in [AS86], there is a map

$$f \in I_h \longmapsto \textstyle\sum_{u,v} f(u,v)(vX-uY)^{\underline{-h}} \in \sigma_{\underline{-h}}(h), \tag{2}$$

which gives an isomorphism

$$I_h/\sigma_{\overline{h}} \cong \sigma_{\underline{-h}}(h),$$

and therefore the only two factors of $I_h$ are $\sigma_{\overline{h}}$ ("the submodule") and $\sigma_{\underline{-h}}(h)$ ("the quotient"). If $\overline{h} \neq p-1$, then $\sigma_{\underline{-h}}(h)$ is not a submodule of $I_h$. This is because the actions of $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ on $\sigma_{\underline{-h}}(h)$ and $I_h$ do not match. Hence in this case $\sigma_{\overline{h}}$ is the only submodule of $I_h$. If, on the other hand, $\overline{h} = p-1$, then $\sigma_{\underline{-h}}(h) = \sigma_0$ is also a submodule of $I_h = I_0$: the submodule of those functions that are equal to a constant everywhere except (possibly) at the origin.

If $A \subseteq B \subseteq \mathrm{ind}^G \Sigma_r$, we say that an element $x \in \mathrm{ind}^G \Sigma_r$ represents an element $y \in B/A$ if $x \in B$ and $x + A = y \in B/A$. Let

$$\theta := xy^p - x^p y, \qquad r := k-2 \geqslant 0, \qquad s := \overline{r},$$

and for a polynomial $f$ with coefficients in $\overline{\mathbb{Z}}_p$ let $\overline{f}$ denote its reduction modulo $\mathfrak{m}$. Suppose that $r \geqslant \nu(p+1)$. If $\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in K$, then $\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right)\overline{\theta} = (g_1 g_4 - g_2 g_3)\overline{\theta}$, and therefore there is a filtration of submodules

$$\Sigma_r \supset \overline{\theta}\Sigma_{r-p-1} \supset \cdots \supset \overline{\theta}^{\alpha}\Sigma_{r-\alpha(p+1)} \supset \cdots$$

For $\alpha \in \{0, \ldots, \nu-1\}$ let

$$N_\alpha = \overline{\theta}^{\alpha}\Sigma_{r-\alpha(p+1)}/\overline{\theta}^{\alpha+1}\Sigma_{r-(\alpha+1)(p+1)} \cong I_{r-2\alpha}(\alpha).$$

These are the first $\nu$ subquotients of the filtration. This filtration corresponds to a filtration

$$\operatorname{ind}^G \Sigma_r \supset \operatorname{ind}^G(\overline{\theta}\Sigma_{r-p-1}) \supset \cdots \supset \operatorname{ind}^G(\overline{\theta}^{\alpha}\Sigma_{r-\alpha(p+1)}) \supset \cdots$$

of $\operatorname{ind}^G \Sigma_r$, which has corresponding subquotients $(\widehat{N}_\alpha)_{0\leqslant\alpha<\nu}$. Since

$$\overline{\Theta}_{k,a} \cong \operatorname{ind}^G \Sigma_r/\mathscr{I}_a,$$

there is also a filtration

$$\overline{\Theta}_{k,a} = \overline{\Theta}_0 \supset \overline{\Theta}_1 \supset \cdots \supset \overline{\Theta}_\alpha \supset \cdots$$

whose first $\nu$ subquotients are quotients of $(\widehat{N}_\alpha)_{0\leqslant\alpha<\nu}$, i.e. if $\alpha \in \{0,\dots,\nu-1\}$ then there is a surjection

$$\widehat{N}_\alpha \twoheadrightarrow \overline{\Theta}_\alpha/\overline{\Theta}_{\alpha+1},$$

and the kernel of this surjection consists of those elements of the subquotient $\widehat{N}_\alpha$ of $\operatorname{ind}^G \Sigma_r$ that are represented by an element of $\mathscr{I}_a \subset \operatorname{ind}^G \Sigma_r$. In the proof of Theorem 1 we compute $\overline{\Theta}_{k,a}$ by finding elements in the kernels of these surjections and consequently obtaining data about the quotients $(\overline{\Theta}_\alpha/\overline{\Theta}_{\alpha+1})_{0\leqslant\alpha<\nu}$ of $(\widehat{N}_\alpha)_{0\leqslant\alpha<\nu}$. Therefore, the strategy of the proof is to find elements of $\mathscr{I}_a$ that represent non-trivial elements of the subquotients $(\widehat{N}_\alpha)_{0\leqslant\alpha<\nu}$.

For a property $P$ let us define $[P] = 1$ if $P$ is true and $[P] = 0$ if $P$ is false. Lemmas 4.1 and 4.3 and remark 4.4 in [BG09] imply that the ideal $\mathscr{I}_a$ contains $1 \bullet_{\overline{\mathbb{Q}}_p} x^j y^{r-j}$ for all $0 \leqslant j < \nu$ and $1 \bullet_{\overline{\mathbb{Q}}_p} \overline{\theta}^{\nu} h$ for all $h \in \Sigma_{r-\nu(p+1)}$, and thus $\overline{\Theta}_{k,a}$ is a subquotient of

$$\operatorname{ind}^G(\Sigma_r/\langle y^r,\dots,x^{\nu-1}y^{r-\nu+1},\overline{\theta}^{\nu}\Sigma_{r-\nu(p+1)}\rangle),$$

a module which has a series whose factors are subquotients of $\widehat{N}_0,\dots,\widehat{N}_{\nu-1}$. In particular, $\overline{\Theta}_\nu = 0$. For $\alpha \in \{0,\dots,\nu-1\}$ let us denote

$$\begin{aligned}\operatorname{sub}(\alpha) &= \sigma_{\overline{r-2\alpha}}(\alpha) \subset N_\alpha,\\ \operatorname{quot}(\alpha) &= N_\alpha/\sigma_{\overline{r-2\alpha}}(\alpha) \cong \sigma_{\underline{2\alpha-r}}(r-\alpha).\end{aligned}$$

We denote by $T, T_{\mathrm{q},\alpha}, T_{\mathrm{s},\alpha}$ the Hecke operators corresponding to the double coset of $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ on the modules $\operatorname{ind}^G \widetilde{\Sigma}_r, \operatorname{ind}^G \operatorname{quot}(\alpha), \operatorname{ind}^G \operatorname{sub}(\alpha)$, respectively.

## 5 Local constancy in the parameter $k$

The main theorem is true for $p = 3$ (this follows from Theorem 1.6 in [BG09]), so we may assume that $p \geqslant 5$. In particular, since we assume that $v_p(a) < \frac{p-1}{2}$ and $k \geqslant 2p+2$, and since $(4p+2)(p^2-3p+1) \geqslant 3(p-1)^3$ for $p \geqslant 5$, we can conclude that

$$k > 3v_p(a) + \tfrac{(k-1)p}{(p-1)^2} + 1.$$

Therefore Theorem B in [Ber12] implies that there is a constant $m = m(k, a)$ such that

$$\overline{V}_{k,a} \cong \overline{V}_{k',a}$$

whenever $k' \geqslant k$ and $k' \equiv k \bmod (p-1)p^m$. By using this isomorphism we can conclude that if the main theorem is true for $k > p^{100}$ then it is true for all $k$. Therefore in the remainder of this article we assume that $k > p^{100}$.

## 6 Combinatorial definitions

For a formal variable $X$ and $n \in \mathbb{Z}$ let us define

$$\binom{X}{n} := \frac{X_n}{n!} := \begin{cases} \frac{1}{n!}\prod_{j=0}^{n-1}(X-j) \in \mathbb{Q}_p[X] & \text{if } n \geqslant 0, \\ 0 \in \mathbb{Q}_p[X] & \text{if } n < 0. \end{cases}$$

Therefore

$$X_n = \prod_{j=0}^{n-1}(X-j) \in \mathbb{Z}_p[X]$$

denotes the falling factorial when $n \geqslant 0$. For $m \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$ let us define $\binom{m}{n} \in \mathbb{Q}_p$ as the evaluation of $\binom{X}{n}$ at $X = m \in \mathbb{Q}_p$. In particular, binomial coefficients with negative denominators are always zero. Let

$$\binom{X}{n}^{\partial} := \frac{\partial}{\partial X}\binom{X}{n} = \binom{X}{n}\sum_{j=0}^{n-1}\frac{1}{X-j} \in \mathbb{Q}_p[X].$$

For $m \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$ let us define $\binom{m}{n}^{\partial} \in \mathbb{Q}_p$ as the evaluation of $\binom{X}{n}^{\partial}$ at $X = m \in \mathbb{Q}_p$. If $\vartheta(X) \in \mathbb{Z}_p[X]$ then there is the Taylor series expansion

$$\vartheta(b+\epsilon) = \vartheta(b) + \epsilon\vartheta'(b) + \mathsf{O}\big(\epsilon^2\big)$$

for $b, \epsilon \in \mathbb{Z}_p$. Indeed, this follows from the facts that

$$(b+\epsilon)^m = b^m + \epsilon m b^{m-1} + \epsilon^2 \sum_{j=2}^{m}\binom{m}{j}\epsilon^{j-2}b^{m-j}$$

and

$$\sum_{j=2}^{m}\binom{m}{j}\epsilon^{j-2}b^{m-j} \in \mathbb{Z}_p$$

for $b, \epsilon \in \mathbb{Z}_p$ and $m \in \mathbb{Z}_{\geqslant 0}$. Since $p^{v_p(n!)}\binom{X}{n} \in \mathbb{Z}_p[X]$ for $n \in \mathbb{Z}_{\geqslant 0}$,

$$\binom{b+\epsilon}{n} = \binom{b}{n} + \epsilon\binom{b}{n}^{\partial} + \mathsf{O}\big(\epsilon^2 p^{-v_p(n!)}\big) \tag{3}$$

for $b, \epsilon \in \mathbb{Z}_p$ and $n \in \mathbb{Z}_{\geqslant 0}$. For $n, k \in \mathbb{Z}_{\geqslant 0}$ let us define the Stirling number of the first kind $s_1(n,k)$ as the coefficient of $X^k$ in $X_n = X \cdots (X-n+1)$. Therefore,

$$\left(\frac{s_1(i,j)}{i!}\right)_{0 \leqslant i,j \leqslant m} \cdot (1, \ldots, X^m)^T = \left(\binom{X}{0}, \ldots, \binom{X}{m}\right)^T.$$

Let us also define the Stirling number of the second kind $s_2(n,k)$ as the coefficient of $X_k$ in $X^n$, in the sense that

$$X^n = \sum_{k=0}^{n} s_2(n,k) X_k = \sum_{k=0}^{n} s_2(n,k) \prod_{j=0}^{k-1} (X-j).$$

In particular, $(s_2(i,j))_{0\leqslant i,j\leqslant m}$ is the inverse of $(s_1(i,j))_{0\leqslant i,j\leqslant m}$ and

$$(j! s_2(i,j))_{0\leqslant i,j\leqslant m} \cdot \left(\binom{X}{0}, \ldots, \binom{X}{m}\right)^T = (1, \ldots, X^m)^T.$$

For a family $(D_i)_{i\in\mathbb{Z}}$ of elements of $\mathbb{Z}_p$ supported on a finite set of indices, and for $w \in \mathbb{Z}$, let us define

$$\vartheta_w(D_\bullet) = \vartheta_w((D_i)_{i\in\mathbb{Z}}) = \sum_{i\in\mathbb{Z}} D_i \tbinom{i(p-1)}{w}.$$

Let us also define

$$\mathrm{S}_{u,n} = \sum_{i\in\mathbb{Z}} \tbinom{u}{i(p-1)+n}$$

for $u \in \mathbb{Z}_{\geqslant 0}$ and $n \in \mathbb{Z}$, and let $\mathrm{S}_u = \mathrm{S}_{u,0}$. We use the convention that when the range of summation is not specified, it is assumed to be over all of $\mathbb{Z}$, so that "$\sum_{m_1,\ldots,m_k}$" means "$\sum_{m_1\in\mathbb{Z}} \cdots \sum_{m_k\in\mathbb{Z}}$".

## 7 Table of assumptions and definitions

In this section we collate the assumptions, definitions, and notation we have introduced in a convenient table.

| | |
|---|---|
| $p$ | $p > 2$ is the prime. |
| $G, K, Z$ | $G = \mathrm{GL}_2(\mathbb{Q}_p)$, $K = \mathrm{GL}_2(\mathbb{Z}_p)$, and $Z$ is the center of $G$. |
| $\overline{h}$ | the number in $\{1, \dots, p-1\}$ congruent to $h$ modulo $p-1$. |
| $\underline{h}$ | the number in $\{0, \dots, p-2\}$ congruent to $h$ modulo $p-1$. |
| $k, r, s$ | $k$ is the weight and we assume $k > p^{100}$, $r = k-2$, and $s = \overline{r}$. |
| $a, \nu$ | $a$ is the eigenvalue and $\nu = \lceil v_p(a) \rceil \in \{1, \dots, \frac{p-1}{2}\}$. |
| $g \bullet_{\mathbb{F}} w$ | is in $\mathrm{ind}^G W$, is supported on $KZg^{-1}$, and maps $g^{-1} \mapsto w$. |
| $I_t$ | $\overline{\mathbb{F}}_p[KZ]$-module of degree $t$ maps $\mathbb{F}_p^2 \to \overline{\mathbb{F}}_p$ that vanish at $(0,0)$. |
| $\sigma_t$ | $\underline{\mathrm{Sym}}^t(\overline{\mathbb{F}}_p^2)$. |
| $V(m)$ | the twist $V \otimes \det^m$. |
| $\widetilde{\Sigma}_{k-2}$ | $\underline{\mathrm{Sym}}^{k-2}(\overline{\mathbb{Q}}_p^2) = \mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2) \otimes \lvert\det\rvert^{\frac{k-2}{2}}$. |
| $\Sigma_{k-2}$ | the reduction of $\underline{\mathrm{Sym}}^{k-2}(\overline{\mathbb{Z}}_p^2)$ modulo $\mathfrak{m}$. |
| $T$ | Hecke operator for the double coset of $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ on $\mathrm{ind}^G \widetilde{\Sigma}_{k-2}$. |
| $T_{\mathrm{q},\alpha}$ | Hecke operator for the double coset of $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ on $\mathrm{ind}^G \mathrm{quot}(\alpha)$. |
| $T_{\mathrm{s},\alpha}$ | Hecke operator for the double coset of $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ on $\mathrm{ind}^G \mathrm{sub}(\alpha)$. |
| $\mathsf{O}(\alpha)$ | sub-$\overline{\mathbb{Z}}_p$-module of multiples of $\alpha$; also used for $f \in \mathsf{O}(\alpha)$. |
| $\theta$ | $\theta = xy^p - x^p y$. |
| $N_\alpha$ | $N_\alpha = \overline{\theta}^\alpha \Sigma_{r-\alpha(p+1)} / \overline{\theta}^{\alpha+1} \Sigma_{r-(\alpha+1)(p+1)} \cong I_{r-2\alpha}(\alpha)$. |
| $\binom{X}{n}$ | $\binom{X}{n} = \frac{X \cdots (X-n+1)}{n!} \in \mathbb{Q}_p[X]$ for $n \geqslant 0$ and $\binom{X}{n} = 0$ otherwise. |
| $X_n$ | $X_n = n!\binom{X}{n} \in \mathbb{Q}_p[X]$ for $n \geqslant 0$ and $X_n = 0$ otherwise. |
| $\binom{X}{n}^\partial$ | $\binom{X}{n}^\partial = \frac{\partial}{\partial X}\binom{X}{n} = \binom{X}{n} \sum_{j=0}^{n-1} \frac{1}{X-j} \in \mathbb{Q}_p[X]$. |
| $\mathrm{S}_{u,n}$ | $\mathrm{S}_{u,n} = \sum_i \binom{u}{i(p-1)+n}$ for $u \geqslant 0$ and $n \in \mathbb{Z}$, and $\mathrm{S}_u = \mathrm{S}_{u,0}$. |
| $s_1(n,k)$ | the coefficient of $X^k$ in $X_n = X \cdots (X-n+1)$. |
| $s_2(n,k)$ | the coefficient of $X_k$ in $X^n$. |
| $\vartheta_w(D_\bullet)$ | $\vartheta_w(D_\bullet) = \vartheta_w((D_i)_{i\in\mathbb{Z}}) = \sum_{i\in\mathbb{Z}} D_i \binom{i(p-1)}{w}$. |
| $\mathscr{I}_a$ | the kernel of the quotient map $\mathrm{ind}^G \Sigma_{k-2} \twoheadrightarrow \overline{\Theta}_{k,a}$. |
| $[P]$ | $[P] = 1$ if $P$ is true, $[P] = 0$ if $P$ is false. |

## 8 Combinatorial identities

This section comprises nine lemmas about combinatorial identities involving binomial sums. The proofs of these nine lemmas are all standard. Therefore the reader may wish to skip this section on initial reading and refer back to it as required.

Recall that we use the convention that $\binom{X}{n} \in \mathbb{Q}_p[X]$ is a polynomial of degree $n$ if $n \geqslant 0$, and $\binom{X}{n} = 0 \in \mathbb{Q}_p[X]$ if $n < 0$. Moreover, $\binom{m}{n} \in \mathbb{Q}_p$ is the evaluation of $\binom{X}{n}$ at $X = m \in \mathbb{Q}_p$. In particular, we use the convention that binomial coefficients with negative denominators are always zero, which is in contrast with some of the literature. We also use the convention that when the range of summation is not specified, it is assumed to be over all of $\mathbb{Z}$, i.e. we define

$$\sum_{m_1,\ldots,m_k} F(m_1,\ldots,m_k) = \sum_{m_1\in\mathbb{Z}} \cdots \sum_{m_k\in\mathbb{Z}} F(m_1,\ldots,m_k).$$

This never gives rise to convergence issues as $F(m_1,\ldots,m_k)$ is supported on a finite subset of $\mathbb{Z}^k$ whenever such a sum appears in this article.

### 8.1 A formula for $\binom{m}{n}^{\partial}$ when $0 \leqslant m < n$

In general, the derivative of the binomial coefficient is difficult to compute as its formula involves the harmonic numbers. There is a closed formula in one special case, however, given by the following lemma.

Lemma 4. *Suppose that $m, n \in \mathbb{Z}_{\geqslant 0}$ are such that $m < n$. Then*

$$\binom{m}{n}^{\partial} = \frac{(-1)^{m+n+1}}{n\binom{n-1}{m}} = \frac{(-1)^{m+n+1}}{(m+1)\binom{n}{m+1}}.$$

*Proof.* For $j \in \{0,\ldots,n-1\}$, let $f_{n,j} \in \mathbb{Z}_p[X]$ denote the polynomial

$$f_{n,j}(X) = \prod_{i\in\{0,\ldots,n-1\}\setminus\{j\}} (X-i),$$

so that

$$\binom{m}{n}^{\partial} = \tfrac{1}{n!} \sum_{j=0}^{n-1} f_{n,j}(m).$$

If $j \neq m$, then $X - m \mid f_{n,j}$ and therefore $f_{n,j}(m) = 0$, so in fact

$$\binom{m}{n}^{\partial} = \frac{f_{n,m}(m)}{n!} = \frac{(-1)^{n-m-1} m!(n-m-1)!}{n!} = \frac{(-1)^{m+n+1}}{n\binom{n-1}{m}} = \frac{(-1)^{m+n+1}}{(m+1)\binom{n}{m+1}}.$$

□

### 8.2 Combinatorial identities involving binomial sums

In this subsection we prove four lemmas about generic identities between binomial sums.

Lemma 5 (Properties of $\mathrm{S}_{u,n}$). *Suppose throughout this lemma that*

$$n, t \in \mathbb{Z}, \qquad b, d, k, l, w \in \mathbb{Z}_{\geqslant 0}, \qquad m, u, v \in \mathbb{Z}_{\geqslant 1}.$$

1. *If* $u \equiv v \bmod (p-1)p^{m-1}$ *then*

$$\mathrm{S}_{u,n} \equiv \mathrm{S}_{v,n} \bmod p^m. \tag{c-a}$$

2. *Suppose that* $u = t_u(p-1) + s_u$ *with* $s_u = \overline{u}$*, so that* $s_u \in \{1, \dots, p-1\}$ *and* $t_u \in \mathbb{Z}_{\geqslant 0}$*. Then*

$$\mathrm{S}_u = 1 + [u \equiv_{p-1} 0] + \tfrac{t_u}{s_u} p + \mathsf{O}\big(t_u p^2\big). \tag{c-b}$$

3. *If* $n \leqslant 0$ *then*

$$\mathrm{S}_{u,n} = \textstyle\sum_{i=0}^{-n} (-1)^i \binom{-n}{i} \mathrm{S}_{u-n-i}. \tag{c-c}$$

4. *If* $n \geqslant 0$ *then*

$$\mathrm{S}_{u,n} \equiv (1 + [u \equiv_{p-1} n \equiv_{p-1} 0]) \tbinom{\overline{u}}{\underline{n}} \bmod p. \tag{c-d}$$

5. *If* $X$ *is a formal variable then*

$$\tbinom{X}{t+l} \tbinom{t}{w} = \textstyle\sum_v \tbinom{-l}{w-v} \tbinom{X}{v} \tbinom{X-v}{t+l-v}. \tag{c-e}$$

*Consequently, if* $b + l \geqslant d + w$ *then*

$$\textstyle\sum_i \tbinom{b-d+l}{i(p-1)+l} \tbinom{i(p-1)}{w} = \sum_v \tbinom{-l}{w-v} \tbinom{b-d+l}{v} \mathrm{S}_{b-d+l-v,l-v}. \tag{c-f}$$

*Proof.* 1. We can rewrite $\mathrm{S}_{u,n}$ by using the equation

$$\mathrm{S}_{u,n} = \tfrac{1}{p-1} \textstyle\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^{-n} (1 + [\mu])^u.$$

This is because

$$\textstyle\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^\lambda = \begin{cases} p-1 & \text{if } p-1 \mid \lambda, \\ 0 & \text{otherwise.} \end{cases}$$

Since $1 + [\mu] \in \{0\} \cup \mathbb{Z}_p^\times$ for all $\mu \in \mathbb{F}_p$ (as $p$ is odd), we have

$$(1 + [\mu])^u \equiv (1 + [\mu])^v \bmod p^m$$

for all $\mu \in \mathbb{F}_p$ (because $|(\mathbb{Z}/p^m\mathbb{Z})^\times|$ divides $u - v$ and $u, v > 0$). Therefore $\mathrm{S}_{u,n} \equiv \mathrm{S}_{v,n} \bmod p^m$.

2. For $\mu \in \mathbb{F}_p \backslash \{-1, 0\}$ let us define

$$x_\mu = \tfrac{(1+[\mu])^{p-1}-1}{p} \in \mathbb{Z}_p.$$

Then $\mathrm{S}_u$ is equal to

$$1 + [s_u = p-1] + \tfrac{1}{p-1} \textstyle\sum_{\mu \in \mathbb{F}_p \backslash \{-1,0\}} (1+[\mu])^{s_u} \sum_{j=1}^{t_u} \binom{t_u}{j} p^j x_\mu^j.$$

It is easy to show that

$$\tbinom{t_u}{j} p^j = \mathsf{O}\big(t_u p^2\big)$$

for $j > 1$ by writing

$$v_p\left(\tbinom{t_u}{j} p^j\right) \geqslant v_p(t_u) + j - \textstyle\sum_{i \geqslant 1} \lfloor j p^{-i} \rfloor$$

and verifying that the right side is at least $v_p(t_u p^2)$ for $j \in \{2, 3\}$ and at least $v_p(t_u) + \frac{p-2}{p-1} j \geqslant v_p(t_u p^2)$ for $j \geqslant 4$. This implies that if

$$A_{s_u} = \tfrac{1}{p-1} \textstyle\sum_{\mu \in \mathbb{F}_p \backslash \{-1,0\}} (1+[\mu])^{s_u} x_\mu$$

then

$$\mathrm{S}_u = 1 + [s_u = p-1] + A_{s_u} t_u p + \mathsf{O}\big(t_u p^2\big).$$

Moreover, the constant $A_{s_u}$ is independent of $t_u$. For $t_u = 1$ we have

$$\begin{aligned} \mathrm{S}_{s_u+p-1} &= 1 + [s_u = p-1] + \tbinom{s_u+p-1}{p-1} \\ &= 1 + [s_u = p-1] + \tbinom{s_u-1}{p-1} + p\tbinom{s_u-1}{p-1}^{\partial} + \mathsf{O}\big(p^2\big) \\ &= 1 + [s_u = p-1] + p\tbinom{s_u-1}{p-1}^{\partial} + \mathsf{O}\big(p^2\big). \end{aligned}$$

The second equality follows from Equation (3), and the third equality follows from the fact that $s_u - 1 \in \{0, \ldots, p-2\}$. Thus, due to Lemma 4,

$$A_{s_u} = \tbinom{s_u-1}{p-1}^{\partial} + \mathsf{O}(p) = \tfrac{(-1)^{s_u}}{s_u \binom{p-1}{s_u}} + \mathsf{O}(p) = \tfrac{1}{s_u} + \mathsf{O}(p).$$

3. This follows from repeated application of Pascal's triangle equation

$$\mathrm{S}_{u,v} = \mathrm{S}_{u-1,v} + \mathrm{S}_{u-1,v-1},$$

which is true for $u, v \geqslant 1$. We omit the full details.

4. This follows from the congruence

$$\mathrm{S}_{u,n} \equiv -\textstyle\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^{-n} (1+[\mu])^u \equiv -\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^{-\underline{n}} (1+[\mu])^{\overline{u}} \bmod p.$$

5. We can use

$$\tbinom{X}{v}\tbinom{X-v}{t+l-v} = \tbinom{X}{t+l}\tbinom{t+l}{v}$$

to rewrite Equation (c-e) as

$$\tbinom{X}{t+l}\tbinom{t}{w} = \tbinom{X}{t+l}\sum_v \tbinom{-l}{w-v}\tbinom{t+l}{v},$$

which follows from Vandermonde's convolution formula[3]. In particular, if we apply Equation (c-e) to $X = b-d+l$ and $t = i(p-1)$, we get

$$\tbinom{b-d+l}{i(p-1)+l}\tbinom{i(p-1)}{w} = \sum_v \tbinom{-l}{w-v}\tbinom{b-d+l}{v}\tbinom{b-d+l-v}{i(p-1)+l-v}.$$

Then we get Equation (c-f) by summing over all $i \in \mathbb{Z}$.

□

LEMMA 6. *Suppose throughout this lemma that*

$$y \in \mathbb{Z}, \qquad b, d, l, w \in \mathbb{Z}_{\geqslant 0}, \qquad u \in \mathbb{Z}_{\geqslant 1}.$$

1. *We have*

$$\sum_j (-1)^{b+j}\tbinom{j}{y}\tbinom{b}{j} = [y = b]. \tag{c-g}$$

2. *We have*

$$\sum_j (-1)^{j}\tbinom{y}{j}\tbinom{y+l-j}{w-j} = \tbinom{l}{w}. \tag{c-h}$$

3. *We have*

$$\sum_j \tbinom{u-1}{j-1}\tbinom{-l}{j-w} = (-1)^{u-w}\tbinom{l-w}{u-w}. \tag{c-i}$$

4. *We have*

$$\sum_j (-1)^{j}\tbinom{l}{j-b}\tbinom{j}{w} = (-1)^{b+l}\tbinom{b}{w-l}. \tag{c-j}$$

5. *If $u \geqslant (b+l)d$ and $l \geqslant w$ then*

$$\sum_j (-1)^{j-b}\tbinom{l}{j-b}\tbinom{u-dj}{w} = [w = l]d^l. \tag{c-k}$$

*Proof.* 1. We have

$$\begin{aligned}\sum_j (-1)^{b+j}\tbinom{j}{y}\tbinom{b}{j} &= \sum_j (-1)^{b+j}\tbinom{j}{j-y}\tbinom{b}{b-j}\\ &= \sum_j (-1)^{b-y}\tbinom{-y-1}{j-y}\tbinom{b}{b-j}\\ &= (-1)^{b-y}\tbinom{b-y-1}{b-y} = [y = b].\end{aligned}$$

The third equality follows from Vandermonde's convolution formula.

[3]Vandermonde's convolution formula is the fact that, for all $A, B, C \in \mathbb{Z}$,

$$\sum_v \tbinom{A}{v}\tbinom{B}{C-v} = \tbinom{A+B}{C}.$$

2. Since
$$(-1)^j\tbinom{y+l-j}{w-j} = (-1)^w\tbinom{w-y-l-1}{w-j} \text{ and } (-1)^w\tbinom{w-l-1}{w} = \tbinom{l}{w},$$
this follows from Vandermonde's convolution formula.

3. Since
$$\tbinom{u-1}{j-1} = \tbinom{u-1}{u-j} \text{ and } \tbinom{u-l-1}{u-w} = (-1)^{u-w}\tbinom{l-w}{u-w},$$
this follows from Vandermonde's convolution formula.

4. We have
$$\begin{aligned}\textstyle\sum_j(-1)^j\tbinom{l}{j-b}\tbinom{j}{w} &= \textstyle\sum_j(-1)^j\tbinom{l}{j-b}\sum_v\tbinom{j-b}{v}\tbinom{b}{w-v}\\ &= \textstyle\sum_v\tbinom{b}{w-v}\sum_j(-1)^j\tbinom{j-b}{v}\tbinom{l}{j-b}\\ &= \textstyle\sum_v[v=l](-1)^{b+l}\tbinom{b}{w-v} = (-1)^{b+l}\tbinom{b}{w-l}.\end{aligned}$$
The first equality follows from Vandermonde's convolution formula, the second equality is a simple rearrangement of the sums "$\sum_j$" and "$\sum_v$", and the third equality follows from Equation (*c-g*).

5. Because the degree $w$ polynomial $\binom{u-dX}{w}$ is a linear combination of the polynomials $\binom{X}{0},\dots,\binom{X}{w}$, we have
$$\tbinom{u-dj}{w} = (-d)^w\tbinom{j}{w} + h_{w-1}\tbinom{j}{w-1} + \cdots + h_0\tbinom{j}{0}$$
for some $h_{w-1},\dots,h_0\in\mathbb{Z}_p$ that depend on $u,d,w$. The claim follows from the facts that, due to Equation (*c-j*),
$$\textstyle\sum_j(-1)^{j-b}\tbinom{l}{j-b}\tbinom{j}{w-m} = (-1)^l\tbinom{b}{w-m-l} = 0$$
for all $m\in\{1,\dots,w\}$ (since $l\geqslant w$), and
$$\textstyle\sum_j(-1)^{j-b}\tbinom{l}{j-b}\tbinom{j}{w} = (-1)^l\tbinom{b}{w-l} = [w=l](-1)^l.$$

□

Lemma 7. *Let $\alpha\in\mathbb{Z}\cap[0,\dots,\frac{r}{p+1}]$ and let $(D_i)_{i\in\mathbb{Z}}$ be a family of elements of $\mathbb{Z}_p$ such that $D_i=0$ for $i\notin[0,\frac{r-\alpha}{p-1}]$ and $\vartheta_w(D_\bullet)=0$ for all $w\in\{0,\dots,\alpha-1\}$. Then the polynomial*
$$\textstyle\sum_i D_i x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\in\widetilde{\Sigma}_r$$
*can be written in the form $\theta^\alpha h$ for some polynomial $h$ with integer coefficients.*

*Proof.* The $\mathbb{Q}_p$-span of
$$\left\{\tbinom{(p-1)X}{0},\dots,\tbinom{(p-1)X}{\alpha-1}\right\}$$

is the same as the $\mathbb{Q}_p$-span of

$$\left\{\tbinom{X}{0}, \ldots, \tbinom{X}{\alpha-1}\right\}.$$

Note that here we do not put a restriction on the size of $\alpha$, and in particular $\alpha$ may be larger than $p$: the polynomials $\binom{(p-1)X}{j}$ and $\binom{X}{j}$ are in $\mathbb{Q}_p[X]$ (and not necessarily in $\mathbb{Z}_p[X]$) and by the "$\mathbb{Q}_p$-span" we mean the corresponding $\mathbb{Q}_p$-vector subspace of $\mathbb{Q}_p[X]$. Thus the condition that $\vartheta_w(D_\bullet) = 0$ for all $w \in \{0, \ldots, \alpha-1\}$ is equivalent to

$$\textstyle\sum_i D_i \binom{i}{w} = 0$$

for all $w \in \{0, \ldots, \alpha-1\}$. The coefficients of $\theta^\alpha h$ for any polynomial $h$ (which has degree $r - \alpha(p+1)$) satisfy this set of $\alpha$ equations. We can find an $h$ such that

$$\textstyle\sum_i D_i x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} = \theta^\alpha h + \sum_i D'_i x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha}$$

and $D'_i = 0$ if $i \notin \{0, \ldots, \alpha-2\}$. Since the matrix

$$\det\left(\tbinom{i}{w}\right)_{0 \leqslant i,w < \alpha}$$

is lower triangular with 1's on the diagonal, it has full rank, and therefore we have a set of $\alpha - 1$ constants $D'_0, \ldots, D'_{\alpha-2}$ that satisfy $\alpha$ independent linear equations, so all of them must be zero. Hence

$$\textstyle\sum_i D_i x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} = \theta^\alpha h.$$

Moreover, $\theta^\alpha h$ must be integral since the coefficients $(D_i)_{i\in\mathbb{Z}}$ are integers. It is easy to prove that "$\theta g$ is integral" $\Longrightarrow$ "$g$ is integral", implying by induction that $h$ is integral as well. □

Lemma 8. *For $u, v, c \in \mathbb{Z}$ let us define*

$$F_{u,v,c}(X) = \textstyle\sum_w (-1)^{w-c} \binom{w}{c} \binom{X}{w}^{\partial} \binom{X+u-w}{v-w} \in \mathbb{Q}_p[X].$$

*Then*

$$F_{u,v,c}(X) = \tbinom{u}{v-c} \tbinom{X}{c}^{\partial} - \tbinom{u}{v-c}^{\partial} \tbinom{X}{c}.$$

*Proof.* If $c < 0$ or $v < c$ then the claim is trivial. Let $v \geqslant c \geqslant 0$. It is enough to show that $\Phi'(0) = 0$ for

$$\Phi(z) = \textstyle\sum_w (-1)^{w-c} \binom{w}{c} \binom{z+X}{w} \binom{X+u-w}{v-w} - \binom{z+X}{c} \binom{u-z}{v-c} \in \mathbb{Q}_p[X][z].$$

In fact, $\Phi(z)$ is the zero polynomial (over $\mathbb{Q}_p[X]$) as can be seen from

$$\begin{aligned}\textstyle\sum_w (-1)^{w-c} \binom{w}{c} \binom{z+X}{w} \binom{X+u-w}{v-w} &= (-1)^{v-c} \binom{z+X}{c} \textstyle\sum_w \binom{z+X-c}{w-c} \binom{v-u-X-1}{v-w} \\ &= (-1)^{v-c} \binom{z+X}{c} \binom{z+v-u-c-1}{v-c} \\ &= \binom{z+X}{c} \binom{u-z}{v-c}.\end{aligned}$$

Here the first equality is a simple rewrite, i.e. we use the equations

$$\binom{w}{c}\binom{z+X}{w} = \binom{z+X}{c}\binom{z+X-c}{w-c} \text{ and } \binom{X+u-w}{v-w} = (-1)^{v-w}\binom{v-u-X-1}{v-w}.$$

The second equality follows from Vandermonde's convolution formula, and the third equality is a simple rewrite as well. □

### 8.3 Combinatorial identities involving Stirling numbers

In this subsection we prove two lemmas about Stirling numbers. The reason Stirling numbers appear in the proof is because they encode the change of basis of $\mathbb{Q}_p[X]$ from powers $\{1, X, X^2, \ldots\}$ to falling factorials $\{1, X_1, X_2, \ldots\}$.

Lemma 9. *For $\alpha, \mu \in \mathbb{Z}_{\geqslant 0}$ and $\lambda \in \mathbb{Z}_{\geqslant 1}$ let $L_\alpha(\lambda, \mu)$ be the $(\alpha+1)\times(\alpha+1)$ matrix with entries indexed by $0 \leqslant l, j \leqslant \alpha$ and defined by*

$$(L_\alpha(\lambda,\mu))_{l,j} = \sum_{k=0}^{\alpha} \frac{j!}{l!}\left(\frac{\mu}{\lambda}\right)^k s_1(l,k)s_2(k,j),$$

*where $s_1(l,k)$ and $s_2(k,j)$ are the Stirling numbers of the first and second kind, respectively (see section 7). Then*

$$L_\alpha(\lambda,\mu)\left(\binom{\lambda X}{0},\ldots,\binom{\lambda X}{\alpha}\right)^T = \left(\binom{\mu X}{0},\ldots,\binom{\mu X}{\alpha}\right)^T.$$

*Proof.* Straight from the definitions of $s_1(n,k)$ and $s_2(n,k)$ we have

$$\left(\frac{\mu^j s_1(i,j)}{i!}\right)_{0\leqslant i,j\leqslant\alpha} \cdot (1,\ldots,X^\alpha)^T = \left(\binom{\mu X}{0},\ldots,\binom{\mu X}{\alpha}\right)^T$$

and

$$\left(\frac{j!s_2(i,j)}{\lambda^i}\right)_{0\leqslant i,j\leqslant\alpha} \cdot \left(\binom{\lambda X}{0},\ldots,\binom{\lambda X}{\alpha}\right)^T = (1,\ldots,X^\alpha)^T.$$

The claim then follows from the fact that

$$L_\alpha(\lambda,\mu) = \left(\frac{\mu^j s_1(i,j)}{i!}\right)_{0\leqslant i,j\leqslant\alpha} \cdot \left(\frac{j!s_2(i,j)}{\lambda^i}\right)_{0\leqslant i,j\leqslant\alpha}.$$

□

Lemma 10. *For $\alpha \in \mathbb{Z}_{\geqslant 0}$ let $B_\alpha$ be the $(\alpha+1)\times(\alpha+1)$ matrix with entries indexed by $0 \leqslant i, j \leqslant \alpha$ and defined by*

$$(B_\alpha)_{i,j} = j!\sum_{k,l=0}^{\alpha} \frac{(-1)^{i+l+k}}{l!}\binom{l}{i}(1-p)^{-k}s_1(l,k)s_2(k,j),$$

*where $s_1(l,k)$ and $s_2(k,j)$ are the Stirling numbers of the first and second kind, respectively (see section 7). Let $\{X_{i,j}\}_{i,j\geqslant 0}$ be a family of formal variables. For*

*$\beta \in \{0, \dots, \alpha\}$ let $S(\alpha, \beta)$ be the $(\alpha+1) \times (\alpha+1)$ matrix with entries indexed by $0 \leqslant w, j \leqslant \alpha$ and defined by*

$$S(\alpha, \beta)_{w,j} = \sum_{i=1}^{\beta} X_{i,j} \tbinom{i(p-1)}{w}.$$

*Then the matrix $B_\alpha S(\alpha, \beta)$ is zero outside the rows indexed by $1, \dots, \beta$ and*

$$(B_\alpha S(\alpha, \beta))_{i,j} = X_{i,j}$$

*for $i \in \{1, \dots, \beta\}$.*

*Proof.* Let $L = L_\alpha(p-1, 1)$ be the matrix defined in Lemma 9. Then it follows from Lemma 9 that

$$(LS(\alpha, \beta))_{l,j} = \sum_{w=1}^{\beta} X_{w,j} \tbinom{w}{l}.$$

Let $E = \left(\tbinom{w}{l}\right)_{0 \leqslant l, w \leqslant \alpha}$, so that $E^{-1} = ((-1)^{i+l} \tbinom{l}{i})_{0 \leqslant i, l \leqslant \alpha}$ and hence

$$B_\alpha = E^{-1} L.$$

Then

$$\begin{aligned}
(B_\alpha S(\alpha, \beta))_{i,j} &= \sum_{l=0}^{\alpha} (E^{-1})_{i,l} (LS(\alpha, \beta))_{l,j} \\
&= \sum_{l=0}^{\alpha} (-1)^{i+l} \tbinom{l}{i} \sum_{w=1}^{\beta} X_{w,j} \tbinom{w}{l} \\
&= \sum_{w=1}^{\beta} X_{w,j} \sum_{l=0}^{\alpha} (-1)^{i+l} \tbinom{l}{i} \tbinom{w}{l} \\
&= \sum_{w=1}^{\beta} [w = i] X_{w,j} = [i \in \{1, \dots, \beta\}] X_{i,j}.
\end{aligned}$$

The fourth equality follows from Lemma 6, Equation (*c-g*). □

### 8.4 Two ad hoc combinatorial lemmas

The statements of the two lemmas in this subsection are specifically tailored to be applicable in the main proof. This is why they appear overly specific, and why their proofs are unfortunately necessarily somewhat long.

Lemma 11. *Let $\alpha \in \mathbb{Z}_{\geqslant 1}$, let $X$ and $Y$ be formal variables, and let*

$$c_j = (-1)^j \alpha! \left( \tfrac{X+j+1}{j+1} \tbinom{Y}{\alpha-j-1} + \tbinom{Y}{\alpha-j} \right) \in \mathbb{Q}[X, Y] \subset \mathbb{Q}(X, Y)$$

*for $j \in \{1, \dots, \alpha\}$. Let $M$ be the $(\alpha+1) \times (\alpha+1)$ matrix over $\mathbb{Q}(X, Y)$ with entries indexed by $0 \leqslant w, j \leqslant \alpha$ and defined by*

$$\begin{aligned}
M_{w,0} &= (-1)^w \tfrac{(Y-X) X_w}{Y_{w+1}}, \\
M_{w,j} &= \sum_v \tbinom{-j}{w-v} \tbinom{X+j}{v} \left( \tbinom{Y+j-v}{j-v} - \tbinom{X+j-v}{j-v} \right),
\end{aligned}$$

*for $w \in \{0, \dots, \alpha\}$ and $j \in \{1, \dots, \alpha\}$. Let $c = (Y_\alpha, c_1, \dots, c_\alpha)^T$. Then the first $\alpha$ entries of*

$$Mc = (d_0, \dots, d_\alpha)^T$$

*are zero, and $d_\alpha = \frac{(Y-X)_{\alpha+1}}{Y-\alpha}$.*

*Proof.* First let us compute $d_0$. We have

$$\begin{aligned}
\tfrac{d_0}{\alpha!} &= \tfrac{Y-X}{Y}\binom{Y}{\alpha} + \textstyle\sum_{j=1}^{\alpha}(-1)^j \left(\tfrac{X+j+1}{j+1}\binom{Y}{\alpha-j-1} + \binom{Y}{\alpha-j}\right)\left(\binom{Y+j}{j} - \binom{X+j}{j}\right) \\
&= \tfrac{Y-X}{Y}\binom{Y}{\alpha} + (X+1)\binom{Y}{\alpha-1} + \textstyle\sum_{j=1}^{\alpha}(-1)^j \left(\tfrac{X+j+1}{j+1}\binom{\alpha-1}{j}\binom{Y+j}{\alpha-1} + \binom{\alpha}{j}\binom{Y+j}{\alpha}\right) \\
&= -\tfrac{X}{Y}\binom{Y}{\alpha} + \textstyle\sum_{j=0}^{\alpha}(-1)^j \left(\tfrac{X+j+1}{j+1}\binom{\alpha-1}{j}\binom{Y+j}{\alpha-1} + \binom{\alpha}{j}\binom{Y+j}{\alpha}\right) = 0.
\end{aligned}$$

The first equality follows directly from the definition of $d_0$. The second equality follows from telescoping the sum

$$\begin{aligned}
&\textstyle\sum_{j=1}^{\alpha}(-1)^j \left(\tfrac{X+j+1}{j+1}\binom{Y}{\alpha-j-1} + \binom{Y}{\alpha-j}\right)\binom{X+j}{j} \\
&\quad = \textstyle\sum_{j=1}^{\alpha}(-1)^j \left(\binom{X+j+1}{j+1}\binom{Y}{\alpha-j-1} + \binom{X+j}{j}\binom{Y}{\alpha-j}\right) \\
&\quad = \binom{X+\alpha+1}{\alpha+1}\binom{Y}{-1} - \binom{X+1}{1}\binom{Y}{\alpha-1}
\end{aligned}$$

and using the equation

$$\binom{Y}{\beta-j}\binom{Y+j}{j} = \binom{\beta}{j}\binom{Y+j}{\beta},$$

which is true for $\beta, j \in \mathbb{Z}_{\geqslant 0}$. The third equality follows from the fact that the "$j = 0$" term in the last sum is

$$(X+1)\binom{Y}{\alpha-1} + \binom{Y}{\alpha}.$$

Thus we have shown that $d_0 = 0$. Now let us suppose that $w \in \{1, \dots, \alpha\}$. If $j \in \{1, \dots, \alpha\}$ then it is clear that $M_{w,j}$ is a polynomial that belongs to the ideal generated by $Y - X$, and due to Lemma 5, Equation (*c-e*) we have

$$M_{w,j} = \textstyle\sum_v \binom{-j}{w-v}\binom{X+j}{v}\binom{Y+j-v}{j-v}.$$

We want to show that

$$(Y-\alpha)(Mc)_w = (Y-\alpha)d_w = [w=\alpha](Y-X)_{\alpha+1}.$$

Since $Y_{\alpha+1}M_{w,0}$ is a polynomial and $M_{w,j}$ is a polynomial for all $j \in \{1, \dots, \alpha\}$, it follows that $(Y-\alpha)(Mc)_w$ is also a polynomial. The degree of $(Y-\alpha)(Mc)_w$ is at most $\alpha+1$. Let us show that $(Y-\alpha)(Mc)_w$ belongs to the ideal generated by $Y - X - t$ for all $t \in \{0, \dots, \alpha\}$. If $t = 0$ then this is obvious (because $Y_{\alpha+1}M_{w,0}, M_{w,1}, \dots, M_{w,\alpha}$ all belong to the ideal generated by $Y - X$), so let

us suppose that $t \in \{1, \dots, \alpha\}$. In that case $(Mc)_w$ is a polynomial of degree at most $\alpha - 1$ in the quotient ring

$$\mathbb{Q}[X, Y]/(Y - X - t) \cong \mathbb{Q}[X] \cong \mathbb{Q}[Y].$$

(We can write an element of this quotient ring either as a polynomial in $X$ or as a polynomial in $Y$, and it will have the same degree in either variable.) By Lemma 5, Equation (*c-e*),

$$\begin{aligned}
M_{w,j} &= \textstyle\sum_v \binom{-j}{w-v}\binom{X+j}{v}\binom{X+t+j-v}{j-v} \\
&= \textstyle\sum_v \binom{-j}{w-v}\binom{X+j}{v}\sum_l \binom{X+j-v}{j-v-l}\binom{t}{l} \\
&= \textstyle\sum_l \binom{t}{l}\sum_v \binom{-j}{w-v}\binom{X+j}{v}\binom{X+j-v}{j-v-l} \\
&= \textstyle\sum_l \binom{t}{l}\binom{X+j}{j-l}\sum_v \binom{-j}{w-v}\binom{j-l}{v} \\
&= \textstyle\sum_l \binom{t}{l}\binom{X+j}{j-l}\binom{-l}{w} \\
&= (-1)^w \textstyle\sum_l \binom{t}{l}\binom{X+j}{j-l}\binom{w+l-1}{w}.
\end{aligned}$$

The second and fifth equalities follow from Vandermonde's convolution formula, the third equality is a simple rearrangement of the sums "$\sum_v$" and "$\sum_l$", the fourth equality follows from

$$\tbinom{X+j}{v}\tbinom{X+j-v}{j-v-l} = \tbinom{X+j}{j-l}\tbinom{j-l}{v},$$

and the sixth equality follows from $\binom{-l}{w} = (-1)^w\binom{w+l-1}{w}$. So

$$\tfrac{(-1)^w}{\alpha!}\textstyle\sum_{j=1}^{\alpha} M_{w,j}c_j$$

is equal to

$$\begin{aligned}
&\textstyle\sum_l \binom{t}{l}\binom{w+l-1}{w}\sum_{j>0}(-1)^j\binom{X+j}{j-l}\left(\frac{X+j+1}{j+1}\binom{X+t}{\alpha-j-1} + \binom{X+t}{\alpha-j}\right) \\
&\quad= \textstyle\sum_l \binom{t}{l}\binom{w+l-1}{w}\sum_{j>0}(-1)^j\left(\frac{j-l+1}{j+1}\binom{X+j+1}{j-l+1}\binom{X+t}{\alpha-j-1} + \binom{X+j}{j-l}\binom{X+t}{\alpha-j}\right) \\
&\quad= \textstyle\sum_l l\binom{t}{l}\binom{w+l-1}{w}\sum_{j>0}\frac{(-1)^j}{j}\binom{X+j}{j-l}\binom{X+t}{\alpha-j} \\
&\quad= \textstyle\sum_u\sum_l l\binom{t}{l}\binom{w+l-1}{w}\sum_{j>0}\frac{(-1)^j}{j}\binom{\alpha-j+u}{u}\binom{\alpha-t}{j-l-u}\binom{X+t}{\alpha-j+u} \\
&\quad= \textstyle\sum_u \binom{X+t}{u}\sum_l l\binom{t}{l}\binom{w+l-1}{w}\binom{\alpha-t}{\alpha-l-u}\sum_{j>0}\frac{(-1)^j}{j}\binom{u}{u-\alpha+j}.
\end{aligned}$$

Let us provide some justification for this string of equalities. The first equality is a simple rewrite. For the second equality we replace $j + 1$ with $j$ in the first term of the inner sum, i.e. we use the equation

$$\textstyle\sum_{j>0}(-1)^j\frac{j-l+1}{j+1}\binom{X+j+1}{j-l+1}\binom{X+t}{\alpha-j-1} = \sum_{j>1}(-1)^{j-1}\frac{j-l}{j}\binom{X+j}{j-l}\binom{X+t}{\alpha-j}$$

to rewrite

$$\begin{aligned}
&\textstyle\sum_{j>0}(-1)^j\left(\frac{j-l+1}{j+1}\binom{X+j+1}{j-l+1}\binom{X+t}{\alpha-j-1}+\binom{X+j}{j-l}\binom{X+t}{\alpha-j}\right)\\
&\quad=-\binom{X+1}{1-l}\binom{X+t}{\alpha-1}+\textstyle\sum_{j>1}(-1)^j\left(\frac{l-j}{j}+1\right)\binom{X+j}{j-l}\binom{X+t}{\alpha-j}\\
&\quad=(l-1)\binom{X+1}{1-l}\binom{X+t}{\alpha-1}+\textstyle\sum_{j>0}\frac{(-1)^j l}{j}\binom{X+j}{j-l}\binom{X+t}{\alpha-j}
\end{aligned}$$

The extra term $(l-1)\binom{X+1}{1-l}\binom{X+t}{\alpha-1}$ does not contribute to anything since

$$\textstyle\sum_l\binom{t}{l}\binom{w+l-1}{w}(l-1)\binom{X+1}{1-l}\binom{X+t}{\alpha-1}$$

is zero for $l<0$ (as then $\binom{t}{l}=0$), for $l=0$ (as then $\binom{w+l-1}{w}=0$), for $l=1$ (as then $l-1=0$), and for $l>1$ (as then $\binom{X+1}{1-l}=0$). For the third equality we use Vandermonde's convolution formula. To be more precise, we write

$$\begin{aligned}
\binom{X+j}{j-l}\binom{X+t}{\alpha-j}&=\textstyle\sum_u\binom{\alpha-t}{j-l-u}\binom{X+t-\alpha+j}{u}\binom{X+t}{\alpha-j}\\
&=\textstyle\sum_u\binom{\alpha-t}{j-l-u}\binom{\alpha-j+u}{u}\binom{X+t}{\alpha-j+u}.
\end{aligned}$$

Finally, for the fourth equality we simply change the variable $u$ to $u-\alpha+j$. Since the degree of the last polynomial

$$\textstyle\sum_u\binom{X+t}{u}\sum_l l\binom{t}{l}\binom{w+l-1}{w}\binom{\alpha-t}{\alpha-l-u}\sum_{j>0}\frac{(-1)^j}{j}\binom{u}{u-\alpha+j}$$

is at most $\alpha-1$, we can replace the sum $\sum_u$ with $\sum_{u=0}^{\alpha-1}$, and for $u$ in this range we have

$$\begin{aligned}
\textstyle\sum_{j>0}\frac{(-1)^j}{j}\binom{u}{u-\alpha+j}&=\textstyle\sum_j\frac{(-1)^{j+\alpha-u}}{j+\alpha-u}\binom{u}{j}\\
&=-\textstyle\sum_j\binom{0}{j+\alpha-u}^{\partial}\binom{u}{u-j}\\
&=-\textstyle\frac{\partial}{\partial X}\sum_j\binom{X}{j+\alpha-u}\binom{u}{u-j}\Big|_{X=0}\\
&=-\binom{X+u}{\alpha}^{\partial}\Big|_{X=0}\\
&=-\binom{u}{\alpha}^{\partial}\\
&=\textstyle\frac{(-1)^{\alpha-u}(\alpha-u-1)!u!}{\alpha!}.
\end{aligned}$$

The second and sixth equalities follow from Lemma 4, and the fourth equality follows from Vandermonde's convolution formula. Therefore

$$\textstyle\frac{(-1)^w}{\alpha!}\sum_{j=1}^{\alpha}M_{w,j}c_j=t\sum_{u,l}\binom{X+t}{u}\frac{(-1)^{\alpha-u}(\alpha-u-1)!u!}{\alpha!}\binom{t-1}{l-1}\binom{w+l-1}{w}\binom{\alpha-t}{\alpha-l-u}.$$

Thus the equation we want to show, i.e.

$$\textstyle\frac{(-1)^w}{\alpha!}(Mc)_w=\frac{(Y-X)X_w}{Y_{w+1}}\binom{Y}{\alpha}+\frac{(-1)^w}{\alpha!}\sum_{j=1}^{\alpha}M_{w,j}c_j=0$$

(modulo $Y - X - t$), is equivalent to

$$\sum_{u,l} \binom{Y}{u} \tfrac{(-1)^{\alpha-u-1}(\alpha-u-1)!u!}{\alpha!} \binom{t-1}{l-1} \binom{w+l-1}{w} \binom{\alpha-t}{\alpha-l-u} = \tfrac{(Y-t)_w}{Y_{w+1}} \binom{Y}{\alpha}. \tag{4}$$

Here for convenience we look at the relevant elements as polynomials in $Y$ (recall that we identify $\mathbb{Q}[X,Y]/(Y-X-t) \cong \mathbb{Q}[X] \cong \mathbb{Q}[Y]$). Let us denote the left and right side of Equation (4) by $L(t)$ and $R(t)$, respectively. To conclude that $L(t) = R(t)$ for $t \in \{1, \dots, \alpha\}$, it is evidently enough to show that

$$\sum_{j=0}^{m} (-1)^j \binom{m}{j} L(j+1) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} R(j+1) \tag{5}$$

for $m \in \{0, \dots, \alpha - 1\}$. We can uniquely write each side of Equation (5) in the form

$$h_{\alpha-1} \binom{Y}{\alpha-1} + \cdots + h_0 \binom{Y}{0}.$$

To show that the polynomials on the two sides of Equation 5 are equal, it is enough to show that the coefficients of $\binom{Y}{u}$ (i.e. the corresponding $h_u$) are the same on both sides, for all $u \in \{0, \dots, \alpha - 1\}$. The coefficient of $\binom{Y}{u}$ on the left side of Equation (5) is

$$\kappa_{\alpha,m,u}^{-1} \sum_{j,l} (-1)^{m+j} \binom{m}{j} \binom{j}{l-1} \binom{w+l-1}{w} \binom{\alpha-j-1}{l+u-j-1},$$

with $\kappa_{\alpha,m,u} = (-1)^{\alpha-m-u-1} \alpha \binom{\alpha-1}{u}$. We have

$$\begin{aligned}
\sum_j (-1)^j \binom{m}{j} R(j+1) &= \sum_j (-1)^j \binom{m}{j} \tfrac{(Y-j-1)_w}{Y_{w+1}} \binom{Y}{\alpha} \\
&= \tfrac{w!}{Y_{w+1}} \binom{Y}{\alpha} \sum_j (-1)^j \binom{m}{j} \binom{Y-j-1}{w} \\
&= \tfrac{w!}{Y_{w+1}} \binom{Y}{\alpha} \sum_j (-1)^{w+j} \binom{m}{j} \binom{w+j-Y}{w} \\
&= \tfrac{w!}{Y_{w+1}} \binom{Y}{\alpha} \sum_j (-1)^{w+j} \binom{m}{j} \sum_l \binom{j}{l} \binom{w-Y}{w-l} \\
&= \tfrac{w!}{Y_{w+1}} \binom{Y}{\alpha} \sum_l \binom{w-Y}{w-l} \sum_j (-1)^{w+j} \binom{m}{j} \binom{j}{l} \\
&= \tfrac{w!}{Y_{w+1}} \binom{Y}{\alpha} (-1)^{w+m} \sum_l [l = m] \binom{w-Y}{w-l} \\
&= \tfrac{w!}{Y_{w+1}} \binom{Y}{\alpha} \binom{Y-m-1}{w-m} \\
&= \tfrac{w_m}{\alpha_{m+1}} \binom{Y-m-1}{\alpha-m-1} \\
&= \sum_u \binom{Y}{u} \tfrac{w_m}{\alpha_{m+1}} \binom{-m-1}{\alpha-m-u-1} \\
&= \sum_u \binom{Y}{u} \tfrac{(-1)^{\alpha-m-u-1} w_m}{\alpha_{m+1}} \binom{\alpha-u-1}{m}.
\end{aligned}$$

Here the second, third, fifth, seventh, eighth, and tenth equalities are simple rewrites and rearrangements of sums, the fourth and ninth equalities follow from Vandermonde's convolution formula, and the sixth equality follows from Lemma 6, Equation (*c-g*). Therefore the coefficient of $\binom{Y}{u}$ on the right side of Equation (5) is

$$\kappa_{\alpha,m,u}^{-1} \alpha \binom{\alpha-1}{u} \tfrac{w_m}{\alpha_{m+1}} \binom{\alpha-u-1}{m} = \kappa_{\alpha,m,u}^{-1} \binom{\alpha-m-1}{u} \binom{w}{m}.$$

Thus we want to show that

$$\sum_{j,l}(-1)^{m+j}\binom{m}{j}\binom{j}{l-1}\binom{w+l-1}{w}\binom{\alpha-j-1}{l+u-j-1}=\binom{\alpha-m-1}{u}\binom{w}{m}. \tag{6}$$

Let us show that Equation (6) is true more generally for all $\alpha, m, u, w \in \mathbb{Z}_{\geqslant 0}$. Let $L(\alpha, u)$ and $R(\alpha, u)$ denote the left and right side of Equation (6), respectively. Then it is easy to verify that

$$\star(\alpha, u) = \star(\alpha-1, u) + \star(\alpha-1, u-1)$$

for $\star \in \{L, R\}$. Therefore we only need to show Equation (6) in the boundary cases, i.e. when either $u = 0$ or $\alpha = 0$. Suppose that $u = 0$. If $l \in \{0, \dots, j\}$ then $\binom{\alpha-j-1}{l-j-1} = 0$, and if $l \notin \{0, \dots, j+1\}$ then $\binom{j}{l-1} = 0$, so the only terms in $L(\alpha, 0)$ that are non-zero are the ones such that $l - 1 = j$. Thus, the equation is

$$\sum_j (-1)^{m+j}\binom{m}{j}\binom{w+j}{j} = \binom{w}{m}.$$

This follows from

$$\binom{w+j}{j} = (-1)^j\binom{-w-1}{j} \text{ and } \binom{w}{m} = (-1)^m\binom{m-w-1}{m}$$

and Vandermonde's convolution formula. If $\alpha = 0$ then the equation is

$$\sum_{j,l}(-1)^{m+l+1}\binom{m}{j}\binom{j}{l-1}\binom{w+l-1}{w}\binom{l+u-1}{j} = \binom{m+u}{u}\binom{w}{m},$$

which follows from the fact that

$$\sum_{w,m,u,j,l\geqslant 0}(-1)^{m+l+1}\binom{m}{j}\binom{j}{l-1}\binom{w+l-1}{w}\binom{l+u-1}{j} Z_1^w Z_2^m Z_3^u \in \mathbb{Q}(Z_1, Z_2, Z_3)$$

is equal to

$$\begin{aligned}
&\sum_{w,m,u,j,l\geqslant 0}(-1)^{l+1}\binom{m}{j}\binom{j}{l-1}\binom{-l}{w}\binom{l+u-1}{j}(-Z_1)^w(-Z_2)^m Z_3^u \\
&\quad = \sum_{w,m,u,j,l\geqslant 0}(-1)^{l+1}\binom{m}{j}\binom{j}{l-1}\binom{-l}{w}\binom{l+u-1}{j}(-Z_1)^w(-Z_2)^m Z_3^u \\
&\quad = -\sum_{m,u,j,l\geqslant 0}\binom{m}{j}\binom{j}{l-1}\binom{l+u-1}{j}(Z_1-1)^{-l}(-Z_2)^m Z_3^u \\
&\quad = -\tfrac{1}{1+Z_2}\sum_{u,j,l\geqslant 0}\binom{j}{l-1}\binom{l+u-1}{j}(Z_1-1)^{-l}\left(-\tfrac{Z_2}{1+Z_2}\right)^j Z_3^u \\
&\quad = -\tfrac{Z_3}{1+Z_2-Z_3-Z_2Z_3}\sum_{j,l\geqslant 0}\binom{j}{l-1}\left(-\tfrac{1}{Z_3-Z_1Z_3}\right)^l\left(-\tfrac{Z_2Z_3}{1+Z_2-Z_3-Z_2Z_3}\right)^j \\
&\quad = \tfrac{1}{(1-Z_1)(1+Z_2-Z_3-Z_2Z_3)}\sum_{j\geqslant 0}\left(\tfrac{(1-Z_3+Z_1Z_3)Z_2}{(1-Z_1)(1+Z_2-Z_3-Z_2Z_3)}\right)^j \\
&\quad = \tfrac{1}{1-Z_1-Z_3-Z_1Z_2+Z_1Z_3} \in \mathbb{Q}(Z_1, Z_2, Z_3)
\end{aligned}$$

and the fact that

$$\sum_{w,m,u\geqslant 0}\binom{m+u}{u}\binom{w}{m} Z_1^w Z_2^m Z_3^u \in \mathbb{Q}(Z_1, Z_2, Z_3)$$

is equal to

$$\begin{aligned}&\tfrac{1}{1-Z_1}\sum_{m,u\geqslant 0}\tbinom{m+u}{u}\left(\tfrac{Z_1Z_2}{1-Z_1}\right)^m Z_3^u\\&\quad=\tfrac{1}{1-Z_1-Z_1Z_2}\sum_{u\geqslant 0}\left(\tfrac{Z_3-Z_1Z_3}{1-Z_1-Z_1Z_2}\right)^u\\&\quad=\tfrac{1}{1-Z_1-Z_3-Z_1Z_2+Z_1Z_3}\in\mathbb{Q}(Z_1,Z_2,Z_3).\end{aligned}$$

To summarize, we have shown that $(Y-\alpha)d_w=(Y-\alpha)(Mc)_w$ has degree at most $\alpha+1$ and belongs to the ideal generated by $Y-X-t$ for all $t\in\{0,\dots,\alpha\}$. Therefore it must be a constant multiple of $(Y-X)_{\alpha+1}$. We can deduce that the constant is indeed $[w=\alpha]$ by comparing the coefficients of $Y^{\alpha+1}$, thus completing the proof. □

Lemma 12. *Suppose that $s,\alpha,\beta\in\mathbb{Z}$ are such that*

$$1\leqslant\beta\leqslant\alpha\leqslant\tfrac{s}{2}-2\leqslant\tfrac{p-5}{2}.$$

*Let $B=B_\alpha$ denote the matrix defined in Lemma 10. Let $M$ denote the $(\alpha+1)\times(\alpha+1)$ matrix with entries in $\mathbb{F}_p$ such that if $i\in\{1,\dots,\beta\}$ and $j\in\{0,\dots,\alpha\}$ then*

$$M_{i,j}=\tbinom{\beta}{i}\cdot\begin{cases}\binom{s-\alpha-\beta+i}{i}^{-1}(-1)^{i+1} & \text{if } j=0,\\ \binom{s-\alpha-\beta+j}{j-i} & \text{if } j>0,\end{cases}$$

*and if $i\in\{0,\dots,\alpha\}\backslash\{1,\dots,\beta\}$ and $j\in\{0,\dots,\alpha\}$ then $M_{i,j}$ is the reduction modulo $p$ of*

$$\begin{aligned}&p^{-[j=0]}\textstyle\sum_{w=0}^{\alpha}B_{i,w}\sum_v\binom{-j}{w-v}\binom{s+\beta(p-1)-\alpha+j}{v}^{\partial}\sum_{u=0}^{\beta}\binom{s+\beta(p-1)-\alpha+j-v}{u(p-1)+j-v}\\&\quad-[i=0]\tbinom{s+\beta(p-1)-\alpha+j}{j}^{\partial}-[j=0]\textstyle\sum_{w=0}^{\alpha}B_{i,w}\binom{s+\beta(p-1)-\alpha}{w}\frac{(-1)^w w!}{(s-\alpha)_{w+1}}.\end{aligned}$$

*Then there is a solution of*

$$M(z_0,\dots,z_\alpha)^T=(1,0,\dots,0)^T$$

*such that $z_0\neq 0$.*

*Proof.* Let us simplify $M_{i,j}$ for $i\in\{0,\dots,\alpha\}\backslash\{1,\dots,\beta\}$ and $j\in\{0,\dots,\alpha\}$. The matrix $\overline{B}$ can be defined as

$$\overline{B}\left(\tbinom{-X}{0},\dots,\tbinom{-X}{\alpha}\right)^T=\left(\textstyle\sum_{l=0}^{\alpha}(-1)^{i+l}\binom{l}{i}\binom{X}{l}\right)^T_{0\leqslant i\leqslant\alpha}.$$

Since

$$\tbinom{X}{l}=(-1)^l\tbinom{-X+l-1}{l}=(-1)^l\textstyle\sum_w\binom{-X}{w}\binom{l-1}{l-w}$$

for $l \in \mathbb{Z}_{\geqslant 1}$, it follows that

$$\overline{B}_{i,w} = [(i,w) = (0,0)] + \textstyle\sum_{l=1}^{\alpha} (-1)^i \binom{l}{i} \binom{l-1}{l-w}. \tag{7}$$

In particular, $\overline{B}_{0,w} = \binom{\alpha}{w}$, and

$$\begin{aligned}
\textstyle\sum_{w=0}^{\alpha} \overline{B}_{i,w} \binom{-j}{w-v} &= \textstyle\sum_{w=0}^{\alpha} \left( [(i,w) = (0,0)] + \sum_{l=1}^{\alpha} (-1)^i \binom{l}{i} \binom{l-1}{l-w} \right) \binom{-j}{w-v} \\
&= [(i,v) = (0,0)] + \textstyle\sum_{w,l=1}^{\alpha} (-1)^i \binom{l}{i} \binom{l-1}{w-1} \binom{-j}{w-v} \\
&= [(i,v) = (0,0)] + (-1)^{i+v} \textstyle\sum_{l=1}^{\alpha} (-1)^l \binom{l}{i} \binom{j-v}{l-v} \\
&= (-1)^{i+v} \textstyle\sum_{l=0}^{\alpha} (-1)^l \binom{l}{i} \binom{j-v}{l-v}.
\end{aligned}$$

The first equality follows from Equation (7). The third equality follows from Lemma 6, Equation (*c-i*). When $0 \leqslant v \leqslant j \leqslant \alpha$, due to Lemma 6, Equation (*c-j*),

$$(-1)^{i+v} \textstyle\sum_{l=0}^{\alpha} (-1)^l \binom{l}{i} \binom{j-v}{l-v} = (-1)^{i+j+v} \binom{v}{j-i}.$$

Hence we can simplify $M_{i,j}$ for $i \notin \{1, \dots, \beta\}$ as

$$\begin{cases} \sum_{w=0}^{\alpha} \overline{B}_{i,w} \left( \beta \binom{s-\alpha-\beta}{w}^{\partial} - \binom{s-\alpha-\beta}{w} \right) \frac{(-1)^w w!}{(s-\alpha)_{w+1}} & \text{if } j = 0, \\ \sum_{v} (-1)^{i+j+v} \binom{v}{j-i} \binom{s-\alpha-\beta+j}{v}^{\partial} \binom{s-\alpha+j-v}{j-v} - [i=0] \binom{s-\alpha-\beta+j}{j}^{\partial} & \text{if } j > 0. \end{cases}$$

Here the simplification for $j = 0$ follows from the equation

$$\textstyle\sum_u \binom{s+\beta(p-1)-\alpha-w}{u(p-1)-w} = \frac{(-1)^w w! \beta p}{(s-\alpha)_{w+1}},$$

which follows from Lemma 5, Equation (*c-c*). If $i \in \{\beta+1, \dots, \alpha\}$ then, due to Lemma 8,

$$\begin{aligned}
\textstyle\sum_v (-1)^{i+j+v} \binom{v}{i-j} \binom{s-\alpha-\beta+j}{v}^{\partial} \binom{s-\alpha+j-v}{j-v} &= F_{\beta,j,j-i}(s-\alpha-\beta+j) \\
&= \binom{\beta}{i}^{\partial} \binom{s-\alpha-\beta+j}{j-i},
\end{aligned}$$

so we can further simplify $M_{i,j}$ for $i \in \{\beta+1, \dots, \alpha\}$ as

$$\begin{cases} \sum_{w=0}^{\alpha} \overline{B}_{i,w} \left( \beta \binom{s-\alpha-\beta}{w}^{\partial} - \binom{s-\alpha-\beta}{w} \right) \frac{(-1)^w w!}{(s-\alpha)_{w+1}} & \text{if } j = 0, \\ \binom{\beta}{i}^{\partial} \binom{s-\alpha-\beta+j}{j-i} - [i=0] \binom{s-\alpha-\beta+j}{j}^{\partial} & \text{if } j > 0. \end{cases}$$

It follows immediately from these expressions that all entries of $M$ that are below the diagonal and are not in the zeroth column must be zero, since

$$\binom{s-\alpha-\beta+j}{j-i} = 0$$

when $j < i$. It also follows that all entries in the zeroth row except for the one that is in the zeroth column must be zero, since the only non-zero term in the relevant sum

$$\textstyle\sum_v (-1)^{j+v} \binom{v}{j} \binom{s-\alpha-\beta+j}{v}^{\partial} \binom{s-\alpha+j-v}{j-v}$$

is the one with $v = j$. This is because $\binom{v}{j} = 0$ for $v < j$ and $\binom{s-\alpha+j-v}{j-v} = 0$ for $v > j$. Therefore

$$M = \begin{bmatrix} M_{0,0} & 0 \\ v & U \end{bmatrix}$$

for some vector $v$ and some upper triangular $\alpha \times \alpha$ matrix $U$.[4] Consequently, the equation

$$M(z_0, \dots, z_\alpha)^T = (1, 0, \dots, 0)^T$$

has a solution such that $z_0 \neq 0$ as long as the diagonal entries of $M$ are non-zero. Since $\overline{B}_{0,w} = \binom{\alpha}{w}$, we have

$$\tfrac{(s-\alpha)_{\alpha+1}}{\alpha!\beta} M_{0,0} = \textstyle\sum_{w=0}^{\alpha} (-1)^w \left( \binom{s-\alpha-\beta}{w}^{\partial} - \frac{1}{\beta}\binom{s-\alpha-\beta}{w} \right) \binom{s-\alpha-w-1}{\alpha-w}.$$

Due to Lemma 6, Equation (*c-h*),

$$-\tfrac{1}{\beta} \textstyle\sum_{w=0}^{\alpha} (-1)^w \binom{s-\alpha-\beta}{w} \binom{s-\alpha-w-1}{\alpha-w} = -\frac{1}{\beta}\binom{\beta-1}{\alpha} = 0.$$

Due to Lemma 8,

$$\textstyle\sum_{w=0}^{\alpha} (-1)^w \binom{s-\alpha-\beta}{w}^{\partial} \binom{s-\alpha-w-1}{\alpha-w} = F_{\beta-1,\alpha,0}(s-\alpha-\beta) = -\binom{\beta-1}{\alpha}^{\partial}.$$

Thus, due to Lemma 4,

$$M_{0,0} = -\tfrac{\alpha!\beta}{(s-\alpha)_{\alpha+1}} \binom{\beta-1}{\alpha}^{\partial} = \tfrac{(-1)^{\alpha+\beta+1}}{(\alpha+1)\binom{\alpha}{\beta}\binom{s-\alpha}{\alpha+1}} \neq 0.$$

The diagonal entries $M_{1,1}, \dots, M_{\beta,\beta}$ are equal to $\binom{\beta}{1}, \dots, \binom{\beta}{\beta}$, respectively, all of which are non-zero. For $j \in \{\beta+1, \dots, \alpha\}$ we have, due to Lemma 4,

$$M_{j,j} = \binom{\beta}{j}^{\partial} = \tfrac{(-1)^{\beta+j+1}}{(\beta+1)\binom{j}{\beta+1}} \neq 0.$$

So the diagonal entries of $M$ are indeed non-zero. □

[4] For example, when $\alpha \geqslant 4$ this means that

$$M = \begin{bmatrix} M_{0,0} & 0 & 0 & 0 & \cdots & 0 \\ M_{1,0} & M_{1,1} & M_{1,2} & M_{1,3} & \cdots & M_{1,\alpha} \\ M_{2,0} & 0 & M_{2,2} & M_{2,3} & \cdots & M_{2,\alpha} \\ M_{3,0} & 0 & 0 & M_{3,3} & \cdots & M_{3,\alpha} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ M_{\alpha,0} & 0 & 0 & 0 & \cdots & M_{\alpha,\alpha} \end{bmatrix}.$$

## 9 Computing $\overline{\Theta}_{k,a}$

This section comprises three lemmas about properties of the ideal $\mathrm{im}(T-a)$. The key lemma is Lemma 15, and Lemmas 13 and 14 are auxiliary lemmas that are only used to prove Lemma 15. In Sections 10 and 11 we use Lemma 15 to show that $\overline{\Theta}_{k,a}$ is irreducible under the conditions of Theorem 3. As remarked in Section 4, the main strategy we use to compute $\overline{\Theta}_{k,a}$ is to find elements of $\mathscr{I}_a$ that represent non-trivial elements of the subquotients $(\widehat{N}_\alpha)_{0\leqslant\alpha<\nu}$, and this relates to $\mathrm{im}(T-a)$ because if an element of $\mathrm{ind}^G \Sigma_r$ is the reduction modulo $\mathfrak{m}$ of an integral element of $\mathrm{im}(T-a)$ then it is also in $\mathscr{I}_a$.

We refer to section 7 for the relevant notation. We recall that $\nu \leqslant \frac{p-1}{2} < p$ and $k > p^{100}$ (and therefore $r = k-2 > p^{99}$). Let us write $n = p^2$, so that $r > np^2$. If $w \in \{0,\dots,\lfloor \frac{r}{p+1} \rfloor\}$ and $u \in \{-w,\dots,r-wp\}$ then we write

$$\theta^w x^u y^{r-w(p+1)-u} = \textstyle\sum_j (-1)^j \binom{w}{j} x^{u+w+j(p-1)} y^{r-w-j(p-1)-u},$$

which is an element of $\mathrm{ind}^G \Sigma_r$. That is, the notation $\theta^w x^u y^v$ makes sense even if either $u$ or $v$ is in $\{-w,\dots,-1\}$ since $\theta^w$ is divisible by $(xy)^w$.

Lemma 13. *Suppose that $\alpha \in \{0,\dots,\nu-1\}$.*

1. *We have*

$$\begin{aligned}(T-a)\,(1 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}) \\ = \textstyle\sum_j (-1)^j \binom{n}{j} p^{j(p-1)+\alpha} \left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} x^{j(p-1)+\alpha} y^{r-j(p-1)-\alpha} \\ - a \textstyle\sum_j (-1)^j \binom{n-\alpha}{j} \bullet_{\overline{\mathbb{Q}}_p} \theta^\alpha x^{j(p-1)} y^{r-j(p-1)-\alpha(p+1)} + \mathsf{O}(p^n).\end{aligned}$$

2. *The submodule $\mathrm{im}(T-a) \subset \mathrm{ind}^G \widetilde{\Sigma}_r$ contains*

$$\textstyle\sum_i \left(\sum_{l=\beta-\gamma}^{\beta} C_l \binom{r-\beta+l}{i(p-1)+l}\right) \bullet_{\overline{\mathbb{Q}}_p} x^{i(p-1)+\beta} y^{r-i(p-1)-\beta} + \mathsf{O}\big(ap^{-\beta+v_C} + p^{p-1}\big)$$

*for all $0 \leqslant \beta \leqslant \gamma < \nu$ and all families $(C_l)_{l\in\mathbb{Z}}$ of elements of $\mathbb{Z}_p$, where*

$$v_C = \min_{\beta-\gamma\leqslant l\leqslant\beta}(v_p(C_l)+l).$$

*The $\mathsf{O}\big(ap^{-\beta+v_C} + p^{p-1}\big)$ term is equal to $\mathsf{O}\big(p^{p-1}\big)$ plus*

$$-\tfrac{ap^{-\beta}}{p-1} \textstyle\sum_{l=\beta-\gamma}^{\beta} C_l p^l \sum_{0\neq\mu\in\mathbb{F}_p} [\mu]^{-l} \left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\beta-l-n} y^{r-np-\beta+l}.$$

*Proof.* (1) Let us recall the formula

$$T(\gamma \bullet_{\overline{\mathbb{Q}}_p} v) = \textstyle\sum_{\mu\in\mathbb{F}_p} \gamma\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \left(\left(\begin{smallmatrix}1 & -[\mu]\\ 0 & p\end{smallmatrix}\right)\cdot v\right) + \gamma\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \left(\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)\cdot v\right)$$

for $T$. Let

$$\begin{aligned} 1 \bullet_{\overline{\mathbb{Q}}_p} v &= 1 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} \\ &= \textstyle\sum_{j=0}^{n} (-1)^j \binom{n}{j} \bullet_{\overline{\mathbb{Q}}_p} x^{\alpha+j(p-1)} y^{r-j(p-1)-\alpha}. \end{aligned}$$

If we apply the formula for $T$ to $1 \bullet_{\overline{\mathbb{Q}}_p} v = 1 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}$, then the first part of the formula, the part

$$\textstyle\sum_{\mu \in \mathbb{F}_p} \gamma\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1 \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \left(\left(\begin{smallmatrix} 1 & -[\mu] \\ 0 & p \end{smallmatrix}\right) \cdot v\right),$$

can be expanded into

$$\textstyle\sum_{\mu \in \mathbb{F}_p} \sum_{j,\xi \geqslant 0} \left(\begin{smallmatrix} p & [\mu] \\ 0 & 1 \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} (-1)^j \binom{n}{j} \binom{r-j(p-1)-\alpha}{\xi} (-[\mu])^{r-j(p-1)-\alpha-\xi} p^{\xi} x^{r-\xi} y^{\xi}.$$

The part of this sum with $\xi \geqslant n$ is in $\mathsf{O}(p^n)$, and moreover $(-[\mu])^{r-j(p-1)-\alpha-\xi}$ is independent of $j$ when $\xi < n$ since $r > p^{99}$ implies

$$r - j(p-1) - \alpha - \xi > r - np - p - n > 0.$$

The coefficient of $x^{r-\xi} y^{\xi}$ vanishes when $\xi < n$ since

$$\textstyle\sum_j (-1)^j \binom{n}{j} \binom{r-j(p-1)-\alpha}{\xi} = 0,$$

due to Lemma 6, Equation (*c-k*) applied to $(u, b, d, l, w) = (r-\alpha, 0, p-1, n, \xi)$. The second part of the formula, the part

$$\gamma\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \left(\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot v\right),$$

is precisely

$$\textstyle\sum_j (-1)^j \binom{n}{j} p^{j(p-1)+\alpha} \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} x^{j(p-1)+\alpha} y^{r-j(p-1)-\alpha},$$

and $-a \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}$ is precisely

$$-a \textstyle\sum_j (-1)^j \binom{n-\alpha}{j} \bullet_{\overline{\mathbb{Q}}_p} \theta^{\alpha} x^{j(p-1)} y^{r-j(p-1)-\alpha(p+1)}.$$

By adding these three terms up we obtain the required expression for

$$(T-a)\left(1 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}\right).$$

(2) Let us multiply the equation in the statement of part 1 on the left by

$$C_{\beta-\alpha} p^{-\alpha} \textstyle\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^{\alpha-\beta} \left(\begin{smallmatrix} p & [\mu] \\ 0 & 1 \end{smallmatrix}\right)$$

(that is, let us act on both sides of the equation in part 1 by the above element of $\overline{\mathbb{Q}}_p[G]$). Since $\mathrm{im}(T-a)$ is a $G$-module, both sides still end up in $\mathrm{im}(T-a)$. The "$j = 0$" part of the first sum on the right side becomes

$$\begin{aligned} & C_{\beta-\alpha} \textstyle\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^{\alpha-\beta} \left(\begin{smallmatrix} 1 & [\mu] \\ 0 & 1 \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} x^{\alpha} y^{r-\alpha} \\ &= C_{\beta-\alpha} \bullet_{\overline{\mathbb{Q}}_p} \textstyle\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^{\alpha-\beta} \left(\begin{smallmatrix} 1 & [\mu] \\ 0 & 1 \end{smallmatrix}\right) x^{\alpha} y^{r-\alpha} \\ &= C_{\beta-\alpha} \bullet_{\overline{\mathbb{Q}}_p} \textstyle\sum_{0 \neq \mu \in \mathbb{F}_p} [\mu]^{\alpha-\beta} x^{\alpha} ([\mu] x + y)^{r-\alpha} \\ &= (p-1) \textstyle\sum_i C_{\beta-\alpha} \binom{r-\alpha}{i(p-1)+\beta-\alpha} \bullet_{\overline{\mathbb{Q}}_p} x^{i(p-1)+\beta} y^{r-i(p-1)-\beta}. \end{aligned}$$

The third equality follows from the fact that

$$\textstyle\sum_{0\neq\mu\in\mathbb{F}_p}[\mu]^w = (p-1)[w\equiv_{p-1}0]$$

for $w\in\mathbb{Z}$. The "$j>0$" part of the first sum on the right becomes $\mathsf{O}\big(p^{p-1}\big)$. The rest of the right side becomes

$$-aC_{\beta-\alpha}p^{-\alpha}\textstyle\sum_{0\neq\mu\in\mathbb{F}_p}[\mu]^{\alpha-\beta}\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right)\bullet_{\overline{\mathbb{Q}}_p}\theta^n x^{\alpha-n}y^{r-np-\alpha}+\mathsf{O}(p^{n-\alpha}).$$

Thus, since $n-\alpha>p^2-p>p$, we get that $\operatorname{im}(T-a)$ contains

$$\begin{aligned}(p-1)\textstyle\sum_i C_{\beta-\alpha}\binom{r-\alpha}{i(p-1)+\beta-\alpha}\bullet_{\overline{\mathbb{Q}}_p}x^{i(p-1)+\beta}y^{r-i(p-1)-\beta}+\mathsf{O}\big(p^{p-1}\big)\\ -aC_{\beta-\alpha}p^{-\alpha}\textstyle\sum_{0\neq\mu\in\mathbb{F}_p}[\mu]^{\alpha-\beta}\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right)\bullet_{\overline{\mathbb{Q}}_p}\theta^n x^{\alpha-n}y^{r-np-\alpha}.\end{aligned}$$

If we sum this over all $\alpha\in\{0,\dots,\gamma\}$ and then divide by $p-1$, we get

$$\begin{aligned}\textstyle\sum_{\alpha=0}^{\gamma}\sum_i C_{\beta-\alpha}\binom{r-\alpha}{i(p-1)+\beta-\alpha}\bullet_{\overline{\mathbb{Q}}_p}x^{i(p-1)+\beta}y^{r-i(p-1)-\beta}+\mathsf{O}\big(p^{p-1}\big)\\ -\tfrac{a}{p-1}\textstyle\sum_{\alpha=0}^{\gamma}C_{\beta-\alpha}p^{-\alpha}\sum_{0\neq\mu\in\mathbb{F}_p}[\mu]^{\alpha-\beta}\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right)\bullet_{\overline{\mathbb{Q}}_p}\theta^n x^{\alpha-n}y^{r-np-\alpha},\end{aligned}$$

This element is in $\operatorname{im}(T-a)$ and, after changing to the variable $l=\beta-\alpha$, it turns into precisely the element we want. □

Lemma 14. *Suppose that $\alpha\in\mathbb{Z}$ and $v\in\mathbb{Q}$ and the family $(D_i)_{i\in\mathbb{Z}}$ of elements of $\mathbb{Z}_p$ are such that*

$$\begin{aligned}\alpha&\in\{0,\dots,\nu-1\},\\ D_i&=0\text{ for }i\notin[0,\tfrac{r-\alpha}{p-1}],\\ v&\leqslant v_p(\vartheta_\alpha(D_\bullet)),\\ v'=\min\{v_p(a)-\alpha,v\}&\leqslant v_p(\vartheta_w(D_\bullet))\text{ for }\alpha<w<2\nu-\alpha,\\ v'=\min\{v_p(a)-\alpha,v\}&<v_p(\vartheta_w(D_\bullet))\text{ for }0\leqslant w<\alpha.\end{aligned}$$

*Note that $2\nu-\alpha\leqslant 2\cdot\frac{p-1}{2}<p$. Let, for $j\in\mathbb{Z}$,*

$$\Delta_j:=(-1)^{j-1}(1-p)^{-\alpha}\tbinom{\alpha}{j-1}\vartheta_\alpha(D_\bullet),$$

*so that $(\Delta_j)_{j\in\mathbb{Z}}$ is supported on the set of indices $\{1,\dots,\alpha+1\}$ and therefore $\vartheta_w(\Delta_\bullet)$ is properly defined for $0\leqslant w<\alpha$, and $v\leqslant v_p(\vartheta_\alpha(\Delta_\bullet))\leqslant v_p(\Delta_j)$ for all $j\in\mathbb{Z}$. Then we have*

$$\begin{aligned}&\textstyle\sum_i(\Delta_i-D_i)\bullet_{\overline{\mathbb{Q}}_p}x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\\ &\quad=[\alpha\leqslant s](-1)^{n+1}D_{\frac{r-s}{p-1}}\bullet_{\overline{\mathbb{Q}}_p}\theta^n x^{r-np-s+\alpha}y^{s-\alpha-n}\\ &\qquad-D_0\bullet_{\overline{\mathbb{Q}}_p}\theta^n x^{\alpha-n}y^{r-np-\alpha}\\ &\qquad+E\bullet_{\overline{\mathbb{Q}}_p}\theta^{\alpha+1}h+F\bullet_{\overline{\mathbb{Q}}_p}h'+\mathrm{ERR}_1+\mathrm{ERR}_2,\end{aligned}$$

*for some integral* $\mathrm{ERR}_1 \in \mathrm{ind}^G \widetilde{\Sigma}_r$ *and* $\mathrm{ERR}_2 \in \mathrm{ind}^G \widetilde{\Sigma}_r$ *such that*

$$\mathrm{ERR}_1 \in \mathrm{im}(T-a) \text{ and } \mathrm{ERR}_2 = \mathsf{O}\big(p^{\nu - v_p(a)+v} + p^{\nu-\alpha}\big),$$

*some polynomials* $h$ *and* $h'$*, and some* $E, F \in \overline{\mathbb{Q}}_p$ *such that* $v_p(E) \geqslant v'$ *and* $v_p(F) > v'$*.*

*Proof.* By using the equation

$$g = a^{-1}Tg - (T-a)(a^{-1}g) \tag{8}$$

we can rewrite

$$g = \textstyle\sum_i (\Delta_i - D_i) \bullet_{\overline{\mathbb{Q}}_p} x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha}$$

as

$$\begin{aligned} &- \textstyle\sum_{\xi=0}^{2\nu-1-\alpha} a^{-1} X_\xi p^\xi \sum_{0\neq\lambda\in\mathbb{F}_p} [-\lambda]^{r-\alpha-\xi} \left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} x^{r-\xi} y^\xi \\ &\quad - [\alpha \leqslant s](-1)^{n+1} D_{\frac{r-s}{p-1}} \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{r-np-s+\alpha} y^{s-\alpha-n} \\ &\quad + D_0 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} + \mathsf{O}(p^{\nu-\alpha}) \\ &\quad + \mathrm{ERR}_3, \end{aligned} \tag{9}$$

where $\mathrm{ERR}_3 \in \mathrm{ind}^G \widetilde{\Sigma}_r$ is such that $\mathrm{ERR}_3 \in \mathrm{im}(T-a)$, and

$$X_\xi = \textstyle\sum_i (\Delta_i - D_i) \binom{r-i(p-1)-\alpha}{\xi}.$$

The first three lines of Equation (9) come from the "$a^{-1}Tg$" part of Equation (8), and to obtain the second and third lines we use part (1) of Lemma 13 to replace terms of type $a^{-1}\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} h_1$ with terms of type $1 \bullet_{\overline{\mathbb{Q}}_p} h_2$ plus some error terms that are in $\mathrm{im}(T-a)$ and other error terms that are in $\mathsf{O}(p^{n-\alpha})$—we omit the full details. Note that $X_\xi$ is well-defined since $(D_i)_{i\in\mathbb{Z}}$ and $(\Delta_i)_{i\in\mathbb{Z}}$ are both supported on the finite set of indices $i \in \{0, \dots, \lfloor \frac{r-\alpha}{p-1} \rfloor\}$. The constants $(\Delta_i)_{i\in\mathbb{Z}}$ are precisely designed in a way that $\vartheta_w(\Delta_\bullet) = 0$ for all $w \in \{0, \dots, \alpha-1\}$ and $\vartheta_\alpha(\Delta_\bullet) = \vartheta_\alpha(D_\bullet)$, and this follows immediately from lemma 6, Equation (*c-k*) applied to $(b, l, u) = (0, \alpha, (p-1)(\alpha+1))$. By writing $\binom{r-X-\alpha}{\xi} \in \mathbb{Q}_p[X]$ as a $\mathbb{Z}_p$-linear combination of $\binom{X}{0}, \dots, \binom{X}{\xi} \in \mathbb{Q}_p[X]$ we get that

$$\textstyle\sum_i (\Delta_i - D_i) \binom{r-i(p-1)-\alpha}{\xi}$$

is a $\mathbb{Z}_p$-linear combination of $\vartheta_0(\Delta_\bullet) - \vartheta_0(D_\bullet), \dots, \vartheta_\xi(\Delta_\bullet) - \vartheta_\xi(D_\bullet)$. Thus we can conclude that

$$v_p(X_\xi) > v' \text{ for all } \xi \in \{0, \dots, \alpha\}.$$

We also have

$$v_p(\Delta_i) \geqslant v_p(\vartheta_\alpha(D_\bullet)) \geqslant v \geqslant v'$$

by assumption, so we can conclude that

$$v_p(X_\xi) \geqslant v' \text{ for all } \xi \in \{\alpha+1, \dots, 2\nu-1-\alpha\}.$$

Thus the part of the sum "$\sum_{\xi=0}^{2\nu-1-\alpha}$" in the first line of (9) consisting of the indices $\xi \in \{\nu, \dots, 2\nu-1-\alpha\}$ is in

$$\mathsf{O}\Big(p^{\nu-v_p(a)+v'}\Big) = \mathsf{O}\big(p^{\nu-v_p(a)+v} + p^{\nu-\alpha}\big).$$

Due to part (1) of Lemma 13, the part of the sum consisting of the indices $\xi \in \{\alpha+1, \dots, \nu-1\}$ is

$$\begin{aligned} &a^{-1} \textstyle\sum_{\xi=\alpha+1}^{\nu-1} X_\xi p^\xi \sum_{0\neq\lambda\in\mathbb{F}_p} [-\lambda]^{r-\alpha-\xi} \left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} x^{r-\xi} y^\xi \\ &\quad = a^{-1} \textstyle\sum_{\xi=\alpha+1}^{\nu-1} X_\xi a \sum_{0\neq\lambda\in\mathbb{F}_p} [-\lambda]^{r-\alpha-\xi} \left(\begin{smallmatrix} 1 & [\lambda] \\ 0 & 1 \end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \theta^\xi h_\xi + \mathrm{ERR}_4 \\ &\quad = E \bullet_{\overline{\mathbb{Q}}_p} \theta^{\alpha+1} h + \mathrm{ERR}_4, \end{aligned}$$

where $\mathrm{ERR}_4 \in \mathrm{ind}^G \widetilde{\Sigma}_r$ is such that

$$\mathrm{ERR}_4 + \mathsf{O}\big(p^{\nu-v_p(a)+v} + p^{\nu-\alpha}\big) \in \mathrm{im}(T-a)$$

and $h$ and $E$ are such that $v_p(E) \geqslant v'$ (the constant $E$ can be chosen in this way since $v_p(X_\xi) \geqslant v'$ for all $\xi \in \{\alpha+1, \dots, \nu-1\}$). Similarly, the part of the sum consisting of the indices $\xi \in \{0, \dots, \alpha\}$ is

$$\textstyle\sum_{\xi=0}^{\alpha} F_\xi \bullet_{\overline{\mathbb{Q}}_p} \theta^\xi h_\xi + \mathrm{ERR}_5,$$

where $\mathrm{ERR}_5 \in \mathrm{ind}^G \widetilde{\Sigma}_r$ is such that

$$\mathrm{ERR}_5 + \mathsf{O}\big(p^{\nu-v_p(a)+v} + p^{\nu-\alpha}\big) \in \mathrm{im}(T-a)$$

and $h_\xi$ and $F_\xi$ are such that $v_p(F_\xi) \geqslant v_p(X_\xi) > v'$. We get the identity we want after writing

$$Fh' = \textstyle\sum_{\xi=0}^{\alpha} F_\xi \theta^\xi h_\xi$$

for suitable $h'$ and $F$. □

Lemma 15. *Let $(C_l)_{l\in\mathbb{Z}}$ be any family of elements of $\mathbb{Z}_p$. Suppose that $\alpha \in \{0, \dots, \nu-1\}$ and $v \in \mathbb{Q}$, and suppose that the constants*

$$D_i := [i=0]C_{-1} + [0 < i(p-1) < r-2\alpha] \textstyle\sum_{l=0}^{\alpha} C_l \binom{r-\alpha+l}{i(p-1)+l}$$

*satisfy the conditions of Lemma 14, i.e.*

$$\begin{aligned} v &\leqslant v_p(\vartheta_\alpha(D_\bullet)), \\ v' := \min\{v_p(a)-\alpha, v\} &\leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } \alpha < w < 2\nu-\alpha, \\ v' &< v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha. \end{aligned}$$

*Note that $(D_i)_{i\in\mathbb{Z}}$ is supported on the finite set of indices $\{0, \dots, \lfloor \frac{r-2\alpha}{p-1} \rfloor\}$ by definition. Moreover, suppose that $C_0$ is a unit. Let*

$$\vartheta' := (1-p)^{-\alpha} \vartheta_\alpha(D_\bullet) - C_{-1}.$$

*Suppose that $v_p(C_{-1}) \geqslant v_p(\vartheta')$.*

1. *If* $v_p(\vartheta') \leqslant v'$ *then there is some element* $\mathrm{gen}_1 \in \mathscr{I}_a$ *that represents a generator of* $\widehat{N}_\alpha$.

2. *If* $v_p(a) - \alpha < v$ *then there is some element* $\mathrm{gen}_2 \in \mathscr{I}_a$ *that represents a generator of a finite-codimensional submodule of*

$$T_{\mathrm{q},\alpha}\left(\mathrm{ind}^G \mathrm{quot}(\alpha)\right) = T_{\mathrm{q},\alpha}\left(\widehat{N}_\alpha / \mathrm{ind}^G \mathrm{sub}(\alpha)\right),$$

*where* $T_{\mathrm{q},\alpha}$ *denotes the endomorphism of* $\mathrm{ind}^G \mathrm{quot}(\alpha)$ *corresponding to the double coset of* $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

*Proof.* Before proceeding to the proofs of (1) and (2), let us make some initial remarks. Due to part (2) of Lemma 13, we know that $\mathrm{im}(T - a)$ contains

$$\textstyle\sum_i D_i \bullet_{\overline{\mathbb{Q}}_p} x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} + \mathsf{O}(ap^{-\alpha}). \tag{10}$$

The conditions imposed on the constants $D_i$ are designed in a way that

$$\textstyle\sum_i D_i x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} = \theta^\alpha h + h'$$

for some polynomials $h, h'$ such that $v_p(h') > v'$ (that is, such that the valuation of each of the coefficients of $h'$ is strictly greater than $v'$). In the very special case when $\vartheta_w(D_\bullet) = 0$ for $0 \leqslant w < \alpha$, this is because these conditions are precisely the equations needed to imply that

$$\textstyle\sum_i D_i x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha}$$

can be factored as $\theta^\alpha h$, due to Lemma 7. The general case when $\vartheta_w(D_\bullet) > v'$ for $0 \leqslant w < \alpha$ can be reduced to this special case by adding a term $h'$ such that $v_p(h') > v'$. Then $\overline{\theta}^\alpha \overline{h}$ is an element of $N_\alpha$, and the number $\vartheta'$ is specifically designed in a way that $\overline{\theta}^\alpha \overline{g}$ is precisely $\overline{\vartheta'}$ times a generator of $N_\alpha$. If $\vartheta'$ is a unit then this immediately gives us an integral element of $\mathrm{im}(T - a)$ whose reduction modulo $\mathfrak{m}$ represents a generator of $\widehat{N}_\alpha$. Note that in general the valuation of $\vartheta'$ is an integer. If that integer is strictly positive then we would like to multiply $\theta^\alpha h$ by $p^{-v_p(\vartheta')}$ prior to reducing modulo $\mathfrak{m}$. We cannot do this directly, since almost certainly there exist some $D_i$ whose valuation is strictly smaller than the valuation of $\vartheta'$, so after multiplying $\theta^\alpha h$ by $p^{-v_p(\vartheta')}$ we might not get an integral element. Thus we would like to "smoothen" the $D_i$ to better constants $\Delta_i$ which have much of the same qualities as the $D_i$ (i.e. satisfy the same conditions) but whose valuations are all at least as large as the valuation of $\vartheta'$. We use the constants $\Delta_i$ from Lemma 14, and we replace $D_i$ with $\Delta_i$ by adding

$$\textstyle\sum_i (\Delta_i - D_i) \bullet_{\overline{\mathbb{Q}}_p} x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} + D_0 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}$$

to (10). We know, directly from the definition of the constants $\Delta_i$, that

$$\begin{aligned}\textstyle\sum_i \Delta_i \bullet_{\overline{\mathbb{Q}}_p} x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} + D_0 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} \\ = (1-p)^{-\alpha} \vartheta_\alpha(D_\bullet) \bullet_{\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} \\ + C_{-1} \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha},\end{aligned}$$

and, for any $A, B \in \overline{\mathbb{Z}}_p$, the reduction modulo $\mathfrak{m}$ of

$$A \bullet_{\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} + B \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}$$

is $\overline{A-B}$ times a generator of $\widehat{N}_\alpha$. We use Lemma 14 to deduce that if we add to

$$\textstyle\sum_i (\Delta_i - D_i) \bullet_{\overline{\mathbb{Q}}_p} x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} + D_0 \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}$$

a certain error term that looks like

$$-E \bullet_{\overline{\mathbb{Q}}_p} \theta^{\alpha+1} h - F \bullet_{\overline{\mathbb{Q}}_p} h' + \mathrm{ERR}_1 + \mathrm{ERR}_2$$

then we get an element of $\mathrm{im}(T-a)$, so that $\mathrm{im}(T-a)$ contains

$$\begin{aligned}(\vartheta' + C_{-1}) \bullet_{\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} + C_{-1} \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} \\ + E \bullet_{\overline{\mathbb{Q}}_p} \theta^{\alpha+1} h + F \bullet_{\overline{\mathbb{Q}}_p} h' + \mathsf{O}\big(p^{\nu-v_p(a)+v} + p^{v_p(a)-\alpha}\big),\end{aligned} \tag{11}$$

for some $h, h', E, F$ with $v_p(E) \geqslant v'$ and $v_p(F) > v'$. Now let us proceed to the proofs of (1) and (2).

(1) Suppose that $v_p(\vartheta') \leqslant v'$. Let us note that $v_p(C_{-1}) \geqslant v_p(\vartheta')$. The terms in the first line of Equation (11) have valuations at least $v_p(\vartheta')$, and the terms in the second line of Equation (11) have valuations at least $v' \geqslant v_p(\vartheta')$. Thus if we we multiply (11) by $|\vartheta'| = p^{-v_p(\vartheta')}$ then we get an integral element $\widetilde{\mathrm{gen}}_1$ that is still an element of $\mathrm{im}(T-a)$. As $v_p(E) \geqslant v'$ and $\theta^{\alpha+1} h$ is trivial in $N_\alpha$, the reduction modulo $\mathfrak{m}$ of

$$|\vartheta'| E \bullet_{\overline{\mathbb{Q}}_p} \theta^{\alpha+1} h$$

is trivial in $\widehat{N}_\alpha$. As $v_p(F) > v'$, the reduction modulo $\mathfrak{m}$ of

$$|\vartheta'| F \bullet_{\overline{\mathbb{Q}}_p} h'$$

is trivial. And, as $v_p(a)$ is not an integer, the inequality $v_p(a) - \alpha \geqslant v_p(\vartheta')$ which follows from the assumption that $v' \geqslant v_p(\vartheta')$ must in fact be a strict inequality. Therefore the reduction modulo $\mathfrak{m}$ of the last term

$$|\vartheta'| \mathsf{O}\big(p^{\nu-v_p(a)+v} + p^{v_p(a)-\alpha}\big)$$

is trivial. Thus the reduction modulo $\mathfrak{m}$ of $\widetilde{\mathrm{gen}}_1$ is the reduction of

$$|\vartheta'| (\vartheta' + C_{-1}) \bullet_{\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} + |\vartheta'| C_{-1} \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha},$$

which, as mentioned, is $\overline{|\vartheta'|(\vartheta'+C_{-1})-|\vartheta'|C_{-1}} \in \overline{\mathbb{F}}_p^{\times}$ times a generator of $\widehat{N}_\alpha$. We define the desired element as the reduction modulo $\mathfrak{m}$ of $\widetilde{\mathrm{gen}}_1$.

(2) Suppose that $v_p(a)-\alpha < v$. We may without loss of generality assume that $v_p(\vartheta') > v' = v_p(a)-\alpha$ since otherwise we could apply the first part of this lemma and reach an even stronger conclusion. Then the dominant term in (11) comes from the error term $\mathsf{O}(ap^{-\alpha})$. This is because the terms in the first line of Equation (11) have valuation at least $v_p(\vartheta') > v_p(a)-\alpha$, the "$F$" and "$\mathsf{O}\big(p^{\nu-v_p(a)+v}\big)$" terms in the second line of Equation (11) have valuation bigger than $v' = v_p(a)-\alpha$, and $v_p(E) \geqslant v' = v_p(a)-\alpha$ and $\theta^{\alpha+1}h$ is trivial in $N_\alpha$ so the reduction modulo $\mathfrak{m}$ of

$$p^{\alpha-v_p(a)}E \bullet_{\overline{\mathbb{Q}}_p} \theta^{\alpha+1}h$$

is trivial in $\widehat{N}_\alpha$. The term $\mathsf{O}(ap^{-\alpha})$ is described in the last displayed equation in the statement of Lemma 13, and it is

$$-\tfrac{ap^{-\alpha}C_0}{p-1}\textstyle\sum_{0\neq\lambda\in\mathbb{F}_p}\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right) \bullet_{\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n}y^{r-np-\alpha}.$$

Thus after we multiply the element given by Equation (11) with $\frac{p-1}{ap^{-\alpha}C_0}$ and reduce the resulting element modulo $\mathfrak{m}$, we get a representative of

$$\left(\textstyle\sum_{\lambda\in\mathbb{F}_p}\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right) + A\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right) + [r \equiv_{p-1} 2\alpha]B\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right)\right) \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha-r}},$$

for some $A, B \in \overline{\mathbb{F}}_p$. Let $\gamma$ denote this element, which belongs to

$$\mathrm{ind}^G \mathrm{quot}(\alpha) = \widehat{N}_\alpha / \mathrm{ind}^G \mathrm{sub}(\alpha) \cong \mathrm{ind}^G(\sigma_{\underline{2\alpha-r}}(r-\alpha))$$

and is represented by the reduction modulo $\mathfrak{m}$ of an integral element of $\mathrm{im}(T-a)$ (and therefore by an element of $\mathscr{I}_a$). The classification given in Theorem 2 implies that either $T_{\mathrm{q},\alpha}-\lambda$ acts trivially on $\mathrm{ind}^G \mathrm{quot}(\alpha)$ modulo $\mathscr{I}_a$ for some $\lambda \in \overline{\mathbb{F}}_p$, or $s \in \{1,3,\dots,2\nu-1\}$ and $(T_{\mathrm{q},\alpha}-\lambda)(T_{\mathrm{q},\alpha}-\lambda^{-1})$ acts trivially on $\mathrm{ind}^G \mathrm{quot}(\alpha)$ modulo $\mathscr{I}_a$ for some $\lambda \in \overline{\mathbb{F}}_p^{\times}$.

- Let us first consider the case when $T_{\mathrm{q},\alpha}-\lambda$ acts trivially. Then

$$\left(A\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right) + \lambda - [r \equiv_{p-1} 2\alpha](1-B)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right)\right) \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha-r}} \tag{12}$$

  in $\mathrm{ind}^G \mathrm{quot}(\alpha)$ is represented by an element of $\mathscr{I}_a$. First suppose that $\underline{2\alpha-r} > 0$. If $A \neq 0$ then either $\lambda = 0$ in which case $\mathrm{ind}^G \mathrm{quot}(\alpha)$ is trivial modulo $\mathscr{I}_a$, or $\lambda \neq 0$ in which case we can multiply (12) on the left by $[\mu]^{p-2}\left(\begin{smallmatrix} 1 & 0 \\ [\mu] & 1\end{smallmatrix}\right)$ and sum over all $\mu \in \mathbb{F}_p$ to obtain that $\lambda \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha-r}-1}Y$ is represented by an element of $\mathscr{I}_a$, so we can take

$$\mathrm{gen}_2 = \lambda \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha-r}-1}Y.$$

  If $A = 0$ then either $\lambda \neq 0$ in which case $\mathrm{ind}^G \mathrm{quot}(\alpha)$ is trivial modulo $\mathscr{I}_a$, or $\lambda = 0$ in which case we can take

$$\mathrm{gen}_2 = T_{\mathrm{q},\alpha}\left(1 \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha-r}}\right).$$

Now suppose that $\underline{2\alpha - r} = 0$. Then we can use the decomposition of $G$ into cosets of $KZ$ given in Section 2.1.2 of [Bre03b] together with the fact that the element given by Equation (12) is trivial modulo $\mathscr{I}_a$ to conclude that any element of $\operatorname{ind}^G \operatorname{quot}(\alpha)$ can be written in the form

$$(\mu_1 \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) + \mu_2) \bullet_{\overline{\mathbb{F}}_p} 1 + h''$$

for some $h''$ which is represented by an element of $\mathscr{I}_a$, and thus we can find a suitable $\operatorname{gen}_2 \in \mathscr{I}_a$ that represents a generator of a submodule of $T_{\mathrm{q},\alpha}(\operatorname{ind}^G \operatorname{quot}(\alpha))$ which has codimension at most two.

- Now let us consider the case when $(T_{\mathrm{q},\alpha} - \lambda)(T_{\mathrm{q},\alpha} - \lambda^{-1})$ acts trivially. Thus $\lambda \neq 0$ and $s \in \{1, 3, \dots, 2\nu - 1\}$, and in particular $\underline{2\alpha - r} > 0$. As

$$\left(\sum_{\lambda \in \mathbb{F}_p} \left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right) + A\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha - r}}$$

is trivial in $\operatorname{ind}^G \operatorname{quot}(\alpha)$ modulo $\mathscr{I}_a$, it follows that so is

$$\left(A^2 \left(\begin{smallmatrix} p^2 & 0 \\ 0 & 1 \end{smallmatrix}\right) + (\lambda + \lambda^{-1}) A \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) + 1\right) \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha - r}}.$$

Again after multiplying on the left by $[\mu]^{p-2} \left(\begin{smallmatrix} 1 & 0 \\ [\mu] & 1 \end{smallmatrix}\right)$ and summing over all $\mu \in \mathbb{F}_p$ we conclude that $1 \bullet_{\overline{\mathbb{F}}_p} X^{\underline{2\alpha - r}^{-1}} Y$ is trivial (since $\underline{2\alpha - r} > 0$) and therefore that $\operatorname{ind}^G \operatorname{quot}(\alpha)$ is trivial modulo $\mathscr{I}_a$.

Consequently, either $\mathscr{I}_a$ contains a representative of a generator of a finite-codimensional submodule of $T_{\mathrm{q},\alpha}(\operatorname{ind}^G \operatorname{quot}(\alpha))$, or it contains a representative of a generator of $\operatorname{ind}^G \operatorname{quot}(\alpha)$ (the latter being a stronger statement), and we can take $\operatorname{gen}_2$ to be that element of $\mathscr{I}_a$. □

## 10 Proof of theorem 1

The proof is based on the approach outlined in [BG09], and roughly consists of finding enough elements in $\mathscr{I}_a$, consequently eliminating enough subquotients of $\operatorname{ind}^G \Sigma_r$, and using that information to find enough data about $\overline{\Theta}_{k,a}$.

Throughout Sections 10 and 11 we assume that

$$r = s + \beta(p-1) + u_0 p^t + \mathsf{O}(p^{t+1})$$

for some $\beta \in \{0, \dots, p-1\}$ and $u_0 \in \mathbb{Z}_p^\times$ and $t \in \mathbb{Z}_{\geqslant 1}$. Let us write $\epsilon = u_0 p^t$. Recall also that we assume $\nu - 1 < v_p(a) < \nu$ for some $\nu \in \{1, \dots, \frac{p-1}{2}\}$, that $s \in \{2\nu, \dots, p-1\}$, and that $k > p^{100}$ (and consequently $r > p^{99}$).

Recall that Theorem 1 is equivalent to Theorem 3. Let us show that Theorem 3 follows from the following proposition.

Proposition 16. *For each $\alpha \in \{0, \dots, \nu-2\}$, there is some element* $\mathrm{gen} \in \mathscr{I}_a$ *that represents a generator of a finite-codimensional submodule of*

$$T_{\mathrm{q},\alpha}\left(\mathrm{ind}^G \mathrm{quot}(\alpha)\right) = T_{\mathrm{q},\alpha}\left(\widehat{N}_\alpha / \mathrm{ind}^G \mathrm{sub}(\alpha)\right).$$

*Proof.* Proof that Proposition 16 implies Theorem 3. The classifications given by Theorem 2 and Theorem 2.7.1 in [Bre03a] imply that if $\overline{\Theta}_{k,a}$ is reducible then it must have exactly two infinite-dimensional factors. It may have up to two additional one-dimensional factors. Thus suppose that $\overline{\Theta}_{k,a}$ is reducible and its infinite-dimensional factors are $R_1$ and $R_2$. Recall from Section 4 that $\overline{\Theta}_{k,a}$ is a subquotient of

$$\mathrm{ind}^G(\Sigma_r / \langle y^r, \dots, x^{\nu-1}y^{r-\nu+1}, \overline{\theta}^\nu \Sigma_{r-\nu(p+1)} \rangle),$$

a module which has a series whose factors are subquotients of $\widehat{N}_0, \dots, \widehat{N}_{\nu-1}$. Thus each of $R_1, R_2$ is a quotient of one of the representations

$$\mathrm{ind}^G \mathrm{sub}(0), \dots, \mathrm{ind}^G \mathrm{sub}(\nu-1), \mathrm{ind}^G \mathrm{quot}(0), \dots, \mathrm{ind}^G \mathrm{quot}(\nu-1).$$

If $R_j$ happened to be a quotient of $\mathrm{quot}(\alpha)$ for some $\alpha \in \{0, \dots, \nu-2\}$ and some $j \in \{1, 2\}$, then Proposition 16 would imply that $R_j$ must be a quotient of a representation that contains $\mathrm{ind}^G \mathrm{quot}(\alpha)/T_{\mathrm{q},\alpha}$ as a finite-codimensional submodule. Since $\mathrm{ind}^G \mathrm{quot}(\alpha)/T_{\mathrm{q},\alpha}$ is irreducible (and infinite-dimensional) and $R_j$ is infinite-dimensional, it would follow in light of the classification given by Theorem 2 that $R_j \cong \mathrm{ind}^G \mathrm{quot}(\alpha)/T_{\mathrm{q},\alpha}$, resulting in a contradiction. Thus neither $R_1$ nor $R_2$ can happen to be a quotient of $\mathrm{quot}(\alpha)$ for some $\alpha \in \{0, \dots, \nu-2\}$. Moreover, neither $R_1$ nor $R_2$ can happen to be a quotient of $\mathrm{ind}^G \mathrm{sub}(0)$, since $\mathscr{I}_a$ contains $1 \bullet_{\overline{\mathbb{Q}}_p} y^r$, which generates $\mathrm{ind}^G \mathrm{sub}(0)$. Hence each of them is a quotient of one of the representations

$$\mathrm{ind}^G \mathrm{sub}(1), \dots, \mathrm{ind}^G \mathrm{sub}(\nu-1), \mathrm{ind}^G \mathrm{quot}(\nu-1).$$

Suppose that $R_1$ and $R_2$ are quotients of $\mathrm{ind}^G(\sigma_b(b'))$ and $\mathrm{ind}^G(\sigma_d(d'))$, respectively. By Theorem 2 we must have

$$b' - d' \equiv d + 1 \bmod p-1,$$
$$b + d \equiv -2 \bmod p-1.$$

In particular, $\mathrm{ind}^G(\sigma_b(b'))$ and $\mathrm{ind}^G(\sigma_d(d'))$ cannot happen to be the representations $\mathrm{ind}^G \mathrm{sub}(\alpha)$ and $\mathrm{ind}^G \mathrm{sub}(\alpha')$, as that would imply that

$$\{2, \dots, 2\nu-2\} \ni \alpha + \alpha' \equiv_{p-1} r + 1 \equiv_{p-1} s + 1 \notin \{2, \dots, 2\nu\},$$

resulting in a contradiction. Similarly, $\mathrm{ind}^G(\sigma_b(b'))$ and $\mathrm{ind}^G(\sigma_d(d'))$ cannot happen to be the representations $\mathrm{ind}^G \mathrm{sub}(\alpha)$ and $\mathrm{ind}^G \mathrm{quot}(\nu-1)$, as that would imply that

$$\alpha \equiv \nu \bmod p-1,$$

resulting in a contradiction. And finally, $\mathrm{ind}^G(\sigma_b(b'))$ and $\mathrm{ind}^G(\sigma_d(d'))$ cannot happen to both be the representation $\mathrm{ind}^G \mathrm{quot}(\nu-1)$, as that would imply that

$$s \equiv 2\nu - 1 \bmod p-1,$$

resulting in a contradiction. Therefore we reach a contradiction in all cases, implying that $\overline{\Theta}_{k,a}$ must in fact be irreducible. □

The next section is dedicated to proving Proposition 16.

## 11 Proof of proposition 16

Recall from Section 7 that

$$X_n = X(X-1)\cdots(X-n+1) \in \mathbb{Z}_p[X]$$

is the falling factorial. Let $\alpha \in \{0,\dots,\nu-2\}$. The goal is to apply Lemma 15 with a certain family $(C_l)_{l\in\mathbb{Z}}$ of elements of $\mathbb{Z}_p$ and certain $v \in \mathbb{Q}$. For any such $(C_l)_{l\in\mathbb{Z}}$ and $v \in \mathbb{Q}$ let us define

$$D_i := [i=0]C_{-1} + [0 < i(p-1) < r-2\alpha] \sum_{l=0}^{\alpha} C_l \tbinom{r-\alpha+l}{i(p-1)+l}.$$

Thus throughout the proof the constants $(D_i)_{i\in\mathbb{Z}}$ depend on and are defined entirely by the constants $(C_{-1}, C_0, \dots, C_\alpha)$. Let us note from the definition of $\vartheta_j(D_\bullet)$ for $j \in \{0,\dots,p-1\}$ that it is a $\mathbb{Z}_p$-linear combination of the constants $(C_{-1}, C_0, \dots, C_\alpha)$. We always pick $C_j = 0$ for $j \notin \{-1, 0, \dots, \alpha\}$. In the proof we make choices for $(C_{-1}, C_0, \dots, C_\alpha)$ and $v$ so that the constants $(D_i)_{i\in\mathbb{Z}}$ satisfy the conditions of Lemma 15, i.e.

$$v \leqslant v_p(\vartheta_\alpha(D_\bullet)), \tag{$*1$}$$

$$v' := \min\{v_p(a)-\alpha, v\} \leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } \alpha < w < 2\nu-\alpha, \tag{$*2$}$$

$$v' < v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha, \tag{$*3$}$$

$$C_0 \in \mathbb{Z}_p^\times, \tag{$*4$}$$

$$v_p(C_{-1}) \geqslant v_p(\vartheta'). \tag{$*5$}$$

We call $(C_{-1}, C_0, \dots, C_\alpha)$ and $v \in \mathbb{Q}$ "suitable" if the five conditions ($*1$), ($*2$), ($*3$), ($*4$), ($*5$) are satisfied and if moreover either $v_p(\vartheta') \leqslant v'$ or $v_p(a)-\alpha < v$. Suppose that we are indeed able to find suitable $(C_{-1}, C_0, \dots, C_\alpha)$ and $v$. If $v_p(a)-\alpha < v$ then we can conclude from part (2) of Lemma 15 that there is some element $\mathrm{gen} \in \mathscr{I}_a$ that represents a generator of a finite-codimensional submodule of

$$T_{\mathrm{q},\alpha}\left(\mathrm{ind}^G \mathrm{quot}(\alpha)\right) = T_{\mathrm{q},\alpha}\left(\widehat{N}_\alpha / \mathrm{ind}^G \mathrm{sub}(\alpha)\right),$$

and if $v_p(\vartheta') \leqslant v'$ we can use part (1) of Lemma 15 to reach an even stronger conclusion, that there is some element $\mathrm{gen} \in \mathscr{I}_a$ that represents a generator of $\widehat{N}_\alpha$ (and therefore gen also represents a generator of $T_{\mathrm{q},\alpha}(\mathrm{ind}^G \mathrm{quot}(\alpha))$). Thus all we need to do to prove Proposition 16 is to find suitable $(C_{-1}, C_0, \ldots, C_\alpha)$ and $v$, for $\alpha \in \{0, \ldots, \nu - 2\}$.

Let $U$ denote the $(2\nu - \alpha) \times (\alpha + 1)$ matrix with entries in $\mathbb{Q}_p$ indexed by $0 \leqslant w < 2\nu - \alpha$ and $0 \leqslant j \leqslant \alpha$, defined by

$$U(C_0, C_1, \ldots, C_\alpha)^T = (\vartheta_0(D_\bullet) - C_{-1}, \vartheta_1(D_\bullet), \ldots, \vartheta_{2\nu-\alpha-1}(D_\bullet))^T.$$

Note that only the constants $C_0, \ldots, C_\alpha$ appear in the linear combinations on the right side, so this equation does indeed define a linear map. Let $U^{sub}$ denote the $(\alpha + 1) \times (\alpha + 1)$ submatrix consisting of the top $\alpha + 1$ rows of $U$, i.e. of those entries indexed by $0 \leqslant w, j \leqslant \alpha$.[5] Due to Lemma 5, Equation (*c-f*),

$$U_{w,j} = \sum_v \tbinom{-j}{w-v} \tbinom{r-\alpha+j}{v} \left( \tbinom{s-\alpha+j-v}{j-v} - \tbinom{r-\alpha+j-v}{j-v} \right) + \mathsf{O}(p)$$

for $0 \leqslant w < 2\nu - \alpha$ and $0 \leqslant j \leqslant \alpha$, so the entries of $U$ are in fact integers.

Let us consider four different cases:

- $\alpha = 0$,
- $\alpha > 0$ and $\beta \notin \{0, \ldots, \alpha\}$,
- $\alpha > 0$ and $\beta = 0$,
- $\alpha > 0$ and $\beta \in \{1, \ldots, \alpha\}$.

In order to prove Proposition 16, we must find constants $(C_{-1}, C_0, \ldots, C_\alpha)$ and $v \in \mathbb{Q}_p$ that are "suitable" (i.e. such that the five conditions (∗1), (∗2), (∗3), (∗4), (∗5) are satisfied and either $v_p(\vartheta') \leqslant v'$ or $v_p(a) - \alpha < v$) in each case.

- *Suppose that* $\alpha = 0$. In this case we choose $(C_{-1}, C_0) = (0, 1)$. Then the two conditions (∗1), (∗2) are equivalent to

$$v \leqslant v_p(\vartheta_0(D_\bullet)),$$
$$v' := \min\{v_p(a), v\} \leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } 0 < w < 2\nu,$$

  and the three conditions (∗3), (∗4), (∗5) are vacuously true. Moreover, we set $v = v_p(\vartheta_0(D_\bullet))$, so that condition (∗1) is also satisfied and we trivially have either $v_p(\vartheta') = v \leqslant v'$ or $v_p(a) < v$. Thus all we need to check is that $v' \leqslant v_p(\vartheta_w(D_\bullet))$ for $0 < w < 2\nu$. Due to Lemma 5, Equation (*c-b*),

$$\vartheta_0(D_\bullet) = \tfrac{s-r}{s} p + \mathsf{O}\big((s-r)p^2\big).$$

[5] Note that $\alpha \in \{0, \ldots, \nu - 2\}$ implies that $\alpha + 1 < 2\nu - \alpha$.

Moreover, due to Lemma 5, Equation (*c-b*) and Lemma 5, Equation (*c-c*),

$$\begin{aligned}\vartheta_w(D_\bullet) &= \textstyle\sum_{0<i(p-1)<r} \binom{r}{i(p-1)}\binom{i(p-1)}{w} \\ &= \textstyle\sum_{0<i(p-1)<r} \binom{r-w}{i(p-1)-w}\binom{r}{w} \\ &= \textstyle\binom{r}{w}\sum_{0<i(p-1)<r}\sum_{u=0}^{w}(-1)^u\binom{w}{u}\binom{r-u}{i(p-1)} \\ &= \textstyle\binom{r}{w}(s-r)p\sum_{u=0}^{w}(-1)^u\binom{w}{u}\frac{1}{s-u} + \mathsf{O}\big((s-r)p^2\big) \\ &= \textstyle\frac{(-1)^w(s-r)r_w}{s_{w+1}}p + \mathsf{O}\big((s-r)p^2\big) = \mathsf{O}((s-r)p) \qquad (13)\end{aligned}$$

for $0 < w < 2\nu$. The first equality follows from the definition of $\vartheta_w(D_\bullet)$, the second equality is a simple rewrite, the third equality follows from Lemma 5, Equation (*c-c*), the fourth equality follows from Lemma 5, Equation (*c-b*), and the fifth equality follows from the equation

$$\textstyle\sum_{u=0}^{w}(-1)^u\binom{w}{u}\frac{1}{X} = \frac{(-1)^w w!}{X_{w+1}} \in \mathbb{Q}(X)$$

and the fact that $s_{w+1} \neq 0$ (because $s \geqslant 2\nu$). If $0 = \alpha < \max\{\nu - t - 1, \beta\}$, then either $\beta > 0$ in which case $s - r \in \mathbb{Z}_p^\times$ and $\vartheta_0(D_\bullet) \in \mathbb{Z}_p^\times$ and therefore the constants $(C_{-1}, C_0)$ are suitable for $v = 0$, or $\beta = 0$ and $t \leqslant \nu - 2$ in which case $v_p(\vartheta_0(D_\bullet)) = t + 1$ and $v_p(\vartheta_w(D_\bullet)) \geqslant t + 1$ for $0 < w < 2\nu$ and therefore the constants $(C_{-1}, C_0)$ are suitable for $v = v' = t + 1$. If, on the other hand, $\max\{\nu - t - 1, \beta\} = 0$, then $\beta = 0$ and $t \geqslant \nu - 1$ and $v = t + 1$ and $v' = v_p(a) < v \leqslant v_p(\vartheta_w(D_\bullet))$ for $0 < w < 2\nu$, so again the constants $(C_{-1}, C_0)$ are suitable for $v = t + 1$.

- *Suppose that* $\alpha > 0$ *and* $\beta \notin \{0, \ldots, \alpha\}$. The second condition implies that $v_p((s-r)_{\alpha+1}) = 0$. Let $M$ and $c$ be the matrix and vector that are defined in Lemma 11. The entries of $M$ and $c$ are in $\mathbb{Q}(X, Y) \subset \mathbb{Q}_p(X, Y)$. Let us make the substitutions $X = r - \alpha$ and $Y = s - \alpha$, so that we end up with the matrix $M^\circ$ and vector $v^\circ$ with entries in $\mathbb{Q}_p$. In this case we choose $(C_{-1}, C_0) = (0, 1)$ and
$$C_j = \textstyle\frac{c_j^\circ p}{(s-\alpha)_\alpha}$$
for $0 < j \leqslant \alpha$. Recall that
$$U(1, C_1, \ldots, C_\alpha)^T = (\vartheta_0(D_\bullet), \ldots, \vartheta_{2\nu-\alpha-1}(D_\bullet))^T.$$
Due to Lemma 5, Equation (*c-b*) and Lemma 5, Equation (*c-f*),
$$\begin{aligned}U_{w,0} &= \textstyle\frac{(-1)^w(s-r)(r-\alpha)_w}{(s-\alpha)_{w+1}}p + \mathsf{O}\big(p^2\big), \\ U_{w,j} &= \textstyle\sum_v \binom{-j}{w-v}\binom{r-\alpha+j}{v}\left(\binom{s-\alpha+j-v}{j-v} - \binom{r-\alpha+j-v}{j-v}\right) + \mathsf{O}(p),\end{aligned}$$
for $0 \leqslant w < 2\nu - \alpha$ and $0 < j \leqslant \alpha$. The first line follows as in Equation (13). In particular,
$$U_{w,j} = p^{[j=0]}(M_{w,j}^\circ + \mathsf{O}(p))$$

for $0 \leqslant w < 2\nu - \alpha$ and $0 < j \leqslant \alpha$. Therefore, due to Lemma 11, the first $\alpha$ entries of the resulting column vector $(\vartheta_0(D_\bullet), \dots, \vartheta_{2\nu-\alpha-1}(D_\bullet))^T$ are $\mathsf{O}(p^2)$, and the entry indexed $\alpha$ is

$$\vartheta_\alpha(D_\bullet) = \tfrac{(s-r)_{\alpha+1}}{(s-\alpha)_{\alpha+1}} p + \mathsf{O}(p^2) \in p\mathbb{Z}_p^\times.$$

Since all subsequent entries are evidently $\mathsf{O}(p)$, we can conclude that the constants $(C_{-1}, C_0, \dots, C_\alpha)$ are suitable for $v = 1$ (we omit the fine details of checking that all of the conditions are satisfied).

- *Suppose that $\alpha > 0$ and $\beta = 0$.* Let us define $M^\circ$ and $c^\circ$ as in the previous case, and let $(C_{-1}, C_0) = (0, 1)$ and

$$C_j = \tfrac{c_j^\circ p}{(s-\alpha)_\alpha}$$

for $0 < j \leqslant \alpha$. We can similarly compute

$$\begin{aligned} U_{w,0} &= \tfrac{(-1)^w (s-r)(r-\alpha)_w}{(s-\alpha)_{w+1}} p + \mathsf{O}(p^{t+2}), \\ U_{w,j} &= \textstyle\sum_v \binom{-j}{w-v} \binom{r-\alpha+j}{v} \left( \binom{s-\alpha+j-v}{j-v} - \binom{r-\alpha+j-v}{j-v} \right) + \mathsf{O}(p^{t+1}), \end{aligned}$$

for $0 \leqslant w < 2\nu - \alpha$ and $0 < j \leqslant \alpha$. Again,

$$U(1, C_1, \dots, C_\alpha)^T = (\vartheta_0(D_\bullet), \dots, \vartheta_{2\nu-\alpha-1}(D_\bullet))^T.$$

The first $\alpha$ entries of this column vector are in $\mathsf{O}(p^{t+2})$, and the entry indexed $\alpha$ is

$$\tfrac{(s-r)_{\alpha+1}}{(s-\alpha)_{\alpha+1}} p + \mathsf{O}(p^{t+2}) \in p^{t+1}\mathbb{Z}_p^\times.$$

Moreover, as long as $w < 2\nu - \alpha$, we have

$$U_{w,0} = \tfrac{(-1)^w (s-r)(r-\alpha)_w}{(s-\alpha)_{w+1}} p + \mathsf{O}(p^{t+2}) = \mathsf{O}(p^{t+1}),$$

and, since $r = s + \mathsf{O}(p^t)$, we have

$$\tbinom{r-\alpha+l}{l} = \tbinom{s-\alpha+l}{l} + \mathsf{O}(p^t)$$

when $l < p$, implying directly from the formula for $U_{w,j}$ that $U_{w,j} = \mathsf{O}(p^t)$ for $0 < w < 2\nu - \alpha$ and $j > 0$. Since $v_p(C_j) \geqslant 1$ for $1 \leqslant j \leqslant \alpha$, it follows that the last $2\nu - 2\alpha - 1$ entries of $(\vartheta_0(D_\bullet), \dots, \vartheta_{2\nu-\alpha-1}(D_\bullet))^T$ are in $\mathsf{O}(p^{t+1})$. Therefore the constants $(C_{-1}, C_0, \dots, C_\alpha)$ are suitable for $v = t + 1$ (again we omit the fine details of checking that all of the conditions are satisfied).

- *Suppose that $\alpha > 0$ and $\beta \in \{1, \dots, \alpha\}$.* This is the final and most involved case. In this case we are not able to give an explicit formula for the constants $(C_{-1}, C_0, \dots, C_\alpha)$, instead we can only show that such constants exist. This is also the first case in which we must choose a non-zero $C_{-1}$. Let $A$ be

the $(2\nu-\alpha)\times(\alpha+1)$ matrix with entries indexed by $0\leqslant w<2\nu-\alpha$ and $0\leqslant j\leqslant\alpha$ and defined by

$$A_{w,j}=p^{-[j=0]}\sum_{i>0}\tbinom{r-\alpha+j}{i(p-1)+j}\tbinom{i(p-1)}{w},$$

for all $0\leqslant w<2\nu-\alpha$ and $0\leqslant j\leqslant\alpha$. The matrix $A$ is precisely the matrix obtained from $U$ by dividing the first column by $p$, and we have

$$\begin{aligned}&A(C_0,C_1/p,\dots,C_\alpha/p)^T\\&\quad=((\vartheta_0(D_\bullet)-C_{-1})/p,\vartheta_1(D_\bullet)/p,\dots,\vartheta_{2\nu-\alpha-1}(D_\bullet)/p)^T.\end{aligned}$$

Let $A^{sub}$ denote the $(\alpha+1)\times(\alpha+1)$ submatrix consisting of the top $\alpha+1$ rows of $A$, i.e. of those entries indexed by $0\leqslant w,j\leqslant\alpha$. We have

$$\begin{aligned}A_{w,0}&=\tfrac{(-1)^w(s-r)(r-\alpha)_w}{(s-\alpha)_{w+1}}+\mathsf{O}(p),\\A_{w,j}&=\textstyle\sum_v\binom{-j}{w-v}\binom{r-\alpha+j}{v}\left(\binom{s-\alpha+j-v}{j-v}-\binom{r-\alpha+j-v}{j-v}\right)+\mathsf{O}(p),\end{aligned}$$

for all $0\leqslant w<2\nu-\alpha$ and $0\leqslant j\leqslant\alpha$, so in particular $A$ has integer entries. However, these expressions for the entries of $A$ are not useful as we need to compute $A$ up to precision $\mathsf{O}\big(p^{t+1}\big)$. Recall the definition of

$$\tbinom{X}{n}^{\partial}=\tfrac{\partial}{\partial X}\tbinom{X}{n}\in\mathbb{Q}_p[X]$$

from Section 6. Let us also consider the $(2\nu-\alpha)\times(\alpha+1)$ matrices $S$ and $N$ with integer entries indexed by $0\leqslant w<2\nu-\alpha$ and $0\leqslant j\leqslant\alpha$ and defined by

$$\begin{aligned}S_{w,j}&=p^{-[j=0]}\textstyle\sum_{i=1}^{\beta}\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w},\\N_{w,j}&=p^{-[j=0]}\textstyle\sum_v\binom{-j}{w-v}\binom{s+\beta(p-1)-\alpha+j}{v}^{\partial}\sum_{i=0}^{\beta}\binom{s+\beta(p-1)-\alpha+j-v}{i(p-1)+j-v}\\&\qquad-[w=0]\tbinom{s+\beta(p-1)-\alpha+j}{j}^{\partial}-[j=0]\tbinom{s+\beta(p-1)-\alpha}{w}\tfrac{(-1)^w w!}{(s-\alpha)_{w+1}},\end{aligned}$$

for all $0\leqslant w<2\nu-\alpha$ and $0\leqslant j\leqslant\alpha$. The fact that $S$ has integer entries can be shown in the same way as the fact that $A$ has integer entries, and $N$ has integer entries because

$$\begin{aligned}&\textstyle\sum_v\binom{0}{w-v}\binom{s+\beta(p-1)-\alpha}{v}^{\partial}\sum_{i=0}^{\beta}\binom{s+\beta(p-1)-\alpha-v}{i(p-1)-v}\\&\quad=\tbinom{s+\beta(p-1)-\alpha}{w}^{\partial}\mathrm{S}_{s+\beta(p-1)-\alpha-w,-w}\\&\quad=\tbinom{s+\beta(p-1)-\alpha}{w}^{\partial}\textstyle\sum_{i=0}^{w}(-1)^i\binom{w}{i}\mathrm{S}_{s+\beta(p-1)-\alpha-i}\\&\quad=\tbinom{s+\beta(p-1)-\alpha}{w}^{\partial}\textstyle\sum_{i=0}^{w}(-1)^i\binom{w}{i}(1+[s-\alpha-i=0]+\mathsf{O}(p))\\&\quad=\tbinom{s+\beta(p-1)-\alpha}{w}^{\partial}\textstyle\sum_{i=0}^{w}(-1)^i\binom{w}{i}(1+\mathsf{O}(p))\\&\quad=[w=0]\tbinom{s+\beta(p-1)-\alpha}{w}^{\partial}+\mathsf{O}(p)=\mathsf{O}(p).\end{aligned}$$

The second equality follows from Lemma 5, Equation (*c-c*), the third equality follows from Lemma 5, Equation (*c-b*), and the fourth equality follows from $s \geqslant 2\nu > \alpha + w$. Let also $S^{sub}$ and $N^{sub}$ denote the $(\alpha+1)\times(\alpha+1)$ submatrices consisting of the top $\alpha+1$ rows of $S$ and $N$, respectively. Recall that $\epsilon = u_0 p^t$. Let us prove the following claim.

*Approximation claim.*

$$A = S + \epsilon N + \mathsf{O}(\epsilon p).$$

*Proof of the approximation claim.* First let us look at the entries with $j > 0$. Due to Lemma 5, Equation (*c-f*),

$$\begin{aligned} A_{w,j} &= \textstyle\sum_v \binom{-j}{w-v}\binom{r-\alpha+j}{v}\sum_{i>0}\binom{r-\alpha+j-v}{i(p-1)+j-v} \\ &= \textstyle\sum_v \binom{-j}{w-v}\binom{r-\alpha+j}{v}\sum_{i}\binom{r-\alpha+j-v}{i(p-1)+j-v} - \binom{r-\alpha+j}{j}\binom{0}{w}. \end{aligned}$$

The second equality here simply amounts to extracting the "$i = 0$" term from the sum. We now use the equation

$$\binom{r-\alpha+j}{j} = \binom{s+\beta(p-1)-\alpha+j}{j} + \epsilon\binom{s+\beta(p-1)-\alpha+j}{j}^{\partial} + \mathsf{O}(\epsilon p), \tag{14}$$

which is true because $j < p$ (see section 4). Due to Lemma 5, Equation (*c-f*),

$$S_{w,j} = \textstyle\sum_v \binom{-j}{w-v}\binom{s+\beta(p-1)-\alpha+j}{v}\sum_{i>0}\binom{s+\beta(p-1)-\alpha+j-v}{i(p-1)+j-v}.$$

By combining these facts we get that $A_{w,j} - S_{w,j} - \epsilon N_{w,j}$ is

$$\begin{aligned} &\textstyle\sum_v \binom{-j}{w-v}\binom{s+\beta(p-1)-\alpha+j}{v}\sum_i\left(\binom{r-\alpha+j-v}{i(p-1)+j-v} - \binom{s+\beta(p-1)-\alpha+j-v}{i(p-1)+j-v}\right) \\ &\quad + \epsilon\textstyle\sum_v \binom{-j}{w-v}\binom{s+\beta(p-1)-\alpha+j}{v}^{\partial}\sum_i\left(\binom{r-\alpha+j-v}{i(p-1)+j-v} - \binom{s+\beta(p-1)-\alpha+j-v}{i(p-1)+j-v}\right) \\ &\quad - \binom{r-\alpha+j}{j}\binom{0}{w} + \binom{s+\beta(p-1)-\alpha+j}{j}\binom{0}{w} + \epsilon\binom{s+\beta(p-1)-\alpha+j}{j}^{\partial}\binom{0}{w}. \end{aligned}$$

The first two lines are in $\mathsf{O}(\epsilon p)$ since, due to Lemma 5, Equation (*c-a*),

$$\textstyle\sum_i \binom{r-\alpha+j-v}{i(p-1)+j-v} \equiv \sum_i \binom{s+\beta(p-1)-\alpha+j-v}{i(p-1)+j-v} \bmod \epsilon p.$$

The third line is in $\mathsf{O}(\epsilon p)$ because of Equation (14). Thus

$$A_{w,j} = S_{w,j} + \epsilon N_{w,j} + \mathsf{O}(\epsilon p)$$

for all $0 \leqslant w < 2\nu - \alpha$ and $0 < j \leqslant \alpha$. Now let us look at the entries with $j = 0$. In this case

$$\begin{aligned} pA_{w,0} &= \textstyle\sum_{i>0}\binom{r-\alpha}{i(p-1)}\binom{i(p-1)}{w} = \binom{r-\alpha}{w}\sum_{i>0}\binom{r-\alpha-w}{i(p-1)-w}, \\ pS_{w,0} &= \textstyle\sum_{i>0}\binom{s+\beta(p-1)-\alpha}{i(p-1)}\binom{i(p-1)}{w} = \binom{s+\beta(p-1)-\alpha}{w}\sum_{i>0}\binom{s+\beta(p-1)-\alpha-w}{i(p-1)-w}, \\ pN_{w,0} &= \textstyle\binom{s+\beta(p-1)-\alpha}{w}^{\partial}\sum_{i>0}\binom{s+\beta(p-1)-\alpha-w}{i(p-1)-w} - \binom{s+\beta(p-1)-\alpha}{w}\frac{(-1)^w w!}{(s-\alpha)_{w+1}}p. \end{aligned}$$

So $p(A_{w,0} - S_{w,0} - \epsilon N_{w,0})$ is equal to

$$\begin{aligned}
&\tbinom{r-\alpha}{w}\textstyle\sum_{i>0}\left(\tbinom{r-\alpha-w}{i(p-1)-w} - \tbinom{s+\beta(p-1)-\alpha-w}{i(p-1)-w}\right)\\
&\quad+\left(\tbinom{r-\alpha}{w} - \tbinom{s+\beta(p-1)-\alpha}{w} - \epsilon\tbinom{s+\beta(p-1)-\alpha}{w}^{\partial}\right)\textstyle\sum_{i>0}\tbinom{s+\beta(p-1)-\alpha-w}{i(p-1)-w}\\
&\quad+\tbinom{s+\beta(p-1)-\alpha}{w}\tfrac{(-1)^w w!}{(s-\alpha)_{w+1}}\epsilon p.
\end{aligned}$$

Due to Lemma 5, Equation (c-b) in combination with Lemma 5, Equation (c-c), we have

$$\textstyle\sum_{i>0}\tbinom{s+\beta(p-1)-\alpha-w}{i(p-1)-w} = \mathsf{O}(p),$$

so the second line is in $\mathsf{O}(\epsilon p^2)$. Since

$$s_{r-\alpha-j} = s_{s+\beta(p-1)-\alpha-j} = s-\alpha-j$$

(in the notation of Lemma 5, Equation (c-b)), and since

$$\mathrm{S}_u = 1 + [s_u = p-1] + \tfrac{1}{p-1}\textstyle\sum_{\mu\in\mathbb{F}_p\setminus\{-1,0\}}(1+[\mu])^{s_u}\sum_{j=1}^{t_u}\binom{t_u}{j}p^j x_\mu^j$$

(this equation is shown in the proof of Lemma 5, Equation (c-b)), we can write $\mathrm{S}_{r-\alpha-j} - \mathrm{S}_{s+\beta(p-1)-\alpha-j}$ as

$$\tfrac{1}{p-1}\textstyle\sum_{\mu\in\mathbb{F}_p\setminus\{-1,0\}}(1+[\mu])^{s-\alpha-j}\sum_{j=1}^{\infty}\left[\binom{t_{r-\alpha-j}}{j} - \binom{t_{s+\beta(p-1)-\alpha-j}}{j}\right]p^j x_\mu^j.$$

Let $b = t_{s+\beta(p-1)-\alpha-j}$, so that

$$t_{r-\alpha-j} = b + \tfrac{r-s-\beta(p-1)}{p-1} = b - \epsilon(1+h_0 p)$$

for some $h_0 \in \mathbb{Z}_p$. Then

$$\begin{aligned}
\tbinom{t_{r-\alpha-j}}{j} - \tbinom{t_{s+\beta(p-1)-\alpha-j}}{j} &= \tbinom{b-\epsilon(1+h_0p)}{j} - \tbinom{b}{j}\\
&= -\epsilon(1+h_0p)\tbinom{b}{j}^{\partial} + \mathsf{O}\big(\epsilon^2 p^{-v_p(j!)}\big)
\end{aligned}$$

for all $j \in \mathbb{Z}_{\geqslant 1}$ (because $p^{v_p(j!)}\binom{X}{j} \in \mathbb{Z}_p[X]$). Since $j - v_p(j!) \geqslant 2$ for $j \in \mathbb{Z}_{\geqslant 2}$ (as shown in the proof of Lemma 5, Equation (c-b)), we have

$$\mathrm{S}_{r-\alpha-j} - \mathrm{S}_{s+\beta(p-1)-\alpha-j} = -A_{s-\alpha-j}\tbinom{b}{1}^{\partial}\epsilon p + \mathsf{O}(\epsilon p^2) = \tfrac{-\epsilon p}{s-\alpha-j} + \mathsf{O}(\epsilon p^2)$$

(where $A_{s-\alpha-j}$ is as in the proof of Lemma 5, Equation (c-b)). Thus

$$\begin{aligned}
&\textstyle\sum_{i>0}\left(\binom{r-\alpha-w}{i(p-1)-w} - \binom{s+\beta(p-1)-\alpha-w}{i(p-1)-w}\right)\\
&\quad= \textstyle\sum_{j=0}^{w}(-1)^j\binom{w}{j}(\mathrm{S}_{r-\alpha-j} - \mathrm{S}_{s+\beta(p-1)-\alpha-j})\\
&\quad= \textstyle\sum_{j=0}^{w}(-1)^j\binom{w}{j}\left(\frac{-\epsilon p}{s-\alpha-j} + \mathsf{O}(\epsilon p^2)\right)\\
&\quad= -\tfrac{(-1)^w w!}{(s-\alpha)_{w+1}}\epsilon p + \mathsf{O}(\epsilon p^2).
\end{aligned}$$

The third equality follows from the equation

$$\textstyle\sum_{j=0}^{w}(-1)^j\binom{w}{j}\frac{1}{s-\alpha-j}=\frac{(-1)^w w!}{(s-\alpha)_{w+1}}.$$

Thus $p(A_{w,0}-S_{w,0}-\epsilon N_{w,0})$ is equal to

$$\tfrac{(-1)^w w!}{(s-\alpha)_{w+1}}\left(\tbinom{s+\beta(p-1)-\alpha}{w}-\tbinom{r-\alpha}{w}\right)\epsilon p+\mathsf{O}\big(\epsilon p^2\big)=\mathsf{O}\big(\epsilon p^2\big).$$

Therefore we have

$$A_{w,j}=S_{w,j}+\epsilon N_{w,j}+\mathsf{O}(\epsilon p)$$

for all $0\leqslant w<2\nu-\alpha$ and $0\leqslant j\leqslant\alpha$, implying that

$$A=S+\epsilon N+\mathsf{O}(\epsilon p).$$

□

Let $B=B_\alpha$ be the $(\alpha+1)\times(\alpha+1)$ matrix defined in Lemma 10. That lemma implies that

$$BS^{sub}=\left([w\in\{1,\dots,\beta\}]\,p^{-[j=0]}\tbinom{s+\beta(p-1)-\alpha+j}{w(p-1)+j}\right)_{0\leqslant w,j\leqslant\alpha}.$$

Let $\overline{Q}$ be the matrix that is obtained from $\overline{BN^{sub}}$ by replacing the rows indexed $1,\dots,\beta$ with the corresponding rows of $\overline{BS^{sub}}$. If $i\in\{1,\dots,\beta\}$ then we can write $\overline{Q}_{i,j}$ as the reduction modulo $p$ of

$$p^{-[j=0]}\tbinom{s+\beta(p-1)-\alpha+j}{i(p-1)+j},$$

which can be simplified as

$$\tbinom{\beta}{i}\cdot\begin{cases}\binom{s-\alpha-\beta+i}{i}^{-1}(-1)^{i+1} & \text{if } j=0,\\ \binom{s-\alpha-\beta+j}{j-i} & \text{if } j>0.\end{cases}$$

If $i\notin\{1,\dots,\beta\}$ then we can write $\overline{Q}_{i,j}$ as the reduction modulo $p$ of

$$\begin{aligned}&p^{-[j=0]}\textstyle\sum_{w=0}^{\alpha}B_{i,w}\sum_v\binom{-j}{w-v}\binom{s+\beta(p-1)-\alpha+j}{v}^{\partial}\sum_{u=0}^{\beta}\binom{s+\beta(p-1)-\alpha+j-v}{u(p-1)+j-v}\\&\quad-[i=0]\tbinom{s+\beta(p-1)-\alpha+j}{j}^{\partial}-[j=0]\textstyle\sum_{w=0}^{\alpha}B_{i,w}\binom{s+\beta(p-1)-\alpha}{w}\frac{(-1)^w w!}{(s-\alpha)_{w+1}}.\end{aligned}$$

Thus $\overline{Q}$ is the matrix $M$ from Lemma 12, and that lemma implies that there is a solution of

$$\overline{Q}(z_0,\dots,z_\alpha)^T=(1,0,\dots,0)^T$$

such that $z_0\neq0$. Let $\overline{u}=(z_0,\dots,z_\alpha)^T$. Then $\overline{u}$ is in $\ker\overline{BS^{sub}}=\ker\overline{S^{sub}}$. Let $\widetilde{u}$ be any lift of $\overline{u}$ with entries in $\mathbb{Z}_p$, so that $BS^{sub}\widetilde{u}$ is zero outside the entries indexed $1,\dots,\beta$, and any non-zero entries of $BS^{sub}\widetilde{u}$ are $\mathsf{O}(p)$. Because $BS^{sub}$ is zero outside the rows indexed $1,\dots,\beta$ and the submatrix

of $BS^{sub}$ consisting of the rows indexed $1, \dots, \beta$ has full rank $\beta$, there is a solution of the equation

$$BS^{sub}y = \tfrac{1}{p}BS^{sub}\widetilde{u},$$

for some vector $y$ with entries in $\mathbb{Z}_p$. Then $u = \widetilde{u} - py$ is a lift of $\overline{u}$ such that $u \in \ker BS^{sub} = \ker S^{sub}$. Moreover, because the submatrix of $\overline{BS^{sub}}$ consisting of the rows indexed $1, \dots, \beta$ has full rank $\beta$, we have

$$\overline{BN^{sub}}\overline{u} + \overline{BS^{sub}}\overline{v} = (1, 0, \dots, 0)^T$$

for some $\overline{v}$ with entries in $\mathbb{F}_p$. Let $v$ be any lift of $\overline{v}$ with entries in $\mathbb{Z}_p$. Then

$$B(S^{sub} + \epsilon N^{sub})(u + \epsilon v) = (\epsilon, 0, \dots, 0)^T + \mathsf{O}(\epsilon p).$$

Since $A = S + \epsilon N + \mathsf{O}(\epsilon p)$, if we write

$$(C_0, C_1/p, \dots, C_\alpha/p)^T = u + \epsilon v,$$

then $C_0$ must be a unit since $z_0 \neq 0$, and $C_j = \mathsf{O}(p)$ for $j > 0$, and

$$BA^{sub}(C_0, C_1/p, \dots, C_\alpha/p)^T = (\epsilon, 0, \dots, 0)^T + \mathsf{O}(\epsilon p).$$

Since the zeroth column of $B$ is $(1, 0, \dots, 0)^T$, the zeroth column of $B^{-1}$ is also $(1, 0, \dots, 0)^T$, and consequently we also have

$$\begin{aligned} &A^{sub}(C_0, C_1/p, \dots, C_\alpha/p)^T \\ &\quad = (\epsilon, 0, \dots, 0)^T + \mathsf{O}(\epsilon p) \\ &\quad = ((\vartheta_0(D_\bullet) - C_{-1})/p, \vartheta_1(D_\bullet)/p, \dots, \vartheta_\alpha(D_\bullet)/p)^T. \end{aligned}$$

Let us choose $C_{-1} = -\epsilon p$, so that

$$(\vartheta_0(D_\bullet)/p, \vartheta_1(D_\bullet)/p, \dots, \vartheta_\alpha(D_\bullet)/p)^T = \mathsf{O}(\epsilon p).$$

Then $\vartheta_\alpha(D_\bullet) = \mathsf{O}\big(p^{t+2}\big)$, which makes

$$v_p(\vartheta') = v_p(C_{-1}) = t + 1.$$

We moreover have

$$\vartheta_w(D_\bullet) = \mathsf{O}\big(p^{t+2}\big)$$

for all $w \in \{0, \dots, \alpha\}$. Since

$$A \equiv S \bmod \epsilon$$

(because the entries of $N$ are integers), and since all rows of $S$ are linear combinations of the rows of $BS$ indexed $1, \dots, \beta$, it follows that every entry

of $A(C_0, C_1/p, \dots, C_\alpha/p)^T$ is $\mathsf{O}(\epsilon)$.[6] Therefore we have

$$\vartheta_w(D_\bullet) = \mathsf{O}\big(p^{t+1}\big)$$

for all $w \in \{\alpha+1, \dots, 2\nu-\alpha-1\}$. So the constants $(C_{-1}, C_0, \dots, C_\alpha)$ are suitable for $v = t+1$ (we omit the fine details of checking that all of the conditions are satisfied).

Therefore we can always find suitable constants $(C_{-1}, C_0, \dots, C_\alpha)$ and suitable $v \in \mathbb{Q}_p$, and that concludes the proof of Proposition 16. ∎

## 12 Final remarks

The proof in Section 11 gives a partial classification of $\overline{V}_{k,a}$ which we summarize in this section.

Theorem 17. *Suppose that $v_p(a) \notin \mathbb{Z}$ and $\nu = \lceil v_p(a) \rceil$ is such that*

$$k \not\equiv 3, 4, \dots, 2\nu, 2\nu+1 \bmod p-1.$$

*Then $\overline{V}_{k,a} \cong \operatorname{ind}(\omega_2^{\overline{k-2\nu+1}}) \otimes \omega^{\nu-1}$ if*

$$v_p(k-s-\beta(p-1)-2) = 0 \text{ for all } \beta \in \{0, \dots, \nu-2\},$$

*and $\overline{V}_{k,a}$ is isomorphic to one of the representations in the set*

$$\left\{ \operatorname{ind}(\omega_2^{\overline{k-2\nu+2l+1}}) \otimes \omega^{\nu-l-1} \,\middle|\, l \in \{0, \dots, \min\{j, \nu-\beta-1\}\} \right\}$$

*if*

$$v_p(k-s-\beta(p-1)-2) = j > 0 \text{ for some } \beta \in \{0, \dots, \nu-2\}.$$

*Proof.* We know by Proposition 16 that $\overline{\Theta}_{k,a}$ is irreducible, and we know from the proof of Proposition 16 that it must be a factor of one of the representations

$$\operatorname{ind}^G \operatorname{sub}(1), \dots, \operatorname{ind}^G \operatorname{sub}(\nu-1), \operatorname{ind}^G \operatorname{quot}(\nu-1). \tag{15}$$

Let us recall that the proof of Proposition 16 is based on finding constants $(C_{-1}, C_0, \dots, C_\alpha)$ and $v \in \mathbb{Q}_p$ that satisfy the five conditions (∗1), (∗2), (∗3), (∗4), (∗5) and such that either $v_p(\vartheta') \leqslant v'$ or $v_p(a) - \alpha < v$. The key point is

[6] Note that it is crucial here that the entries of $N$ be integers. In this case they are since all equations in the proof of the approximation claim hold true for $w < s-\alpha$. If $w \geqslant s-\alpha$ then the equation for $N_{w,j}$ is different—as, for instance,

$$\textstyle\sum_{j=0}^{w} (-1)^j \binom{w}{j} \frac{1}{s-\alpha-j} \neq \frac{(-1)^w w!}{(s-\alpha)_{w+1}}.$$

This is one of the places where the proof breaks down if $s < 2\nu$.

that if $v_p(\vartheta') \leqslant v'$ then we can reach a stronger conclusion than the one in the statement of Proposition 16: that there is some element $\mathrm{gen} \in \mathscr{I}_a$ that represents a generator of $\widehat{N}_\alpha$. In particular, if for $\alpha \in \{1, \dots, \nu-2\}$ the constants we choose in the proof of Proposition 16 satisfy $v_p(\vartheta') \leqslant v'$, then we can eliminate $\mathrm{sub}(\alpha)$ from the list (15). Suppose first that

$$v_p(k-s-\beta(p-1)-2) = 0 \text{ for all } \beta \in \{0, \dots, \nu-2\}.$$

Then, for all $\alpha \in \{1, \dots, \nu-2\}$, the constants we choose come from the second case in the proof of Proposition 16. So $v = 1$ and $v' = \min\{v_p(a) - \alpha, 1\} = 1$, and $v_p(\vartheta') = v_p(\vartheta_\alpha(D_\bullet)) = 1 \leqslant v'$. Thus we can eliminate

$$\mathrm{sub}(1), \dots, \mathrm{sub}(\nu-2)$$

from the list (15), implying that $\overline{\Theta}_{k,a}$ is a factor of one of the representations

$$\mathrm{ind}^G \mathrm{sub}(\nu-1), \mathrm{ind}^G \mathrm{quot}(\nu-1)$$

and hence, due to the classification given in Theorem 2, that

$$\overline{V}_{k,a} \cong \mathrm{ind}(\omega_2^{\overline{k-2\nu+1}}) \otimes \omega^{\nu-1}.$$

Now suppose that

$$v_p(k-s-\beta(p-1)-2) = j > 0 \text{ for some } \beta \in \{0, \dots, \nu-2\}.$$

If $\alpha \in \{1, \dots, \beta-1\}$ then the constants we choose come from the second case in the proof of Proposition 16, so we can similarly eliminate $\mathrm{sub}(\alpha)$ from the list (15). If $\beta = 0$ then the constants we choose come from the third case in the proof of Proposition 16, so $v_p(\vartheta') = j+1$ and $v' = \min\{v_p(a) - \alpha, j+1\}$. Thus if $\alpha < \nu - j - 1$ and $\beta = 0$ then we can eliminate $\mathrm{sub}(\alpha)$ from the list (15). Finally, if $\beta > 0$ and $\alpha \in \{\beta, \dots, \nu-2\}$ then the constants we choose come from the fourth case in the proof of Proposition 16, so $v_p(\vartheta') = j+1$ and $v' = \min\{v_p(a) - \alpha, j+1\}$, implying that if $\alpha < \nu - j - 1$ then we can eliminate $\mathrm{sub}(\alpha)$ from the list (15). To summarize, we can eliminate $\mathrm{sub}(\alpha)$ from the list (15) for all

$$\alpha \in \{1, \dots, \beta-1\} \cup \{1, \dots, \nu-j-2\}.$$

So $\overline{\Theta}_{k,a}$ is a factor of one of the representations

$$\mathrm{ind}^G \mathrm{sub}(\max\{\nu-j-1, \beta\}), \dots, \mathrm{ind}^G \mathrm{sub}(\nu-1), \mathrm{ind}^G \mathrm{quot}(\nu-1)$$

and hence, due to the classification given in Theorem 2, $\overline{V}_{k,a}$ is isomorphic to one of the representations in the set

$$\left\{ \mathrm{ind}(\omega_2^{\overline{k-2\nu+2l+1}}) \otimes \omega^{\nu-l-1} \,\middle|\, l \in \{0, \dots, \min\{j, \nu-\beta-1\}\} \right\}.$$

□

## References


[Ars21] Bodan Arsovski, *On the reductions of certain two-dimensional crystabelline representations*, Res. Math. Sci. 8 (2021), no. 1, paper 12, 50 pp.

[Ars] Bodan Arsovski, *On the reductions of certain two-dimensional crystalline representations, II*, preprint, 2021. https://arxiv.org/abs/1808.03224.

[AS86] Avner Ash and Glenn Stevens, *Modular forms in characteristic $\ell$ and special values of their L-functions*, Duke Math. J. 53 (1986), no. 3, 849–868.

[Ber10] Laurent Berger, *Représentations modulaires de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et représentations galoisiennes de dimension 2*, Astérisque, Société Mathématique de France 330 (2010), 263–279.

[Ber11] Laurent Berger, *Trianguline representations*, Bull. Lond. Math. Soc. 43 (2011), no. 4, 619–635.

[Ber12] Laurent Berger, *Local constancy for the reduction mod p of 2-dimensional crystalline representations*, Bull. Lond. Math. Soc. 44 (2012), no. 3, 451–459.

[BB10] Laurent Berger and Christophe Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbb{Q}_p)$, Astérisque, Société Mathématique de France 330 (2010), 155–211.

[BLZ04] Laurent Berger, Hanfeng Li, and Hui June Zhu, *Construction of some families of two-dimensional crystalline representations*, Math. Ann. 329 (2004), no. 2, 365–377.

[Bha20] Shalini Bhattacharya, *Reduction of certain crystalline representations and local constancy in the weight space*, J. Théor. Nombres Bordeaux 32 (2020), no. 1, 25–47.

[BG15] Shalini Bhattacharya and Eknath Ghate, *Reductions of Galois representations for slopes in* $(1, 2)$, Doc. Math. 20 (2015), 943–987.

[BGR18] Shalini Bhattacharya, Eknath Ghate, and Sandra Rozensztajn, *Reduction of Galois representations of slope 1*, J. Algebra 508 (2018), 98–156.

[Bre03a] Christophe Breuil, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbb{Q}_p)$*, I*, Compos. Math. 138 (2003), no. 2, 165–188.

[Bre03b] Christophe Breuil, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbb{Q}_p)$*, II*, J. Inst. Math. Jussieu 2 (2003), no. 1, 23–58.

[Bre04] Christophe Breuil, *Invariant $\mathscr{L}$ et série spéciale p-adique*, Ann. Sci. Éc. Norm. Supér. (4) 37 (2004), 559–610.

[Buz05] Kevin Buzzard, *Questions about slopes of modular forms*, Astérisque, Société Mathématique de France 298 (2005), 1–15.

[Buz07] Kevin Buzzard, *Eigenvarieties*, London Math. Soc. Lecture Note Ser. 320 (2007), 59–120.

[BG09] Kevin Buzzard and Toby Gee, *Explicit reduction modulo p of certain two-dimensional crystalline representations*, Int. Math. Res. Not. IMRN 12 (2009), 2303–2317.

[BG13] Kevin Buzzard and Toby Gee, *Explicit reduction modulo p of certain two-dimensional crystalline representations, II*, Bull. Lond. Math. Soc. 45 (2013), no. 4, 779–788.

[BG16] Kevin Buzzard and Toby Gee, *Slopes of modular forms*, Families of automorphic forms and the trace formula. Proceedings of the Simons symposium (2016), 93–109.

[BK05] Kevin Buzzard and Lloyd J. P. Kilford, *The 2-adic eigencurve at the boundary of weight space*, Compos. Math. 141 (2005), no. 3, 605–619.

[Che13] Gaëtan Chenevier, *Sur la densité des représentations cristallines du groupe de Galois absolu de* $\mathrm{Gal}(\overline{\mathbb{Q}}_p\mathbb{Q}_p)$, Math. Ann. 335 (2013), 1469–1525.

[Col96] Robert F. Coleman, *Classical and overconvergent modular forms*, Invent. Math. 124 (1996), 215–241.

[Col97] Robert F. Coleman, *p-adic Banach spaces and families of modular forms*, Invent. Math. 127 (1997), 417–479.

[CM98] Robert F. Coleman and Barry Mazur, *The eigencurve*, London Math. Soc. Lecture Note Ser. 254 (1998), 1–113.

[Col08] Pierre Colmez, *Représentations triangulines de dimension 2*, Astérisque, Société Mathématique de France 319 (2008), 213–258.

[CF00] Pierre Colmez and Jean-Marc Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. 140 (2000), 1–43.

[DS74] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids 1*, Ann. Sci. École Norm. Sup. (4) 7 (1974), 507–530.

[Edi92] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. 109 (1992), 563–594.

[Fon94] Jean-Marc Fontaine, *Le corps des périodes p-adiques*, Astérisque, Société Mathématique de France 223 (1994), 59–111.

[GR] Eknath Ghate and Vivek Rai, *Reductions of Galois representations of slope* $\frac{3}{2}$, preprint, 2019. https://arxiv.org/abs/1901.01728.

[Gha] Eknath Ghate, *A zig-zag conjecture and local constancy for Galois representations*, preprint, 2019. https://arxiv.org/abs/1903.08996.

[GG15] Abhijiit Ganguli and Eknath Ghate, *Reductions of Galois representations via the mod p local Langlands correspondence*, J. Number Theory 147 (2015), 250–286.

[GM09] Eknath Ghate and Ariane Mézard, *Filtered modules with coefficients*, Trans. Amer. Math. Soc. 361 (2009), no. 5, 2243–2261.

[Gou01] Fernando Q. Gouvêa, *Where the slopes are?*, J. Ramanujan Math. Soc. 16 (2001), no. 1, 75–99.

[HPS90] Hiroaki Hijikata, Arnold K. Pizer, and Thomas R. Shemanske, *Twists of newforms*, J. Number Theory 35 (1990), 287–324.

[Kil08] Lloyd J. P. Kilford, *On the slopes of the $U_5$ operator acting on overconvergent modular forms*, J. Théor. Nombres Bordeaux 20 (2008), no. 1, 165–182.

[KM12] Lloyd J. P. Kilford and Ken McMurdy, *Slopes of the $U_7$ operator acting on a space of overconvergent modular forms*, LMS J. Comput. Math. 15 (2012), 113–139.

[LWX17] Ruochuan Liu, Daqing Wan, and Liang Xiao, *The eigencurve over the boundary of weight space*, Duke Math. J. 166 (2017), no. 9, 1739–1787.

[RS17] Kenneth A. Ribet and William A. Stein, *Lectures on modular forms and Hecke operators*, 2017. https://wstein.org/books/ribet-stein/main.pdf.

[Roe14] David Roe, *The 3-adic eigencurve at the boundary of weight space*, Int. J. Number Theory 10 (2014), no. 7, 1791–1806.

[Roz18] Sandra Rozensztajn, *An algorithm for computing the reduction of 2-dimensional crystalline representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, Int. J. Number Theory 14 (2018), no. 7, 1857–1894.

[Roz20] Sandra Rozensztajn, *On the locus of 2-dimensional crystalline representations with a given reduction modulo p*, Algebra Number Theory 14 (2020), no. 3, 655–720.

Bodan Arsovski
School of Mathematics and Statistics
University of Sheffield
UK
bodan.arsovski@outlook.com

1980