LOCAL IRREDUCIBILITY ON THE EIGENCURVE

BODAN ARSOVSKI

Abstract. This technical article is a continuation of [Ars21] in which we show the Breuil–Buzzard–Emerton conjecture over the "subtle" components for slopes less than $\frac{p-1}{2}$.

1. Introduction and results

1.1. **Background.** Let p be an odd prime number and $k \geqslant 2$ be an integer, and let a be an element of $\overline{\mathbb{Z}}_p$ such that $v_p(a) > 0$. Let us denote $\nu = \lfloor v_p(a) \rfloor + 1 \in \mathbb{Z}_{>0}$. With this data one can associate a certain two-dimensional crystalline p-adic representation $V_{k,a}$ with Hodge–Tate weights $(0, k-1)$. We give the definition of this representation in section 2 of [Ars21], and we define $\overline{V}_{k,a}$ as the semi-simplification of the reduction modulo the maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{Z}}_p$ of a Galois stable $\overline{\mathbb{Z}}_p$-lattice in $V_{k,a}$ (with the resulting representation being independent of the choice of lattice). The question of computing $\overline{V}_{k,a}$ has been studied extensively, and we refer to the introduction of [Ars21] for a brief exposition of it. Partial results have been obtained by Fontaine, Edixhoven, Breuil, Berger, Li, Zhu, Buzzard, Gee, Bhattacharya, Ganguli, Ghate, et al (see [Ber10], [Bre03a], [Bre03b], [Edi92], [BLZ04], [BG15], [BG09], [BG13], [GG15]). A conjecture of Breuil, Buzzard, and Emerton says the following.

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

The main result of [Ars21] is that this conjecture is true over certain "non-subtle" components of weight space. We say that a weight k belongs to a "non-subtle" component of weight space if and only if

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

Thus there are $\max\{\frac{p-1}{2} - \nu + 1, 0\}$ many "non-subtle" components of weight space. This article is a continuation of [Ars21] in which we also show the conjecture for the "subtle" components for slopes less than $\frac{p-1}{2}$. The main result we show is the following theorem.

Theorem 1. *Conjecture A is true when the slope is less than $\frac{p-1}{2}$.*

2. Computing $\overline{V}_{k,a}$ by computing $\overline{\Theta}_{k,a}$

From now on we assume the notation from sections 2, 3, 4, and 6 of [Ars21]. Moreover, we assume that $k > p^{100}$ as in section 5 of [Ars21]. Theorem 2 in [Ars21] implies that our main theorems can be rewritten in the following equivalent forms. Recall that we assume $p>2$ throughout.

Theorem 2. *If $k\in 2\mathbb{Z}$ and $v_p(a)\in(0,\frac{p-1}{2})\backslash\mathbb{Z}$ then $\overline{\Theta}_{k,a}$ is irreducible.*

Thus our task is to prove theore 2.

3. Combinatorics

Throughout the proof we will refer to the combinatorial results in section 8 of [Ars21]. For convenience, we reproduce the statements here in the form we will use.

Lemma 3. *Suppose throughout this lemma that*

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

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

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

(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

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

(3) If $n\leqslant 0$ then

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

(4) If $n\geqslant 0$ then

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

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

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

(6) If X is a formal variable then

$$\tbinom{X}{t+l}\tbinom{t}{w}=\textstyle\sum_v(-1)^{w-v}\binom{l+w-v-1}{w-v}\binom{X}{v}\binom{X-v}{t+l-v}. \tag{c-f}$$

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

$$\begin{aligned}&\textstyle\sum_i\binom{b-d+l}{i(p-1)+l}\binom{i(p-1)}{w}\\ &=\textstyle\sum_v(-1)^{w-v}\binom{l+w-v-1}{w-v}\binom{b-d+l}{v}\mathrm{M}_{b-d+l-v,l-v}.\end{aligned} \tag{c-g}$$

(7) We have

$$\textstyle\sum_j(-1)^j\binom{y}{j}\binom{y+l-j}{w-j}=(-1)^w\binom{w-l-1}{w}. \tag{c-i}$$

(8) We have

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

(9) We have

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

Lemma 4. *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 $0 \leqslant w < \alpha$. Then*

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

for some polynomial h with integer coefficients.

Lemma 5. *For $\alpha, \lambda, \mu \in \mathbb{Z}_{\geqslant 0}$ let*

$$L_\alpha(\lambda, \mu)$$

be the $(\alpha+1) \times (\alpha+1)$ matrix with entries

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

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

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

Lemma 6. *For $\alpha \in \mathbb{Z}_{\geqslant 0}$ let B_α be the $(\alpha+1) \times (\alpha+1)$ matrix with entries*

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

where $s_1(i,j)$ and $s_2(k,j)$ are the Stirling numbers of the first and second kind, respectively. Let $\{X_{i,j}\}_{i,j \geqslant 0}$ be formal variables. For $\beta \in \mathbb{Z}_{\geqslant 0}$ such that $\alpha \geqslant \beta$ let

$$S(\alpha,\beta) = (S(\alpha,\beta)_{w,j})_{0 \leqslant w,j \leqslant \alpha}$$

be the $(\alpha+1) \times (\alpha+1)$ matrix with entries

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

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

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

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

Lemma 7. *For $u, v, c \in \mathbb{Z}$ let us define*

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

Then

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

Lemma 8. *Let X and Y denote formal variables, and let*

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

be polynomials over $\mathbb{Q}$ of degrees $\alpha - j$, for $1 \leqslant j \leqslant \alpha$. Let

$$M = (M_{w,j})_{0 \leqslant w,j \leqslant \alpha}$$

be the $(\alpha+1) \times (\alpha+1)$ matrix over $\mathbb{Q}(X,Y)$ with entries

$$M_{w,0} = (-1)^w \frac{(Y-X)X_w}{Y_{w+1}},$$

$$M_{w,j} = \sum_v (-1)^{w-v} \binom{j+w-v-1}{w-v} \binom{X+j}{v} \left(\binom{Y+j-v}{j-v} - \binom{X+j-v}{j-v}\right),$$

for $0 \leqslant w \leqslant \alpha$ and $0 < j \leqslant \alpha$. Then the first $\alpha - 1$ entries of

$$Mc = M(Y_\alpha, c_1, \dots, c_\alpha)^T = (d_0, \dots, d_\alpha)^T$$

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

Lemma 9. *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 6. Let M denote the $(\alpha+1)\times(\alpha+1)$ matrix with entries in $\mathbb{F}_p$ such that if $i \in \{1, \ldots, \beta\}$ and $j \in \{0, \ldots, \alpha\}$ then

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

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

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

Then there is a solution of

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

such that $z_0 \neq 0$.

Now let us prove some additional combinatorial results.

Lemma 10. *Suppose that $s, \alpha \in \mathbb{Z}_{\geqslant 0}$ are such that*

$$s \in \{2, 4, \ldots, p-3\} \text{ and } \tfrac{s}{2} \leqslant \alpha < s \text{ and } \alpha \leqslant \tfrac{p-3}{2}.$$

For $w, j \in \mathbb{Z}_{\geqslant 0}$ let $F_{w,j}(z) \in \mathbb{F}_p[z]$ denote the polynomial

$$\textstyle\sum_v (-1)^{w-v} \tbinom{j+w-v-1}{w-v} \tbinom{z-\alpha+j}{v} \overline{\tbinom{s-\alpha+j-v}{\underline{j-v}}} - \tbinom{z-\alpha+j}{j}\tbinom{0}{w} - \tbinom{z-\alpha+j}{s-\alpha}\tbinom{z-s}{w}.$$

Let $C_0(z), \ldots, C_\alpha(z) \in \mathbb{F}_p[z]$ denote the polynomials

$$C_j(z) = \begin{cases} \tbinom{\alpha}{s-\alpha-1}^{-1} \tfrac{s-z}{\alpha+1} & \text{if } j = 0, \\ \tfrac{(-1)^{j+1}}{j+1} \tbinom{s-\alpha-1}{\alpha-j}(z-\alpha) & \text{if } j \in \{1, \ldots, \alpha\}. \end{cases}$$

Let $F_1(z), F_2(z) \in \mathbb{F}_p[z]$ denote the polynomials

$$\begin{aligned} F_1(z) &= \textstyle\sum_{j=0}^{\alpha} C_j(z) F_{w,j}(z), \\ F_2(z) &= -[w=0]\tbinom{s-z-1}{\alpha+1}. \end{aligned}$$

Note that all of these polynomials depend on s and α. Then $F_1(z) = F_2(z)$.

Proof. Let us first show that

$$C_0(z)\tbinom{z-\alpha}{s-\alpha} + \textstyle\sum_{j=1}^{\alpha} C_j(z)\tbinom{z-\alpha+j}{s-\alpha} = \tfrac{(-1)^{\alpha+1}(z-\alpha)}{s-\alpha}. \tag{1}$$

Since

$$C_0(z)\tbinom{z-\alpha}{s-\alpha} = \tbinom{\alpha}{s-\alpha-1}^{-1} \tfrac{s-z}{\alpha+1} \tfrac{z-\alpha}{s-\alpha} \tbinom{z-\alpha-1}{s-\alpha-1},$$

this is equivalent to

$$\tbinom{\alpha}{s-\alpha-1}^{-1} \tfrac{s-z}{\alpha+1} \tbinom{z-\alpha-1}{s-\alpha-1} + \textstyle\sum_{j=1}^{\alpha} \tfrac{(-1)^{j+1}(\alpha-j+1)}{j+1} \tbinom{s-\alpha}{\alpha-j+1} \tbinom{z-\alpha+j}{s-\alpha} = (-1)^{\alpha+1}.$$

The polynomial on the left side has degree at most $s-\alpha$. The coefficient of $z^{s-\alpha}$ in it is $-\frac{(2\alpha-s+1)!}{(\alpha+1)!}$ plus

$$\begin{aligned}\tfrac{1}{(s-\alpha-1)!}\textstyle\sum_j \frac{(-1)^{j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j} &= \tfrac{1}{(s-\alpha-1)!}\textstyle\sum_j \frac{(-1)^{j+1}}{j+1}[X^{s-2\alpha+j-1}](1+X)^{s-\alpha-1}\\ &= \textstyle\sum_j \frac{(-1)^{j+1}}{(j+1)}[X^j]X^{2\alpha-s-1}(1+X)^{s-\alpha-1}\\ &= \tfrac{1}{(s-\alpha-1)!}\textstyle\int_0^{-1} Y^{2\alpha-s+1}(1+Y)^{s-\alpha-1}\,\mathrm{d}Y\\ &= \tfrac{(-1)^s(2\alpha-s+1)!}{(\alpha+1)!}.\end{aligned}$$

Since s is even, that coefficient is zero. Therefore it is enough to show that the two polynomials are equal when evaluated at $z\in\{\alpha+1,\dots,s\}$. At these points the polynomial on the left side is equal to

$$(s-\alpha)\textstyle\sum_j \frac{(-1)^{j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{s-\alpha-\gamma+j}{s-\alpha}$$

for $\gamma\in\{0,\dots,s-\alpha-1\}$. We have

$$\begin{aligned}\textstyle\sum_j \frac{(-1)^{j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{s-\alpha-\gamma+j}{s-\alpha} &= \textstyle\sum_j \frac{(-1)^{s-\alpha+j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{\gamma-j-1}{s-\alpha}\\ &= \textstyle\sum_u \binom{\gamma}{u}\sum_j \frac{(-1)^{s-\alpha+j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{-j-1}{s-\alpha-u}\\ &= \textstyle\sum_u \binom{\gamma}{u}\sum_j \frac{(-1)^{s-\alpha+j}}{s-\alpha-u}\binom{s-\alpha-1}{\alpha-j}\binom{-j-2}{s-\alpha-u-1}\\ &= \textstyle\sum_u \frac{(-1)^{u+1}}{s-\alpha-u}\binom{\gamma}{u}\sum_j \binom{s-\alpha-1}{\alpha-j}\binom{-s+\alpha+u}{j+2}\\ &= \textstyle\sum_u \frac{(-1)^{u+1}}{s-\alpha-u}\binom{\gamma}{u}\binom{u-1}{\alpha+2} = \frac{(-1)^{\alpha+1}}{s-\alpha}.\end{aligned}$$

The third equality follows from $\binom{\gamma}{u}=0$ for $u>s-\alpha-1$, and the last equality follows from $\binom{u-1}{\alpha+2}=0$ for $u\in\{1,\dots,s-\alpha-1\}$. In particular, (1) is indeed true.

So both $F_1(z)$ and $F_2(z)$ have degree at most $\alpha+1$, and therefore they are equal if they are equal when evaluated at

$$z\in\{s+\gamma(p-1)\,|\,\gamma\in\{0,\dots,\alpha+1\}\}.$$

It is easy to verify that $F_1(s)=F_2(s)$, and when

$$z\in\{s+\gamma(p-1)\,|\,\gamma\in\{1,\dots,\alpha+1\}\}$$

the fact that

$$\textstyle\sum_{i=1}^{\gamma-1}\binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = F_{w,j}(s+\gamma(p-1))$$

(due to (c-g)) implies that the equation $F_1(s+\gamma(p-1))=F_2(s+\gamma(p-1))$ is equivalent to

$$\textstyle\sum_{j=0}^{\alpha} C_j(s+\gamma(p-1))\sum_{i=1}^{\gamma-1}\binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = -[w=0]\binom{-\gamma(p-1)-1}{\alpha+1}.$$

Note that $\binom{-\gamma(p-1)-1}{\alpha+1}=\binom{\gamma-1}{\alpha+1}=0$ and therefore the right side vanishes. Let us reiterate that all computations done in this proof are over $\mathbb{F}_p$. Let us write $C_j^\gamma = C_j(s+\gamma(p-1))$. The desired identity

$$\textstyle\sum_{j=0}^{\alpha} C_j^\gamma\sum_{i=1}^{\gamma-1}\binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = 0$$

follows if

$$\textstyle\sum_{j=0}^{\alpha} C_j^\gamma\binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j} = 0$$

for all $i\in\{1,\dots,\gamma-1\}$. If $j>0$ and $C_j^\gamma\neq 0$ then

$$j\geqslant 2\alpha-s+1\geqslant \alpha+\gamma-s$$

and consequently

$$\binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j} = \begin{cases} \binom{\gamma}{i}\binom{s-\alpha-\gamma+j}{s-\alpha-\gamma+i} & \text{if } s-\alpha-\gamma+i \geqslant 0 \\ \binom{\gamma}{i-1}\binom{s-\alpha-\gamma+j}{p+s-\alpha-\gamma+i} & \text{if } s-\alpha-\gamma+i < 0 \end{cases}$$

$$= \binom{\gamma}{i}\binom{s-\alpha-\gamma+j}{s-\alpha-\gamma+i}.$$

On the other hand,

$$\binom{s+\gamma(p-1)-\alpha}{i(p-1)} = \binom{\gamma-1}{i-1}\binom{s-\alpha-\gamma}{s-\alpha-\gamma+i}.$$

Since

$$\binom{\gamma-1}{i-1} = \frac{i}{\gamma}\binom{\gamma}{i} \in \mathbb{F}_p^{\times}$$

(as that $0 < i < \gamma \leqslant \alpha+1$), what we want to show is that

$$C_0^{\gamma}\frac{i}{\gamma}\binom{s-\alpha-\gamma}{s-\alpha-\gamma+i} + \sum_{j=1}^{\alpha} C_j^{\gamma}\binom{s-\alpha-\gamma+j}{s-\alpha-\gamma+i} = 0$$

for all $i \in \{1,\dots,\gamma-1\}$. That is equivalent to

$$F_3(s+\gamma(p-1)) = 0,$$

where $F_3(z) \in \mathbb{F}_p[z]$ is defined as

$$F_3(z) = \binom{\alpha}{s-\alpha-1}^{-1}\frac{s-z-w}{\alpha+1}\binom{z-\alpha-1}{s-\alpha-w-1} + \sum_{j=1}^{\alpha}\frac{(-1)^{j+1}(s-\alpha-w)}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{z-\alpha+j}{s-\alpha-w}$$

with $w = \gamma - i > 0$. The degree of $F_3(z)$ is at most $s-\alpha-w$, and in fact the coefficient of $z^{s-\alpha-w}$ in it is $-\frac{(s-\alpha-1)_w(2\alpha-s+1)!}{(\alpha+1)!}$ plus

$$\frac{1}{(s-\alpha-w-1)!}\sum_j \frac{(-1)^{j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j} = \frac{(s-\alpha-1)_w(2\alpha-s+1)!}{(\alpha+1)!},$$

i.e. the coefficient of $z^{s-\alpha-w}$ in it is zero. Therefore the degree of $F_3(z)$ is less than $s-\alpha-w$, so it is enough to show that $F_3(z)$ is equal to zero when evaluated at

$$z \in \{\alpha+1,\dots,s-w\}.$$

At these points $F_3(z)$ is equal to

$$(s-\alpha-w)\sum_j \frac{(-1)^{j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{s-\alpha-\gamma+j}{s-\alpha-w}$$

for $\gamma \in \{w,\dots,s-\alpha-1\}$. We have

$$\begin{aligned}\sum_j \frac{(-1)^{j+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{s-\alpha-\gamma+j}{s-\alpha-w} &= \sum_j \frac{(-1)^{s-\alpha+j-w+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{\gamma-j-w-1}{s-\alpha-w} \\ &= \sum_u \binom{\gamma-w}{u}\sum_j \frac{(-1)^{s-\alpha+j-w+1}}{j+1}\binom{s-\alpha-1}{\alpha-j}\binom{-j-1}{s-\alpha-u-w} \\ &= \sum_u \binom{\gamma-w}{u}\sum_j \frac{(-1)^{s-\alpha+j-w}}{s-\alpha-u-w}\binom{s-\alpha-1}{\alpha-j}\binom{-j-2}{s-\alpha-u-w-1} \\ &= \sum_u \frac{(-1)^{u+1}}{s-\alpha-u-w}\binom{\gamma-w}{u}\sum_j \binom{s-\alpha-1}{\alpha-j}\binom{-s+\alpha+u+w}{j+2} \\ &= \sum_u \frac{(-1)^{u+1}}{s-\alpha-u-w}\binom{\gamma-w}{u}\sum_j \binom{u+w-1}{\alpha+2} = 0.\end{aligned}$$

The last equality follows from $\binom{\gamma-w}{u} = 0$ for

$$u \notin \{0,\dots,s-\alpha-w-1\}.$$

This proves that indeed $F_3(z) = 0$ and therefore that $F_1(z) = F_2(z)$. ∎

Lemma 11. *Suppose that $\alpha \in \mathbb{Z}_{\geqslant 0}$. For $w, j \in \{0,\dots,\alpha\}$ let*

$$F_{w,j}(z,\psi) \in \mathbb{F}_p[z,\psi]$$

denote the polynomial

$$\sum_v (-1)^{w-v}\binom{j+w-v-1}{w-v}\binom{z-\alpha+j}{v}\left(\binom{\psi-\alpha+j-v}{j-v} - \binom{z-\alpha+j-v}{j-v}\right).$$

Note that this depends on α. Then

$$\textstyle\sum_{j=1}^{\alpha}(-1)^{\alpha-j}\binom{\psi-\alpha+1}{\alpha-j}F_{w,j}(z,\psi)=(-1)^{\alpha}([w=\alpha]-[w=0])\binom{\psi-z}{\alpha}.$$

Proof. Both sides of the equation we want to prove have degree α and the coefficient of z^{α} on each side is $\frac{1}{\alpha!}([w=\alpha]-[w=0])$. So the two sides are equal if they are equal when evaluated at the points (z,ψ) such that

$$(z,\psi)\in\{(u+\gamma(p-1)+\alpha,u+\alpha)\,|\,u\in\{0,\dots,\alpha\},\,\gamma\in\{0,\dots,\alpha-1\}\}.$$

The right side is zero when evaluated at these points, and

$$F_{w,j}(u+\gamma(p-1)+\alpha,u+\alpha)=\textstyle\sum_{i=1}^{\gamma}\binom{u+\gamma(p-1)+j}{i(p-1)+j}\binom{i(p-1)}{w}$$

by (*c-g*). Thus we want to show that

$$\textstyle\sum_{j=1}^{\alpha}(-1)^{\alpha-j}\binom{u+1}{\alpha-j}\sum_{i=1}^{\gamma}\binom{u+\gamma(p-1)+j}{i(p-1)+j}\binom{i(p-1)}{w}=\mathsf{O}(p)$$

for $0\leqslant u,w\leqslant\alpha$ and $0\leqslant\gamma<\alpha$. Since

$$\binom{u+\gamma(p-1)+j}{i(p-1)+j}\binom{i(p-1)}{w}=\binom{\gamma}{i}\binom{u+j-\gamma}{j-i}\binom{-i}{w}+\mathsf{O}(p),$$

that is equivalent to

$$\textstyle\sum_{i,j>0}(-1)^{\alpha+w-i}\binom{u+1}{\alpha-j}\binom{\gamma}{i}\binom{\gamma-u-i-1}{j-i}\binom{i+w-1}{w}=\mathsf{O}(p).$$

This follows from the facts that

$$\textstyle\sum_{j>0}\binom{u+1}{\alpha-j}\binom{\gamma-u-i-1}{j-i}=\binom{\gamma-i}{\alpha-i}$$

for $i>0$ by Vandermonde's convolution formula, and

$$\binom{\gamma}{i}\binom{\gamma-i}{\alpha-i}=\binom{\alpha}{i}\binom{\gamma}{\alpha}=0$$

since $\gamma\in\{0,\dots,\alpha-1\}$. ∎

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

$$s\in\{2,4,\dots,p-3\}\text{ and }\alpha=\beta=\tfrac{s}{2}+1.$$

Let M denote the $(\alpha+1)\times(\alpha+1)$ matrix with entries in $\mathbb{F}_p$ defined in lemma 14. Suppose that $C_0,\dots,C_\alpha\in\mathbb{F}_p$ are defined as

$$C_j=(-1)^{\alpha+j+1}\alpha\binom{\alpha-2}{j-2}.$$

Then

$$M(C_0,\dots,C_\alpha)^T=(0,\dots,0,1)^T.$$

Proof. The equation associated with the ith row of M is straightforward if $i\notin\{0,\alpha\}$. Since $M_{0,j}$ is equal to

$$\textstyle\sum_{l,v=0}^{\alpha}(-1)^{l+v}\binom{j-v}{l-v}\binom{j-2}{v}^{\partial}\binom{\overline{\alpha+j-v-2}}{\underline{j-v}}(1+[\alpha=2\,\&\,j=v])$$
$$-\binom{j-2}{j}^{\partial}-\binom{j-2}{\alpha-2}\binom{0}{\alpha}^{\partial}$$

and since

$$\textstyle\sum_j (-1)^j \binom{\alpha-2}{j-2} \frac{1}{j(j-1)} = \frac{1}{\alpha},$$

$$\textstyle\sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{j-2}{s-\alpha} \binom{0}{\alpha}^{\partial} = (-1)^{\alpha} \binom{0}{\alpha}^{\partial} = -\frac{1}{\alpha},$$

$$\textstyle\sum_l^{\alpha} (-1)^{l+\alpha} \binom{2-\alpha}{l-\alpha} \binom{0}{\alpha}^{\partial} \binom{p-1}{\alpha-2} = -\frac{1}{\alpha},$$

$$\textstyle\sum_l^{\alpha} (-1)^{l+\alpha} \binom{2-\alpha}{l-\alpha} \binom{0}{\alpha}^{\partial} \binom{0}{\alpha-2} = -\frac{[\alpha=2]}{\alpha},$$

the equation associated with the zeroth row is

$$\textstyle\sum_j (-1)^j \binom{\alpha-2}{j-2} \sum_{l,v=0}^{\alpha} (-1)^{l+v} \binom{j-v}{l-v} \binom{j-2}{v}^{\partial} \binom{\alpha+j-v-2}{j-v} = -\frac{1}{\alpha},$$

and it follows from the fact that

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

for $0 \leqslant v \leqslant j \leqslant \alpha$. This shows the equation associated with the zeroth row. Since $M_{\alpha,j}$ is equal to

$$[j=2]\binom{0}{\alpha}^{\partial} + [j=\alpha] F_{\alpha,\alpha,0}(\alpha-2) - \binom{j-2}{\alpha-2}^{\partial} - (-1)^{\alpha} \binom{j-2}{\alpha-2} \binom{-1}{\alpha}^{\partial},$$

the equation associated with the αth row is

$$\binom{0}{\alpha}^{\partial} - \textstyle\sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{j-2}{\alpha-2}^{\partial} = \binom{-1}{\alpha}^{\partial} - (-1)^{\alpha} F_{\alpha,\alpha,0}(\alpha-2) + \frac{(-1)^{\alpha+1}}{\alpha},$$

and it follows from the facts that

$$F_{\alpha,\alpha,0}(\alpha-2) = F_{\alpha,\alpha,0}(-1) = (-1)^{\alpha} \binom{-1}{\alpha}^{\partial}$$

and that the polynomial $\binom{X}{\alpha-2}^{\partial} \in \mathbb{F}_p[X]$ has degree less than $\alpha - 2$ (and is zero if $\alpha = 2$) and therefore

$$\textstyle\sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{j-2}{\alpha-2}^{\partial} = 0.$$

This shows the equation associated with the αth row and concludes the proof. ∎

Lemma 13. *Suppose that $s, \alpha, \beta \in \mathbb{Z}$ are such that*

$$s \in \{2, 4, \ldots, p-3\} \text{ and } \alpha = \tfrac{s}{2} + 1 \text{ and } \beta \in \{\tfrac{s}{2}, \tfrac{s}{2}+1\}.$$

Let A_0 denote the $\beta \times \beta$ matrix with entries in $\mathbb{Q}_p$ defined as

$$A_0 = \left(p^{[j=1]-[i \leqslant \beta-\alpha+1]} \binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} \right)_{0 \leqslant i < \beta,\, \alpha-\beta < j \leqslant \alpha}.$$

Then A_0 has entries in $\mathbb{Z}_p$ and is invertible over $\mathbb{Z}_p$.

Proof. It is easy to verify that A_0 is integral, since if $j > 1$ then

$$s - \alpha - \beta + j \geqslant 0$$

and therefore

$$\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} = \binom{\beta}{i} \binom{s-\alpha-\beta+j}{j-i} + \mathsf{O}(p) = \mathsf{O}(p)$$

for $i \leqslant \beta - \alpha + 1$. Let us show that A_0 is invertible (over $\mathbb{Z}_p$) by showing that $\overline{A}_0$ is invertible (over $\mathbb{F}_p$). Suppose first that $\beta = \alpha - 1$ and denote the columns of A_0 by $\mathbf{c}_2, \ldots, \mathbf{c}_{\alpha}$. The bottom left $(\alpha-3) \times (\alpha-3)$ submatrix of $\overline{A}_0$ is upper triangular with units on the diagonal. Moreover, since

$$\textstyle\sum_j (-1)^j \binom{s-\beta-j-1}{\alpha-i-j-1} \binom{\alpha-2}{j} = \sum_j (-1)^j \binom{\beta-j-1}{i-1} \binom{\beta-1}{j} = 0,$$

$$\textstyle\sum_j (-1)^{j-1} (j-1) \binom{s-\beta-j}{\alpha-i-j} \binom{\alpha-1}{j} = \sum_j (-1)^{j-1} (j-1) \binom{\beta-j}{i-1} \binom{\beta}{j} = 0,$$

all but the top two entries of each of the vectors

$$\begin{aligned}&\mathbf{c}_{\alpha-1} - \tbinom{\alpha-2}{1}\mathbf{c}_{\alpha-2} + \cdots + (-1)^{\alpha-3}\tbinom{\alpha-2}{\alpha-3}\mathbf{c}_2,\\ &\mathbf{c}_{\alpha} - \tbinom{\alpha-1}{2}\mathbf{c}_{\alpha-2} + \cdots + (-1)^{\alpha-3}(\alpha-3)\tbinom{\alpha-1}{\alpha-2}\mathbf{c}_2\end{aligned}$$

are zero. Thus it is enough to show that the 2×2 matrix consisting of those four entries is invertible (over $\mathbb{F}_p$). This 2×2 matrix is

$$\left(\begin{smallmatrix} e_{0,0} & e_{0,1} \\ (-1)^{\beta}\beta & (-1)^{\beta}\beta(\beta-1)\end{smallmatrix}\right)$$

with

$$\begin{aligned} e_{0,0} &= \beta \textstyle\sum_{j=0}^{\beta-1}(-1)^j \binom{\beta-1}{j}\binom{\beta-j-1}{\beta-j}^{\partial} = \sum_{j=0}^{\beta-1} \frac{(-1)^j\beta}{\beta-j}\binom{\beta-1}{j} \\ &= \textstyle\sum_{j=0}^{\beta-1}(-1)^j\binom{\beta}{j} = (-1)^{\beta+1}, \end{aligned}$$

$$\begin{aligned} e_{0,1} &= \beta \textstyle\sum_{j=0}^{\beta}(-1)^{j-1}(j-1)\binom{\beta}{j}\binom{\beta-j}{\beta-j+1}^{\partial} = \sum_{j=0}^{\beta} \frac{(-1)^{j-1}\beta(j-1)}{\beta-j+1}\binom{\beta}{j} \\ &= \textstyle\sum_{j=0}^{\beta} \frac{(-1)^{j-1}\beta(j-1)}{\beta+1}\binom{\beta+1}{j} = \frac{(-1)^{\beta-1}\beta^2}{\beta+1}, \end{aligned}$$

so it has determinant $\frac{\beta}{\beta+1} \in \mathbb{F}_p^{\times}$. Now suppose that $\beta = \alpha$ and denote the columns of A_0 by $\mathbf{c}_1, \ldots, \mathbf{c}_\alpha$. The bottom left $(\alpha-1) \times (\alpha-1)$ submatrix of $\overline{A}_0$ is upper triangular with units on the diagonal, all but the top entry of the vector

$$\mathbf{c}_\alpha - \tbinom{\alpha-2}{1}\mathbf{c}_{\alpha-1} + \cdots + (-1)^{\alpha-2}\tbinom{\alpha-2}{\alpha-2}\mathbf{c}_2$$

are zero, and that top entry is

$$\beta \textstyle\sum_{j=0}^{\beta-2}(-1)^j\binom{\beta-2}{j}\binom{\beta-j-2}{\beta-j}^{\partial} = \sum_{j=0}^{\beta-2}\frac{(-1)^j}{\beta-1}\binom{\beta}{j} = (-1)^{\beta} \in \mathbb{F}_p^{\times}.$$

Therefore $\overline{A}_0$ is invertible. ∎

Lemma 14. *Suppose that* $s, \alpha, \beta \in \mathbb{Z}$ *are such that*

$$s \in \{2, 4, \ldots, p-3\} \text{ and } \tfrac{s}{2} \leqslant \alpha \leqslant s \text{ and } 1 \leqslant \beta \leqslant \alpha.$$

Let M *denote the* $(\alpha+1) \times (\alpha+1)$ *matrix with entries in* $\mathbb{F}_p$ *such that if* $i \in \{1, \ldots, \beta-1\}$ *and* $j \in \{0, \ldots, \alpha\}$ *then*

$$M_{i,j} = \tbinom{s+\beta(p-1)-\alpha+j}{i(p-1)+j},$$

and if $i \in \{0, \ldots, \alpha\} \backslash \{1, \ldots, \beta-1\}$ *and* $j \in \{0, \ldots, \alpha\}$ *then*

$$\begin{aligned} M_{i,j} = &\textstyle\sum_{l,v=0}^{\alpha}(-1)^{i+l+v}\binom{l}{i}\binom{j-v}{l-v}\binom{s-\alpha-\beta+j}{v}^{\partial}\overline{\binom{s-\alpha+j-v}{\underline{j-v}}} \\ &- [i=0]\tbinom{s-\alpha-\beta+j}{j}^{\partial} - [i=\beta]\tbinom{s-\alpha-\beta+j}{s-\alpha}^{\partial} \\ &- (-1)^i\tbinom{s-\alpha-\beta+j}{s-\alpha}\textstyle\sum_{l=0}^{\alpha}\binom{l}{i}\binom{l-\beta-1}{l}^{\partial}. \end{aligned}$$

Suppose that $C_0, \ldots, C_\alpha \in \mathbb{F}_p$ *are defined as*

$$C_j = \begin{cases} 1 & \text{if } j = 0, \\ \frac{(-1)^{j+1}(s-\alpha-\beta)}{\beta}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1} & \text{if } j \in \{1, \ldots, \alpha\}. \end{cases}$$

Then

$$M(C_0, C_1, \ldots, C_\alpha)^T = \left(\frac{(-1)^{\alpha+\beta+1}(s-\alpha)(\alpha-\beta+1)}{\beta^2(2\alpha-s+1)\binom{\alpha}{\beta}}\tbinom{\alpha}{s-\alpha}, 0, \ldots, 0\right)^T.$$

Proof. Let us denote the rows of M by

$$\mathbf{r}_0, \ldots, \mathbf{r}_\alpha.$$

Note that if $j > 0$ and $C_j \neq 0$ then $j > 2\alpha - s$, so $s - \alpha + j > \alpha$ and in particular

$$\overline{\tbinom{s-\alpha+j-v}{\underline{j-v}}} = \tbinom{s-\alpha+j-v}{j-v}.$$

We have the following string of equations:

$$\begin{aligned}
&\textstyle\sum_{j\geqslant 0}(-1)^{j+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{s-\alpha-\beta+j}{s-\alpha} \\
&\quad= \textstyle\sum_u \binom{\beta}{u} \sum_{j\geqslant 0}(-1)^{s-\alpha+j+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{-j-1}{s-\alpha-u} \\
&\quad= \textstyle\sum_u \binom{\beta}{u}\binom{\alpha-u+1}{s-\alpha-u} \sum_{j\geqslant 0}(-1)^{j+u+1}\binom{\alpha+1}{j+1}\binom{s-\alpha+j-u}{\alpha-u+1} \\
&\quad= \textstyle\sum_u \binom{\beta}{u}\binom{\alpha-u+1}{s-\alpha-u}\left((-1)^{u+1}\binom{s-\alpha-u-1}{\alpha-u+1} + \sum_j (-1)^{j+u+1}\binom{\alpha+1}{j+1}\binom{s-\alpha+j-u}{\alpha-u+1}\right) \\
&\quad= \textstyle\sum_u \binom{\beta}{u}\binom{\alpha-u+1}{s-\alpha-u}\left((-1)^{u+1}\binom{s-\alpha-u-1}{\alpha-u+1} + [u=0](-1)^{\alpha+1}\right) \\
&\quad= (-1)^\alpha\left(\tbinom{\beta}{s-\alpha} - \tbinom{\alpha+1}{s-\alpha}\right).
\end{aligned}$$

The first two equalities amount to rewriting the binomial coefficients. The third equality amounts to computing the inner sum. The fourth equality follows from (c-e). The fifth equality amounts to computing the outer sum. This string of equations implies that

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

Our task is to compute $\mathbf{r}_i(C_0, C_1, \ldots, C_\alpha)^T$ for $i \in \{0, \ldots, \alpha\}$.

- *Computing* $\mathbf{r}_0(C_0, C_1, \ldots, C_\alpha)^T$. If $j > 2\alpha - s$ then

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

  for $0 \leqslant v \leqslant j \leqslant \alpha$ and therefore

  $$\begin{aligned}
  M_{0,j} &= \textstyle\sum_{v=0}^{\alpha}(-1)^{j+v}\binom{v}{j}\binom{s-\alpha-\beta+j}{v}^{\partial}\binom{s-\alpha+j-v}{j-v} \\
  &\qquad - \textstyle\binom{s-\alpha-\beta+j}{j}^{\partial} - \binom{s-\alpha-\beta+j}{s-\alpha}\sum_{l=0}^{\alpha}\binom{l-\beta-1}{l}^{\partial} \\
  &= -\textstyle\binom{s-\alpha-\beta+j}{s-\alpha}\sum_{l=0}^{\alpha}\binom{l-\beta-1}{l}^{\partial}.
  \end{aligned}$$

  The second equality follows from the fact that $\binom{v}{j} = 0$ if $v < j$. We also have

  $$\begin{aligned}
  M_{0,0} &= \textstyle\sum_{l,v=0}^{\alpha}(-1)^{l+v}\binom{-v}{l-v}\binom{s-\alpha-\beta}{v}^{\partial}\overline{\binom{s-\alpha-v}{\underline{-v}}} \\
  &\qquad - \textstyle\binom{s-\alpha-\beta}{s-\alpha}\sum_{l=0}^{\alpha}\binom{l-\beta-1}{l}^{\partial} \\
  &= \textstyle\sum_{l,v=0}^{\alpha}(-1)^{\alpha+l+v}\binom{-v}{l-v}\binom{s-\alpha-\beta}{v}^{\partial}\binom{v}{s-\alpha} \\
  &\qquad - \textstyle\binom{s-\alpha-\beta}{s-\alpha}\sum_{l=0}^{\alpha}\binom{l-\beta-1}{l}^{\partial} \\
  &= \textstyle\sum_{l,v=0}^{\alpha}(-1)^{\alpha+l+v}\binom{-v}{l-v}\binom{s-\alpha-\beta}{v}^{\partial}\binom{v}{s-\alpha} \\
  &\qquad + \textstyle\binom{s-\alpha-\beta}{s-\alpha}\sum_{l=0}^{\alpha}(-1)^l\sum_v(-1)^{v+1}\binom{s-\alpha-\beta}{v}^{\partial}\binom{s-\alpha-v}{l-v}.
  \end{aligned}$$

The third equality follows from lemma 7. Thus $\mathbf{r}_0(C_0,\ldots,C_\alpha)^T$ is equal to

$$\begin{aligned}
&\textstyle\sum_{l,v=0}^{\alpha}(-1)^{\alpha+l+v}\binom{s-\alpha-\beta}{v}^{\partial}\left(\binom{-v}{l-v}\binom{v}{s-\alpha}+\frac{s-\alpha-\beta}{\beta}\binom{\alpha+1}{s-\alpha}\binom{s-\alpha-v}{l-v}\right)\\
&\quad=(-1)^{\alpha}\textstyle\sum_{v=0}^{\alpha}\binom{s-\alpha-\beta}{v}^{\partial}\left(\binom{\alpha}{v}\binom{v}{s-\alpha}+\frac{s-\alpha-\beta}{\beta}\binom{\alpha+1}{s-\alpha}\binom{2\alpha-s}{\alpha-v}\right)\\
&\quad=\left(\binom{\alpha}{s-\alpha}+\frac{s-\alpha-\beta}{\beta}\binom{\alpha+1}{s-\alpha}\right)\textstyle\sum_{v=0}^{\alpha}(-1)^{v}\binom{s-\alpha-\beta}{v}^{\partial}\binom{s-\alpha-v-1}{\alpha-v}\\
&\quad=\frac{(-1)^{\alpha+\beta+1}}{\beta\binom{\alpha}{\beta}}\left(\binom{\alpha}{s-\alpha}+\frac{s-\alpha-\beta}{\beta}\binom{\alpha+1}{s-\alpha}\right)\\
&\quad=\frac{(-1)^{\alpha+\beta+1}(s-\alpha)(\alpha-\beta+1)}{\beta^2(2\alpha-s+1)\binom{\alpha}{\beta}}\binom{\alpha}{s-\alpha}.
\end{aligned}$$

The third equality follows from lemma 7. Thus we have computed

$$\mathbf{r}_0(C_0,\ldots,C_\alpha)^T=\frac{(-1)^{\alpha+\beta+1}(s-\alpha)(\alpha-\beta+1)}{\beta^2(2\alpha-s+1)\binom{\alpha}{\beta}}\binom{\alpha}{s-\alpha}.$$

- *Computing* $\mathbf{r}_i(C_0,C_1,\ldots,C_\alpha)^T$ *for* $i\in\{1,\ldots,\beta-1\}$. Let $w\in\mathbb{Z}$ be such that $i=\beta-w\in\{1,\ldots,\beta-1\}$. Then

$$\begin{aligned}
&\textstyle\sum_{j\geqslant 0}\frac{(-1)^{j+1}(s-\alpha-\beta)}{\beta}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{s-\alpha-\beta+j}{s-\alpha-w}\\
&\quad=\textstyle\sum_{u}\binom{\alpha-\beta+1}{u}\sum_{j\geqslant 0}\frac{(-1)^{j+1}(s-\alpha-\beta)}{\beta}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{s-2\alpha+j-1}{s-\alpha-w-u}\\
&\quad=\textstyle\sum_{u}\binom{\alpha-\beta+1}{u}\binom{\alpha-w-u+1}{s-\alpha-w-u}\sum_{j\geqslant 0}\frac{(-1)^{j+1}(s-\alpha-\beta)}{\beta}\binom{j}{\alpha-w-u+1}\binom{\alpha+1}{j+1}\\
&\quad=(-1)^{\alpha-w-u}\frac{s-\alpha-\beta}{\beta}\textstyle\sum_{u}\binom{\alpha-\beta+1}{u}\binom{\alpha-w-u+1}{s-\alpha-w-u}\\
&\quad=\frac{s-\alpha-\beta}{\beta}\textstyle\sum_{u}\binom{\alpha-\beta+1}{u}\binom{s-2\alpha-2}{s-\alpha-w-u}\\
&\quad=\frac{s-\alpha-\beta}{\beta}\binom{s-\alpha-\beta-1}{s-\alpha-w}=-\frac{i}{\beta}\binom{s-\alpha-\beta}{s-\alpha-w}.
\end{aligned}$$

The third equality follows from (*c*-*e*). Consequently, if $i\in\{1,\ldots,\beta-1\}$ then

$$\mathbf{r}_i(C_0,\ldots,C_\alpha)^T=0.$$

- *Computing* $\mathbf{r}_i(C_0,C_1,\ldots,C_\alpha)^T$ *for* $i\in\{\beta,\ldots,\alpha\}$. For these i we have

$$\begin{aligned}
M_{i,0}&=\textstyle\sum_{l,v=0}^{\alpha}(-1)^{\alpha+i+l+v}\binom{l}{i}\binom{v}{s-\alpha}\binom{s-\alpha-\beta}{v}^{\partial}\binom{-v}{l-v}\\
&\qquad-[i=\beta]\binom{s-\alpha-\beta}{s-\alpha}^{\partial}-(-1)^{i}\binom{s-\alpha-\beta}{s-\alpha}\textstyle\sum_{l=0}^{\alpha}\binom{l}{i}\binom{l-\beta-1}{l}^{\partial},
\end{aligned}$$

and for $j>2\alpha-s$ we also have

$$\begin{aligned}
M_{i,j}&=\textstyle\sum_{l,v=0}^{\alpha}(-1)^{i+l+v}\binom{l}{i}\binom{j-v}{l-v}\binom{s-\alpha-\beta+j}{v}^{\partial}\binom{s-\alpha+j-v}{j-v}\\
&\qquad-[i=\beta]\binom{s-\alpha-\beta+j}{s-\alpha}^{\partial}-(-1)^{i}\binom{s-\alpha-\beta+j}{s-\alpha}\textstyle\sum_{l=0}^{\alpha}\binom{l}{i}\binom{l-\beta-1}{l}^{\partial}.
\end{aligned}$$

The identity

$$\begin{aligned}
&\textstyle\sum_{j=0}^{\alpha}(-1)^{j+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{z+s-\alpha+j}{s-\alpha}^{\partial}\\
&\quad=\frac{\partial}{\partial z}\left(\textstyle\sum_{j=0}^{\alpha}(-1)^{j+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{z+s-\alpha+j}{s-\alpha}\right)\\
&\quad=\frac{\partial}{\partial z}\left(\binom{z+s-\alpha-1}{s-\alpha}-\binom{s-2\alpha-2}{s-\alpha}\right)\\
&\quad=\binom{z+s-\alpha-1}{s-\alpha}^{\partial}
\end{aligned}$$

is true over $\mathbb{Q}_p[z]$. By evaluating at $z=-\beta$ we get

$$\sum_{j=1}^{\alpha} C_j \binom{s-\alpha-\beta+j}{s-\alpha}^{\partial} = \frac{s-\alpha-\beta}{\beta}\binom{s-\alpha-\beta-1}{s-\alpha}^{\partial},$$

and consequently

$$\binom{s-\alpha-\beta}{s-\alpha}^{\partial} + \sum_{j=1}^{\alpha} C_j \binom{s-\alpha-\beta+j}{s-\alpha}^{\partial} = \frac{1}{\beta}\binom{s-\alpha-\beta-1}{s-\alpha-1}.$$

This means that $(-1)^{\alpha+i}\beta\mathbf{r}_i(C_0,\ldots,C_\alpha)^T$ is equal to $\Phi(-\beta)$, with

$$\Phi(z) = (\alpha-s)\Phi_1'(z) - \Phi_2(z) + (z+s-\alpha)(\Phi_1'(z)+\Phi_3'(z)+\Phi_4'(z))$$

and

$$\Phi_1(z) = \sum_{l,v=0}^{\alpha}(-1)^{l+v+1}\binom{l}{i}\binom{v}{s-\alpha}\binom{z+s-\alpha}{v}\binom{-v}{l-v},$$

$$\Phi_2(z) = \binom{i-1}{s-\alpha-1}\binom{z+i-1}{i-1},$$

$$\Phi_3(z) = \sum_{l,j,v=0}^{\alpha}(-1)^{\alpha+j+l+v+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{l}{i}\binom{j-v}{l-v}\binom{z+s-\alpha+j}{v}\binom{s-\alpha+j-v}{j-v},$$

$$\Phi_4(z) = \binom{\alpha+1}{s-\alpha}\sum_{l=0}^{\alpha}\binom{l}{i}\binom{z+l-1}{l} = \binom{\alpha+1}{s-\alpha}\binom{z+\alpha}{\alpha-i}\binom{z+i-1}{i}.$$

So we want to show that $\Phi(-\beta)=0$. If $s=\alpha+\beta$ then this equation amounts to

$$\beta\Phi_1'(-\beta)+\Phi_2(-\beta)=0,$$

and indeed

$$\begin{aligned}
\beta\Phi_1'(-\beta) &= \beta\sum_{l,v=0}^{\alpha}(-1)^{l+v+1}\binom{l}{i}\binom{v}{\beta}\binom{0}{v}^{\partial}\binom{-v}{l-v} \\
&= \sum_{l,v=0}^{\alpha}\frac{(-1)^l\beta}{v}\binom{l}{i}\binom{v}{\beta}\binom{-v}{l-v} \\
&= \sum_{l,v=0}^{\alpha}(-1)^l\binom{l}{i}\binom{v-1}{\beta-1}\binom{-v}{l-v} \\
&= \sum_{l,v=0}^{\alpha}([l=0](-1)^{\beta+l+1}+[l=\beta](-1)^l)\binom{l}{i} \\
&= (-1)^{\beta}\binom{\beta}{i} \\
&= [i=\beta](-1)^{\beta} \\
&= -\binom{i-1}{\beta-1}\binom{i-\beta-1}{i-1} = -\Phi_2(-\beta).
\end{aligned}$$

Now suppose that $s\neq\alpha+\beta$. As in the proof of lemma 7 we can simplify $\Phi_1(z)$ to

$$\Phi_1(z) = -\binom{z+s-\alpha}{s-\alpha}\sum_{l=0}^{\alpha}\binom{l}{i}\binom{z+l-1}{l+\alpha-s}.$$

We can also simplify $\Phi_3(z)$ to

$$\begin{aligned}
\Phi_3(z) &= \sum_{j,v=0}^{\alpha}(-1)^{\alpha+v+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{v}{j-i}\binom{z+s-\alpha+j}{v}\binom{s-\alpha+j-v}{j-v} \\
&= \binom{z+i-1}{i}\sum_{j=0}^{\alpha}(-1)^{\alpha+j+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{z+s-\alpha+j}{j-i}.
\end{aligned}$$

Suppose first that $i>\beta$. Then

$$\Phi_1'(-\beta) = -\sum_{l=0}^{\alpha}\binom{l}{i}\left(\binom{s-\alpha-\beta}{s-\alpha}^{\partial}\binom{l-\beta-1}{l+\alpha-s}+\binom{s-\alpha-\beta}{s-\alpha}\binom{l-\beta-1}{l+\alpha-s}^{\partial}\right),$$

$$\Phi_2(-\beta)=0,$$

$$\Phi_3'(-\beta) = \binom{i-\beta-1}{i}^{\partial}\sum_{j=0}^{\alpha}(-1)^{\alpha+j+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{s-\alpha-\beta+j}{j-i},$$

$$\Phi_4'(-\beta) = \binom{\alpha+1}{s-\alpha}\binom{\alpha-\beta}{\alpha-i}\binom{i-\beta-1}{i}^{\partial}.$$

Thus if $s > \alpha + \beta$ then the equation $\Phi(-\beta) = 0$ is equivalent to

$$L_1(s, \alpha, \beta, i) = R_1(s, \alpha, \beta, i)$$

with

$$\begin{aligned} L_1 &:= \textstyle\sum_{l=0}^{\alpha} \binom{l}{\beta+1}\binom{l-\beta-1}{i-\beta-1}\binom{l-\beta-1}{s-\alpha-\beta-1}, \\ R_1 &:= \textstyle\binom{s-\alpha}{\beta+1} \sum_{j=0}^{\alpha} (-1)^{\alpha+j+1} \binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{s-\alpha-\beta+j}{j-i} \\ &\quad + \textstyle\binom{\alpha+1}{\beta+1}\binom{\alpha-\beta}{s-\alpha-\beta-1}\binom{\alpha-\beta}{\alpha-i}. \end{aligned}$$

Let us in fact show that

$$L_1(u, v, w, t) = R_1(u, v, w, t)$$

for all $u, v, w, t \geqslant 0$. We clearly have

$$L_1(u, 0, w, t) = R_1(u, 0, w, t)$$

since both sides are zero, and

$$\begin{aligned} &R_1(u+1, v+1, w, t) - R_1(u, v, w, t) \\ &\qquad - L_1(u+1, v+1, w, t) + L_1(u, v, w, t) \\ &\quad = \textstyle\binom{u-v}{w+1} \frac{u-v}{2v-u+2} \sum_{j=0}^{v} (-1)^{v+j} \binom{j}{2v-u+1}\binom{v+1}{j}\binom{u-v-w+j}{j-t} \\ &\qquad - \textstyle\binom{u-v}{w+1}\binom{v+1}{2v-u+2}\binom{u-w+1}{v-t+1} \\ &\qquad + \textstyle\frac{u-v}{2v-u+2}\binom{v+1}{w+1}\binom{v-w}{u-v-w-1}\binom{v-w+1}{t-w}. \end{aligned}$$

All we need to show is that this is zero for all $u, v, w, t \geqslant 0$, which follows from

$$\begin{aligned} &\textstyle\sum_j (-1)^j \binom{j}{2v-u+1}\binom{v+1}{j}\binom{u-v-w+j}{u-v-w+t} \\ &\quad = \textstyle\sum_{j,e} (-1)^j \binom{v-w+1}{u-v-w+i-e}\binom{j}{2v-u+1}\binom{v+1}{j}\binom{u-2v+j-1}{e} \\ &\quad = \textstyle\sum_{j,e} (-1)^j \binom{v-w+1}{u-v-w+i-e}\binom{j}{2v-u+e+1}\binom{v+1}{j}\binom{2v-u+e+1}{e} \\ &\quad = \textstyle\sum_{j,e} (-1)^{u+e+1} \binom{v-w+1}{u-v-w+t-e}\binom{u-2v-e-2}{j+u-2v-e-1}\binom{v+1}{v-j+1}\binom{2v-u+e+1}{e} \\ &\quad = \textstyle\sum_{e} (-1)^{u+e+1} \binom{v-w+1}{u-v-w+t-e}\binom{u-v-e-1}{u-v-e}\binom{2v-u+e+1}{e} \\ &\quad = \textstyle(-1)^{v+1} \binom{v-w+1}{t-w}\binom{v+1}{u-v}. \end{aligned} \tag{2}$$

Similarly, if $s < \alpha + \beta$ then the equation $\Phi(-\beta) = 0$ is equivalent to

$$L_2(s, \alpha, \beta, i) = R_2(s, \alpha, \beta, i)$$

with

$$\begin{aligned} L_2 &:= \textstyle\sum_{l=\beta+1}^{\alpha} \binom{l}{s-\alpha}\binom{l-\beta-1}{i-\beta-1}, \\ R_2 &:= \textstyle\sum_{j=0}^{\alpha} (-1)^{\alpha+j+1} \binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{s-\alpha-\beta+j}{j-i} + \binom{\alpha+1}{s-\alpha}\binom{\alpha-\beta}{\alpha-i}. \end{aligned}$$

Let us in fact show that

$$L_2(u, v, w, t) = R_2(u, v, w, t)$$

for all $u \geqslant v \geqslant t > w \geqslant 0$. It is easy to verify that

$$L_2(u, t, w, t) = R_2(u, t, w, t),$$

and

$$\begin{aligned} &R_2(u+1,v+1,w,t)-R_2(u,v,w,t)\\ &\qquad -L_2(u+1,v+1,w,t)+L_2(u,v,w,t)\\ &\qquad = \tfrac{u-v}{2v-u+2}\sum_{j=0}^{v}(-1)^{v+j}\tbinom{j}{2v-u+1}\tbinom{v+1}{j}\tbinom{u-v-w+j}{j-t}\\ &\qquad\quad + \tfrac{u-v}{2v-u+2}\tbinom{v+1}{u-v}\tbinom{v-w+1}{t-w}-\tbinom{v+1}{u-v-1}\tbinom{u-w+1}{u-v-w+t}, \end{aligned}$$

which is zero by (2). Finally, suppose that $i=\beta$. Then

$$\begin{aligned} \Phi_1'(-\beta) &= -\sum_{l=0}^{\alpha}\tbinom{l}{\beta}\left(\tbinom{s-\alpha-\beta}{s-\alpha}^{\partial}\tbinom{l-\beta-1}{l+\alpha-s}+\tbinom{s-\alpha-\beta}{s-\alpha}\tbinom{l-\beta-1}{l+\alpha-s}^{\partial}\right),\\ \Phi_2(-\beta) &= (-1)^{\beta+1}\tbinom{\beta-1}{s-\alpha-1},\\ \Phi_3'(-\beta) &= \sum_{j=0}^{\alpha}(-1)^{\alpha+\beta+j+1}\tbinom{j}{2\alpha-s+1}\tbinom{\alpha+1}{j+1}\left(\tbinom{s-\alpha-\beta+j}{j-\beta}^{\partial}-\tbinom{s-\alpha-\beta+j}{s-\alpha}h_\beta\right),\\ \Phi_4'(-\beta) &= (-1)^{\beta}\tbinom{\alpha+1}{s-\alpha}(h_{\alpha-\beta}-h_\beta), \end{aligned}$$

where $h_t = 1+\cdots+\frac{1}{t}$ is the harmonic number for $t\in\mathbb{Z}_{>0}$ and $h_t=0$ for $t\in\mathbb{Z}_{\leqslant 0}$. Since

$$\begin{aligned} &\sum_{j=0}^{\alpha}(-1)^{\alpha+\beta+j+1}\tbinom{j}{2\alpha-s+1}\tbinom{\alpha+1}{j+1}\tbinom{z+s-\alpha+j}{s-\alpha}\\ &\qquad = (-1)^{\alpha+\beta}\left(\tbinom{z+s-\alpha-1}{s-\alpha}-\tbinom{s-2\alpha-2}{s-\alpha}\right), \end{aligned}$$

we can simplify $\Phi_3'(-\beta)$ to

$$\Phi_3'(-\beta)=\sum_{j=0}^{\alpha}(-1)^{\alpha}\tbinom{j}{2\alpha-s+1}\tbinom{\alpha+1}{j+1}\tbinom{\alpha-s-1}{j-\beta}^{\partial}-(-1)^{\beta}\left(\tbinom{\beta}{s-\alpha}-\tbinom{\alpha+1}{s-\alpha}\right)h_\beta.$$

The equation $\Phi(-\beta)=0$ is therefore equivalent to

$$L_3(s,\alpha,\beta)=R_3(s,\alpha,\beta)$$

with

$$\begin{aligned} L_3 &:= \beta\Phi_1'(-\beta),\\ R_3 &:= (s-\alpha-\beta)(\Phi_3'(-\beta)+\Phi_4'(-\beta))-\Phi_2(-\beta). \end{aligned}$$

Let us show that $L_3(u,v,w)=R_3(u,v,w)$ for all $u>v\geqslant w>0$. For $v=w$ this is

$$(-1)^u w\left(\tbinom{w-1}{u-w}^{\partial}\tbinom{-1}{2w-u}-\tbinom{w-1}{u-w}\tbinom{-1}{2w-u}^{\partial}\right)=(2w-u)\tbinom{w}{u-w}h_w+\tbinom{w-1}{u-w-1}.$$

If $u>2w$ then both sides are zero, if $u=2w$ then both sides are 1, and if $2w>u>w$ then both sides are $w(h_{w-1}+\frac{1}{2w-u})$. Thus all we need to do is show that

$$R_3(u+1,v+1,w)-R_3(u,v,w)-L_3(u+1,v+1,w)+L_3(u,v,w)=0$$

for all $u>v\geqslant w>0$. By using the equation

$$\sum_j(-1)^j\tbinom{j}{2v-u+1}\tbinom{v+1}{j}\tbinom{z+u-v-w+j}{j-w}=(-1)^{v+1}\tbinom{v+1}{u-v}\tbinom{z+v-w+1}{v-w+1}$$

we can get rid of the sum $\sum_j$ and, after some simple algebraic manipulations, simplify this to

$$\tbinom{v+1}{w}\left(\tbinom{u-v-w}{u-v}^{\partial}\tbinom{v-w}{2v-u+1}+\tbinom{u-v-w}{u-v}\tbinom{v-w}{2v-u+1}^{\partial}\right)=\tfrac{(-1)^{w+1}(u-v-w)}{w(v-w+1)}\tbinom{v+1}{u-v}.$$

We omit the full tedious details and just mention that since we are able to get rid of the sums $\sum_l$ and $\sum_j$ the aforementioned algebraic manipulations amount to simple cancellations. If $u \geqslant v+w$ then

$$\begin{aligned}\binom{v+1}{w}&\left(\binom{u-v-w}{u-v}^{\partial}\binom{v-w}{2v-u+1}+\binom{u-v-w}{u-v}\binom{v-w}{2v-u+1}^{\partial}\right)\\&=\frac{(-1)^{w+1}(v+1)!(v-w)!(u-v-w)!(w-1)!}{w!(v-w+1)!(2v-u+1)!(u-v-w-1)!(u-v)!}\\&=\frac{(-1)^{w+1}(u-v-w)(v+1)!}{w(v-w+1)(u-v)!(2v-u+1)!}=\frac{(-1)^{w+1}(u-v-w)}{w(v-w+1)}\binom{v+1}{u-v},\end{aligned}$$

and if $u < v+w$ then

$$\begin{aligned}\binom{v+1}{w}&\left(\binom{u-v-w}{u-v}^{\partial}\binom{v-w}{2v-u+1}+\binom{u-v-w}{u-v}\binom{v-w}{2v-u+1}^{\partial}\right)\\&=\frac{(-1)^{w}(v+1)!(w-1)!(v+w-u)!(v-w)!}{w!(v-w+1)!(u-v)!(v+w-u-1)!(2v-u+1)!}\\&=\frac{(-1)^{w+1}(u-v-w)(v+1)!}{w(v-w+1)(u-v)!(2v-u+1)!}=\frac{(-1)^{w+1}(u-v-w)}{w(v-w+1)}\binom{v+1}{u-v}.\end{aligned}$$

We have finally shown that if $i \in \{\beta, \dots, \alpha\}$ then

$$\mathbf{r}_i(C_0, \dots, C_\alpha)^T = 0.$$

■

4. Computing $\overline{\Theta}_{k,a}$

Throughout the proof we use the results from section 9 of [Ars21], which we reproduce here without proofs for convenience.

Lemma 15. *Suppose that $\alpha \in \{0, \dots, \nu-1\}$.*

(1) We have

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

(2) The submodule $\operatorname{im}(T-a) \subset \operatorname{ind}_{KZ}^G \widetilde{\Sigma}_r$ contains

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

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

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

Lemma 16. *Suppose that $\alpha \in \mathbb{Z}$ and $v \in \mathbb{Q}$ are such that*

$$\alpha \in \{0, \dots, \nu - 1\},$$
$$v \leqslant v_p(\vartheta_\alpha(D_\bullet)),$$
$$v' := \min\{v_p(a) - \alpha, v\} \leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } \alpha < w < 2\nu - \alpha,$$
$$v' < v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha.$$

If, for $j \in \mathbb{Z}$,

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

then $v \leqslant v_p(\vartheta_\alpha(\Delta_\bullet)) \leqslant v_p(\Delta_j)$ for all $j \in \mathbb{Z}$, and

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

for some ERR_1 and ERR_2 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 $v_p(F) > v'$.

Lemma 17. *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*

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

satisfy the conditions of lemma 16, i.e.

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

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*

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

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

Let us now prove the following additional results.

Lemma 18. *Let $\{C_l\}_{l\in\mathbb{Z}}$ be any family of elements of $\mathbb{Z}_p$. Suppose that $\alpha \in \mathbb{Z}$ and $v \in \mathbb{Q}$ and the constants*

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

are such that

$$\alpha \in \{0,\dots,\nu-1\},$$
$$v \leqslant v_p(\vartheta_\alpha(D_\bullet)),$$
$$v' := \min\{v_p(a)-\alpha, v\} < v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha.$$

Let

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

Then $\operatorname{im}(T-a)$ contains

$$\begin{aligned}&(\vartheta' + C_{-1}) \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} + C_{-1} \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha}\\ &\quad + \textstyle\sum_{\xi=\alpha+1}^{2\nu-\alpha-1} E_\xi \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\xi h_\xi + F \bullet_{KZ,\overline{\mathbb{Q}}_p} h' + H,\end{aligned} \tag{3}$$

for some h_ξ, h', E_ξ, F, H such that

(1) $E_\xi = \vartheta_\xi(D_\bullet) + \mathsf{O}(p^v) \cup \mathsf{O}(\vartheta_{\alpha+1}(D_\bullet)) \cup \dots \cup \mathsf{O}(\vartheta_{\xi-1}(D_\bullet))$,

(2) if $\underline{\xi+\alpha-s} \leqslant \underline{2\xi-s} \neq 0$ then the reduction modulo $\mathfrak{m}$ of $\theta^\xi h_\xi$ generates N_ξ,

(3) $v_p(F) > v'$, and

(4) $H = \mathsf{O}\big(p^{\nu-v_p(a)+v} + p^{\nu-\alpha}\big)$ and if $v_p(a)-\alpha < v$ then

$$\tfrac{1-p}{ap^{-\alpha}} H = g \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} + \mathsf{O}\big(p^{\nu-v_p(a)}\big)$$

with

$$g = \textstyle\sum_{\lambda\in\mathbb{F}_p} C_0 \left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right) + A\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right) + [r \equiv_{p-1} 2\alpha] B \left(\begin{smallmatrix} 0 & 1 \\ p & 0\end{smallmatrix}\right),$$

where

$$A = -C_{-1} + \textstyle\sum_{l=1}^{\alpha} C_l \binom{r-\alpha+l}{l}$$

and

$$B = \textstyle\sum_{l=0}^{\alpha} C_l \binom{r-\alpha+l}{s-\alpha}.$$

Proof. This lemma is essentially shown under a stronger hypothesis as lemma 17. The stronger hypothesis consists of the three extra conditions that $v_p(\vartheta_w(D_\bullet)) \geqslant \min\{v_p(a)-\alpha, v\}$ for all $\alpha < w < 2\nu-\alpha$, that $C_0 \in \mathbb{Z}_p^\times$, and that $v_p(C_{-1}) \geqslant v_p(\vartheta')$. These extra conditions are not used in the actual construction of the element in (3), rather they are there to ensure that $v_p(E_\xi) \geqslant \min\{v_p(a)-\alpha, v\}$ for all $\alpha < \xi < 2\nu-\alpha$, that the coefficient of $\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right)$ in g is invertible, and that we get an integral element once we divide the element

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

by ϑ'. Therefore we still get the existence of the element in (3) without these extra conditions, and to complete the proof of lemma 18 we need to verify the properties of h_ξ, E_ξ, F, H, A, and B claimed in (1), (2), (3), and (4). The h_ξ and E_ξ come from the proof of lemma 16, and $E_\xi \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\xi h_\xi$ is

$$X_\xi \bullet_{KZ,\overline{\mathbb{Q}}_p} \textstyle\sum_{\lambda\neq 0} [-\lambda]^{r-\alpha-\xi} \left(\begin{smallmatrix} 1 & [\lambda] \\ 0 & 1\end{smallmatrix}\right)(-\theta)^n x^{r-np-\xi} y^{\xi-n},$$

with the notation for X_ξ from the proof of lemma 16. Let $E_\xi = (-1)^{\xi+1}X_\xi$. Then condition (1) is satisfied directly from the definition of X_ξ. Let

$$h_\xi = (-1)^{\xi+1}\textstyle\sum_{\lambda\neq 0}[-\lambda]^{r-\alpha-\xi}\left(\begin{smallmatrix}1 & [\lambda]\\ 0 & 1\end{smallmatrix}\right)(-\theta)^n x^{r-np-\xi}y^{\xi-n}.$$

This reduces modulo $\mathfrak{m}$ to the element

$$(-1)^{\xi}\textstyle\sum_{\lambda\neq 0}[-\lambda]^{r-\alpha-\xi}\left(\begin{smallmatrix}1 & [\lambda]\\ 0 & 1\end{smallmatrix}\right)Y^{\underline{2\xi-r}} = (-1)^{s-\alpha+1}\binom{\underline{2\xi-s}}{\underline{\xi+\alpha-s}}X^{\underline{\xi+\alpha-s}}Y^{\underline{\xi-\alpha}}$$

of

$$\sigma_{\underline{2\xi-r}}(r-\xi) \cong I_{r-2\xi}(\xi)/\sigma_{\overline{r-2\xi}}(\xi) = \mathrm{quot}(\xi).$$

This element is non-trivial and generates N_ξ if $\underline{\xi+\alpha-s} \leqslant \underline{2\xi-s} \neq 0$, since then $X^{\underline{\xi+\alpha-s}}Y^{\underline{\xi-\alpha}}$ generates N_ξ. This verifies condition (2). Condition (3) follows from the assumption $v' < v_p(\vartheta_w(D_\bullet))$ for $0 \leqslant w < \alpha$, as in the proof of lemma 16. Finally, condition (4) follows from the description of the error term in lemma 15, as in the proof of lemma 17. ∎

Corollary 19. *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*

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

are such that

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

Suppose also that $v_p(a) \notin \mathbb{Z}$. Let

$$\vartheta' := (1-p)^{-\alpha}\vartheta_\alpha(D_\bullet) - C_{-1},$$
$$\check{C} := -C_{-1} + \textstyle\sum_{l=1}^{\alpha} C_l\binom{r-\alpha+l}{l}.$$

If $\star$ then $*$ is trivial modulo $\mathscr{I}_a$, for each of the following pairs

$$(\star, *) = (\textit{condition}, \textit{representation}).$$

(1) $\Big(v_p(\vartheta') \leqslant \min\{v_p(C_{-1}), v'\},\ \widehat{N}_\alpha\Big)$.

(2) $\Big(v = v_p(C_{-1}) < \min\{v_p(\vartheta'), v_p(a)-\alpha\},\ \mathrm{ind}_{KZ}^G\,\mathrm{sub}(\alpha)\Big)$.

(3) $\Big(v_p(a)-\alpha < v \leqslant v_p(C_{-1})$ *&* $\check{C} \in \mathbb{Z}_p^\times$ *&* $C_0 \notin \mathbb{Z}_p^\times$ *&* $\underline{2\alpha-r} > 0,\ \widehat{N}_\alpha\Big)$.

(4) $\Big(v_p(a)-\alpha < v \leqslant v_p(C_{-1})$ *&* $\check{C} \in \mathbb{Z}_p^\times,\ \mathrm{ind}_{KZ}^G\,\mathrm{quot}(\alpha)\Big)$.

(5) $\Big(v_p(a)-\alpha < v \leqslant v_p(C_{-1})$ *&* $C_0 \in \mathbb{Z}_p^\times,\ \mathbf{r}_1\Big)$, *where*

$$\mathbf{r}_1$$

is a finite-codimensional submodule of

$$T(\mathrm{ind}_{KZ}^G\,\mathrm{quot}(\alpha)).$$

Proof. There is one extra condition imposed in addition to the conditions from lemma 18: that

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

and it ensures that $v_p(E_\xi) \geqslant v'$ for all $\alpha < \xi < 2\nu - \alpha$. Lemma 18 implies that the element in (3) is in $\operatorname{im}(T - a)$. Let us call this element γ.

(1) The condition $v_p(\vartheta') \leqslant \min\{v_p(C_{-1}), v'\}$ ensures that if we divide γ by ϑ' then the resulting element reduces modulo $\mathfrak{m}$ to a representative of a generator of $\widehat{N}_\alpha$.

(2) The condition $v = v_p(C_{-1}) < \min\{v_p(\vartheta'), v_p(a) - \alpha\}$ ensures that if we divide γ by C_{-1} then the resulting element reduces modulo $\mathfrak{m}$ to a representative of a generator of $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha)$.

(3, 4, 5) The condition $v_p(a) - \alpha < v \leqslant v_p(C_{-1})$ ensures that the term with the dominant valuation in (3) is H, so we can divide γ by $ap^{-\alpha}$ and obtain the element $L + \mathsf{O}\big(p^{\nu - v_p(a)}\big)$, where L is defined by

$$L := \Big(\textstyle\sum_{\lambda \in \mathbb{F}_p} C_0\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right) + A\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) + [r \equiv_{p-1} 2\alpha] B\left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)\Big) \bullet_{KZ, \overline{\mathbb{Q}}_p} \theta^n x^{\alpha - n} y^{r - np - \alpha}$$

with A and B as in lemma 18. This element L is in $\operatorname{im}(T - a)$, and it reduces modulo $\mathfrak{m}$ to a representative of

$$\Big(\textstyle\sum_{\lambda \in \mathbb{F}_p} C_0\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right) + A\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) + [r \equiv_{p-1} 2\alpha](-1)^{r-\alpha} B\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Big) \bullet_{KZ, \overline{\mathbb{F}}_p} X^{\underline{2\alpha - r}}.$$

As shown in the proof of lemma 17, if $C_0 \in \mathbb{Z}_p^\times$ then this element always generates a finite-codimensional submodule of

$$T(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha)),$$

and if additionally $A \neq 0$ (over $\mathbb{F}_p$) then in fact we have the stronger conclusion that it generates

$$\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha).$$

Suppose on the other hand that $C_0 = \mathsf{O}(p)$ and $A \in \mathbb{Z}_p^\times$. In that case we assume that $\underline{2\alpha - r} > 0$ and therefore the reduction modulo $\mathfrak{m}$ of L represents a generator of $\widehat{N}_\alpha$. ■

5. Proof of theorem 2

We prove theorem 2 by proving nine propositions which give just enough information to conclude that $\overline{\Theta}_{k,a}$ is irreducible, but not enough to classify it fully.

We assume that

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

for some $\beta \in \{0, \ldots, p-1\}$ and $u_0 \in \mathbb{Z}_p^\times$ and $t \in \mathbb{Z}_{>0}$, and we write $\eta = u_0 p^t$. As the main result of [Ars21] implies theorem 2 for $s \geqslant 2\nu$, we may assume that

$$s \in \{2, \ldots, 2\nu - 2\}.$$

Recall also that we assume $\nu - 1 < v_p(a) < \nu$ for some $\nu \in \{1, \ldots, \frac{p-1}{2}\}$, and that $k > p^{100}$ (and consequently $r > p^{99}$).

We now give a list of nine propositions, and show that their union implies theorem 2.

Proposition 20. *If* $\alpha < \frac{s}{2}$ *then*

$$\begin{cases} \widehat{N}_\alpha & \text{if } \beta \in \{0,\dots,\alpha-1\} \text{ and } \alpha > v_p(a)-t, \\ \operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha) & \text{otherwise} \end{cases}$$

is trivial modulo $\mathscr{I}_a$.

Proposition 21. *If* $\frac{s}{2} \leqslant \alpha < s$ *and* $\beta \notin \{1,\dots,\alpha+1\}$ *then*

$$\widehat{N}_\alpha$$

is trivial modulo $\mathscr{I}_a$.

Proposition 22. *If* $0 < \alpha < \frac{s}{2}$ *then*

$$\begin{cases} T(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha)) & \text{if } \beta \in \{0,\dots,\alpha\} \text{ and } \alpha > v_p(a)-t, \\ \widehat{N}_{s-\alpha} & \text{if } \beta \in \{0,\dots,\alpha\} \text{ and } \alpha < v_p(a)-t, \\ \widehat{N}_\alpha & \text{if } \beta \in \{\alpha+1,\dots,s-\alpha\}, \\ \widehat{N}_{s-\alpha} & \text{if } \beta > s-\alpha \end{cases}$$

is trivial modulo $\mathscr{I}_a$.

Proposition 23. *If* $\frac{s}{2} \leqslant \alpha < s$ *and* $(\alpha,\beta) \neq (\frac{s}{2}, \frac{s}{2}+1)$ *then*

$$\begin{cases} T(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha)) & \text{if } \beta \in \{1,\dots,s-\alpha\} \text{ and } s-\alpha > v_p(a)-t, \\ T(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha)) & \text{if } \beta \in \{s-\alpha+1,\dots,\alpha\} \text{ and } \alpha > v_p(a)-t, \\ \widehat{N}_\alpha & \text{otherwise} \end{cases}$$

is trivial modulo $\mathscr{I}_a$.

Proposition 24. *If* $\alpha \geqslant s$ *then*

$$\begin{cases} T(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha)) & \text{if } \alpha = \max\{\nu-t-1, \beta-1\}, \\ \widehat{N}_\alpha & \text{otherwise} \end{cases}$$

is trivial modulo $\mathscr{I}_a$.

Proposition 25. *If* $\beta \in \{1,\dots,\frac{s}{2}-1\}$ *and* $t > \nu - \frac{s}{2} - 2$ *then*

$$\widehat{N}_{s/2+1}$$

is trivial modulo $\mathscr{I}_a$.

Proposition 26. *If* $\beta \in \{1,\dots,\frac{s}{2}-1\}$ *and* $t = \nu - \frac{s}{2}$ *then*

$$\widehat{N}_{s/2-1}$$

is trivial modulo $\mathscr{I}_a$.

Proposition 27. *If* $\beta \in \{\frac{s}{2}, \frac{s}{2}+1\}$ *and* $t > \nu - \frac{s}{2} - 1$ *then*

$$\widehat{N}_{s/2+1}$$

is trivial modulo $\mathscr{I}_a$.

Proposition 28. *If* $\beta = \frac{s}{2}+1$ *and* $t = \nu - \frac{s}{2} - 1$ *then*

$$\operatorname{ind}_{KZ}^G \operatorname{sub}(\tfrac{s}{2}+1)$$

is trivial modulo $\mathscr{I}_a$.

Proof that propositions 20–28 imply theorem 2. Let us assume that $\overline{\Theta}_{k,a}$ is reducible with the goal of reaching a contradiction. The classification given by theorem 2 in [Ars21] implies that $\overline{\Theta}_{k,a}$ has two infinite-dimensional factors, each of which is a quotient of a representation in the set

$$\{\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha) \,|\, 0 \leqslant \alpha < \nu\} \cup \{\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha) \,|\, 0 \leqslant \alpha < \nu\},$$

and moreover that the following classification is true.

(1) If the two representations are $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha_1)$ and $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha_2)$ then
$$\alpha_1 + \alpha_2 \equiv_{p-1} s + 1.$$
(2) If the two representations are $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha_1)$ and $\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha_2)$ then
$$\alpha_1 - \alpha_2 \equiv_{p-1} 1.$$
(3) If the two representations are $\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha_1)$ and $\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha_2)$ then
$$\alpha_1 + \alpha_2 \equiv_{p-1} s - 1.$$

The facts that

$$\alpha_1 + \alpha_2 \in \{0, \dots, 2\nu - 2\} \subseteq \{0, \dots, p-3\},$$
$$\alpha_1 - \alpha_2 \in \{1 - \nu, \dots, \nu - 1\} \subseteq \{-\tfrac{p-3}{2}, \dots, \tfrac{p-3}{2}\},$$
$$s \in \{2, \dots, 2\nu - 2\} \subseteq \{2, \dots, p-3\}$$

imply that the following classification is true as well.

(1) If the two representations are $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha_1)$ and $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha_2)$ then
$$\alpha_1 + \alpha_2 = s + 1.$$
(2) If the two representations are $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha_1)$ and $\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha_2)$ then
$$\alpha_1 = \alpha_2 + 1.$$
(3) If the two representations are $\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha_1)$ and $\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha_2)$ then
$$\alpha_1 + \alpha_2 = s - 1.$$

This classification and propositions 20, 21, 22, 23, and 24 together imply that one of the two representations must be either $\operatorname{ind}_{KZ}^G \operatorname{sub}(\frac{s}{2})$ or $\operatorname{ind}_{KZ}^G \operatorname{quot}(\frac{s}{2})$, and in that case the other representation is either

$$\operatorname{ind}_{KZ}^G \operatorname{sub}(\tfrac{s}{2} + 1)$$

(which can only happen if $\beta \in \{1, \dots, \frac{s}{2} - 1\}$ and $t > \nu - \frac{s}{2}$ or $\beta \in \{\frac{s}{2}, \frac{s}{2} + 1\}$ and $t > \nu - \frac{s}{2} - 2$), or

$$\operatorname{ind}_{KZ}^G \operatorname{quot}(\tfrac{s}{2} - 1)$$

(which can only happen if $s = 2$ or $\beta \in \{1, \dots, \frac{s}{2} - 1\}$ and $t = \nu - \frac{s}{2}$). In the latter case if $s = 2$ then either $1 \bullet_{KZ, \overline{\mathbb{Q}}_p} x^2 y^{r-2} \in \mathscr{I}_a$ generates $\operatorname{ind}_{KZ}^G \operatorname{quot}(0)$, or $\nu \leqslant 2$ in which case $\overline{V}_{k,a}$ is known to be irreducible. Propositions 23, 25, 26, 27, and 28 exclude all of the remaining possibilities. Thus if we assume that $\overline{\Theta}_{k,a}$ is reducible we reach a contradiction, so $\overline{\Theta}_{k,a}$ must be irreducible. ∎

Proof of proposition 20. First suppose that $\beta \geqslant \alpha$. We apply part (2) of corollary 19 with $v = 0$ and

$$C_j = \begin{cases} (-1)^\alpha \binom{s-r}{\alpha} & \text{if } j = -1, \\ 0 & \text{if } j = 0, \\ (-1)^{\alpha-j}\binom{s-\alpha+1}{\alpha-j} & \text{if } j \in \{1, \ldots, \alpha\}. \end{cases}$$

Since

$$\tbinom{s-r}{\alpha} = \tbinom{\beta}{\alpha} + \mathsf{O}(p) \in \mathbb{Z}_p^\times,$$

the two conditions we need to verify are $v_p(\vartheta_w(D_\bullet)) > 0$ for $0 \leqslant w < \alpha$ and $v_p(\vartheta') > 0$. These two conditions are equivalent to the system of equations

$$\begin{aligned} &\textstyle\sum_{j=1}^{\alpha}(-1)^{\alpha-j}\binom{s-\alpha+1}{\alpha-j}\sum_{i>0}\binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} \\ &\qquad = (-1)^\alpha([w=\alpha]-[w=0])\tbinom{s-r}{\alpha} + \mathsf{O}(p) \end{aligned} \tag{4}$$

for $0 \leqslant w \leqslant \alpha$. Let $F_{w,j}(z,\psi) \in \mathbb{F}_p[z,\psi]$ denote the polynomial defined in lemma 11. Since

$$\textstyle\sum_{i>0}\binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = F_{w,j}(r,s)$$

by (*c*-*g*), the conclusion of that lemma when evaluated at $z = r$ and $\psi = s$ implies (4). Thus if $\beta \geqslant \alpha$ then we can apply part (2) of corollary 19 and conclude that $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha)$ is trivial modulo $\mathscr{I}_a$.

Suppose now that $\beta \in \{0, \ldots, \alpha-1\}$. If $t > v_p(a) - \alpha$ then the proof of theorem 17 in [Ars21] applies here nearly verbatim since

$$\tbinom{s-\alpha+1}{\alpha} \in \mathbb{Z}_p^\times,$$

and in fact we can conclude that $\widehat{N}_\alpha$ is trivial modulo $\mathscr{I}_a$. So let us suppose that $t < v_p(a) - \alpha$. We apply part (2) of corollary 19 with $v = t$ and

$$C_j = \begin{cases} (-1)^\alpha \binom{s-r}{\alpha} & \text{if } j = -1, \\ 0 & \text{if } j = 0, \\ (-1)^{\alpha-j}\binom{s-\alpha+1}{\alpha-j} + pC_j^* & \text{if } j \in \{1, \ldots, \alpha\}, \end{cases}$$

for some constants $C_1^*, \ldots, C_\alpha^*$ yet to be chosen. Clearly

$$v_p(C_{-1}) = t < v_p(a) - \alpha,$$

and the other conditions that need to be satisfied in order for corollary 19 to be applicable are

$$\begin{aligned} &t < v_p(\vartheta'), \\ &t \leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } \alpha \leqslant w < 2\nu - \alpha, \\ &t < v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha. \end{aligned}$$

Let us consider the matrix $A = (A_{w,j})_{0 \leqslant w,j \leqslant \alpha}$ that has integer entries

$$A_{w,j} = \textstyle\sum_{0<i(p-1)<r-2\alpha}\binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w}.$$

Then exactly as in the proof of theorem 17 in [Ars21] we can show that

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

where

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

We still have equation 4 since the constants are the same, and since

$$\binom{s-r}{\alpha} = \mathsf{O}(p),$$

we have

$$S(C_0,\dots,C_\alpha)^T = (\mathsf{O}(p),\dots,\mathsf{O}(p))^T.$$

Let $B = B_\alpha$ be the $(\alpha+1)\times(\alpha+1)$ matrix defined in lemma 6. That lemma implies that B encodes precisely the row operations that transform S into a matrix with zeros outside the rows indexed $1,\dots,\beta$ and such that

$$(BS)_{w,j} = p^{-[j=0]}\binom{s+\beta(p-1)-\alpha+j}{w(p-1)+j}$$

when $w \in \{1,\dots,\beta\}$. We thus have

$$BS(C_0,\dots,C_\alpha)^T = (0,\mathsf{O}(p),\dots,\mathsf{O}(p),0,\dots)^T,$$

where the only entries of the vector on the right that can possibly be non-zero are the ones indexed $1,\dots,\beta$. As in the proof of theorem 17 in [Ars21] we note that S has rank β and therefore we can choose $C_1^*,\dots,C_\alpha^*$ in a way that $(C_0,\dots,C_\alpha)^T \in \ker BS$. Then $\vartheta_w(D_\bullet) = \mathsf{O}(\epsilon)$ for all w, and the conditions that need to be satisfied are $\vartheta_w(D_\bullet) = \mathsf{O}(\epsilon p)$ for $0 \leqslant w < \alpha$ and $\vartheta' = \mathsf{O}(\epsilon p)$. These two conditions are equivalent to the single equation

$$A(C_0,\dots,C_\alpha)^T = (-C_{-1},0,\dots,0,C_{-1}) + \mathsf{O}(\epsilon p),$$

which is itself equivalent to

$$\begin{aligned} &BN(C_0,\dots,C_\alpha)^T \\ &\qquad = \left(0,-\tbinom{\alpha}{1}(C_{-1}\epsilon^{-1}),\dots,(-1)^\alpha\tbinom{\alpha}{\alpha}(C_{-1}\epsilon^{-1})\right)^T + BSv + \mathsf{O}(p) \end{aligned}$$

for some v. Thus, if $\overline{R}$ is the $\alpha\times\alpha$ matrix over $\mathbb{F}_p$ obtained from $\overline{BN}$ by replacing the rows indexed $1,\dots,\beta$ with the corresponding rows of $\overline{BS}$ and then discarding the zeroth row and the zeroth column, the condition that needs to be satisfied is equivalent to the claim that

$$\left(-(1-[1\leqslant\beta])\tbinom{\alpha}{1},\dots,(-1)^\alpha(1-[\alpha\leqslant\beta])\tbinom{\alpha}{\alpha}\right)^T$$

is in the image of $\overline{R}$ (since $C_0 = \mathsf{O}(p)$ and $C_{-1}\epsilon^{-1} \in \mathbb{Z}_p^\times$). This is indeed the case since $\overline{R}$ is the lower right $\alpha\times\alpha$ submatrix of the matrix $\overline{Q}$ defined in the proof of theorem 17 in [Ars21] (where it is shown that $\overline{Q}$ is equal to the matrix M from lemma 9) and is therefore upper triangular with units on the diagonal. Thus we can apply part (2) of corollary 19 with $v = t$ and conclude that $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha)$ is trivial modulo $\mathscr{I}_a$. ∎

Proof of proposition 21. Let us define $C_{-1}(z), \dots, C_\alpha(z) \in \mathbb{Z}_p[z]$ as

$$C_j(z) = \begin{cases} \binom{s-z-1}{\alpha+1} & \text{if } j = -1, \\ \binom{\alpha}{s-\alpha-1}^{-1} \frac{s-z}{\alpha+1} & \text{if } j = 0, \\ \frac{(-1)^{j+1}}{j+1} \binom{s-\alpha-1}{\alpha-j}(z-\alpha) & \text{if } j \in \{1, \dots, \alpha\}. \end{cases}$$

We apply part (1) of corollary 19 with $v = 0$ and

$$(C_{-1}, C_0, \dots, C_\alpha) = (C_{-1}(r), C_0(r), \dots, C_\alpha(r)).$$

The two conditions we need to verify are $v_p(\vartheta_w(D_\bullet)) > 0$ for $0 \leqslant w < \alpha$ and $v_p(\vartheta') = 0$. These two conditions follow from the system of equations

$$\sum_{j=0}^{\alpha} C_j \sum_{0<i(p-1)<r-2\alpha} \binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = -[w=0]\binom{s-r-1}{\alpha+1} + \mathsf{O}(p) \tag{5}$$

for $0 \leqslant w \leqslant \alpha$. Let $F_{w,j}(z) \in \mathbb{F}_p[z]$ denote the polynomial

$$\sum_v (-1)^{w-v}\binom{j+w-v-1}{w-v}\binom{z-\alpha+j}{v}\overline{\binom{s-\alpha+j-v}{\underline{j-v}}} - \binom{z-\alpha+j}{j}\binom{0}{w} - \binom{z-\alpha+j}{s-\alpha}\binom{z-s}{w}.$$

By (*c*-*g*),

$$\sum_{0<i(p-1)<r-2\alpha} \binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = F_{w,j}(r),$$

so the conclusion of lemma 10 evaluated at $z = r$ implies (5). Thus we can apply part (1) of corollary 19 and conclude that $\widehat{N}_\alpha$ is trivial modulo $\mathscr{I}_a$. ∎

Proof of proposition 22. First let us assume that $\beta \in \{0, \dots, \alpha\}$. If we attempt to copy the proof of theorem 17 in [Ars21] in this setting, the one place where we run into problems is that some entries of the extended associated matrix N are not integers (i.e. when we extend the number of rows in A, S, and N to $2\nu - \alpha$ by defining $A_{w,j}$, $S_{w,j}$, and $N_{w,j}$ with the same equations used for the first $\alpha + 1$ rows, we get entries which are not integers). To be more specific, the equation for $N_{w,0}$ in this setting is

$$pN_{w,0} = \binom{s+\beta(p-1)-\alpha}{w}^{\partial} \sum_{i>0} \binom{s+\beta(p-1)-\alpha-w}{i(p-1)-w} + \mathsf{O}(p),$$

where the second term is $\mathsf{O}(p)$ because it is still true that

$$\sum_{i>0} \binom{r-\alpha-w}{i(p-1)-w} - \sum_{i>0} \binom{s+\beta(p-1)-\alpha-w}{i(p-1)-w} = \mathsf{O}(\epsilon p).$$

On the other hand,

$$\begin{aligned} \sum_{i>0} \binom{s+\beta(p-1)-\alpha-w}{i(p-1)-w} &= \sum_{l=0}^{w} (-1)^l \binom{w}{l} \sum_{i>0} \binom{s+\beta(p-1)-\alpha-l}{i(p-1)} \\ &= (-1)^{s-\alpha}\binom{w}{s-\alpha} + \mathsf{O}(p). \end{aligned}$$

So $A_{w,0} = S_{w,0} + \mathsf{O}(\epsilon)$ is integral if $w < s - \alpha$ and

$$A_{w,0} = S_{w,0} + (-1)^{s-\alpha}\binom{w}{s-\alpha}\binom{s-\alpha-\beta}{w}^{\partial} \epsilon p^{-1} + \mathsf{O}(\epsilon)$$

if $w \geqslant s - \alpha$. Note that $\beta \in \{0, \dots, \alpha\}$ and $s > 2\alpha$ by assumption, so $S_{w,0}$ is still always integral, and if $s - \alpha \leqslant w < 2\nu - \alpha$ then

$$\binom{s-\alpha-\beta}{w}^{\partial} = \frac{(-1)^{s-\alpha-\beta-w+1}}{w\binom{w-1}{s-\alpha-\beta}} \in \mathbb{Z}_p^\times.$$

What this means is that if we proceed with the proof of theorem 17 in [Ars21] and apply lemma 18 with the constants $(C_{-1}, C_0, \dots, C_\alpha)$ constructed there such that C_0 is a unit, then we obtain an element

$$\begin{aligned}(\vartheta' + C_{-1}) \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} + C_{-1} \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} \\ + \textstyle\sum_{\xi=\alpha+1}^{2\nu-\alpha-1} E_\xi \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\xi h_\xi + F \bullet_{KZ,\overline{\mathbb{Q}}_p} h' + H\end{aligned}$$

which is in $\operatorname{im}(T-a)$ and is such that

$$\begin{aligned} v_p(C_{-1}) &= v_p(\vartheta') = t+1, \\ v_p(E_\xi) &\geqslant t+1 \text{ for } \alpha+1 \leqslant \xi < s-\alpha, \\ v_p(F) &> t+1, \end{aligned}$$

and with H as in lemma 18. However, $v_p(E_{s-\alpha}) = t$ and $v_p(E_\xi) \geqslant t$ for $\xi > s-\alpha$. Therefore if $t > v_p(a) - \alpha$ then the dominant term is H and we can conclude that a submodule of finite codimension in $T(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha))$ is trivial modulo $\mathscr{I}_a$, and if $t < v_p(a) - \alpha$ then the dominant term is

$$E_{s-\alpha} \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s-\alpha} h_{s-\alpha}$$

and hence $\widehat{N}_{s-\alpha}$ is trivial modulo $\mathscr{I}_a$ by part (2) of lemma 18.

Now let us assume that $\beta > \alpha$. We use the constants constructed in the second bullet point of the proof of theorem 17 in [Ars21], and we apply lemma 18. This gives an element

$$\begin{aligned}\vartheta' \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} \\ + \textstyle\sum_{\xi=\alpha+1}^{2\nu-\alpha-1} E_\xi \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\xi h_\xi + F \bullet_{KZ,\overline{\mathbb{Q}}_p} h' + H\end{aligned}$$

which is in $\operatorname{im}(T-a)$ and is such that

$$\begin{aligned} v_p(\vartheta') &= 1, \\ v_p(E_\xi) &\geqslant 1 \text{ for } \alpha+1 \leqslant \xi < s-\alpha, \\ v_p(F) &> 1, \\ v_p(E_{s-\alpha}) &= v_p((r-\alpha)_{s-\alpha}), \end{aligned}$$

and with H as in lemma 18. This time the dominant term is either

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

or

$$E_{s-\alpha} \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s-\alpha} h_{s-\alpha}$$

depending on whether $\beta \in \{\alpha+1, \dots, s-\alpha\}$ or $\beta > s-\alpha$. Thus in the former case $\widehat{N}_\alpha$ is trivial modulo $\mathscr{I}_a$, and in the latter case $\widehat{N}_{s-\alpha}$ is trivial modulo $\mathscr{I}_a$. ∎

Proof of proposition 23. By proposition 21 we may assume that $\beta \notin \{1, \dots, \alpha+1\}$, and by proposition 22 we may assume that $\beta \neq \alpha+1$. If $\alpha \neq \frac{s}{2}$ and $\beta \in \{1, \dots, s-\alpha\}$ and $s - \alpha < v_p(a) - t$ then the claim follows from proposition 22. Thus it is enough to show that if $\beta \in \{1, \dots, \alpha\}$ then

$$\begin{cases} T(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha)) & \text{if } \alpha > v_p(a) - t, \\ \widehat{N}_\alpha & \text{if } \alpha < v_p(a) - t \end{cases}$$

is trivial modulo $\mathscr{I}_a$. If $\alpha < v_p(a) - t$ we apply part (1) of corollary 19, and if $\alpha > v_p(a) - t)$ we apply part (5) of corollary 19. In both cases we choose $v = t$ and

$$C_j = \begin{cases} \frac{(-1)^{\alpha+\beta}(s-\alpha)(\alpha-\beta+1)}{\beta^2(2\alpha-s+1)\binom{\alpha}{\beta}}\binom{\alpha}{s-\alpha}\epsilon & \text{if } j = -1, \\ 1 & \text{if } j = 0, \\ \frac{(-1)^{j+1}(s-\alpha-\beta)}{\beta}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1} & \text{if } j \in \{1, \ldots, \alpha\}. \end{cases}$$

Since $v_p(C_{-1}) = t$ and $C_0 = 1$, the conditions we need to verify in order to be able to apply corollary 19 are

$$\begin{aligned} t &\leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } \alpha \leqslant w < 2\nu - \alpha, \\ t &< v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha, \\ \vartheta' &= -C_{-1} + \mathsf{O}(\epsilon p). \end{aligned}$$

Let us consider the matrix

$$A = (A_{w,j})_{0 \leqslant w,j \leqslant \alpha}$$

that has integer entries

$$A_{w,j} = \textstyle\sum_{0 < i(p-1) < r-2\alpha} \binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w}.$$

Then the second and third conditions are equivalent to the claim that

$$A(C_0, \ldots, C_\alpha)^T = (-C_1 + \mathsf{O}(\epsilon p), \mathsf{O}(\epsilon p), \ldots, \mathsf{O}(\epsilon p))^T.$$

As in the proof of the approximation claim in the proof of the main result of [Ars21] (and as in proposition 20) we can show that

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

where

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

The first condition follows from an argument similar to the one in the fourth bullet point in the proof of theorem 17 in [Ars21]: if we extend the number of rows in A, S, and N to $2\nu - \alpha$ by defining $A_{w,j}$, $S_{w,j}$, and $N_{w,j}$ with the same equations used for the first $\alpha + 1$ rows, then we have $A \equiv S \bmod \epsilon$ and so we can replace A with $S + \mathsf{O}(\epsilon)$, and $\vartheta_w(D_\bullet)$ for each $\alpha \leqslant w < 2\nu - \alpha$ is a $\mathbb{Z}_p$-linear combination of $\vartheta_0(D_\bullet) = \mathsf{O}(\epsilon), \ldots, \vartheta_\alpha(D_\bullet) = \mathsf{O}(\epsilon)$. And, as in the proof of theorem 17 in [Ars21], the second and third conditions follow if

$$\begin{aligned} S(C_0, \ldots, C_\alpha)^T &= 0, \\ N(C_0, \ldots, C_\alpha)^T &= \left(-C_1\epsilon^{-1}, 0, \ldots, 0\right)^T + Sv + \mathsf{O}(p) \text{ for some } v. \end{aligned}$$

Let $B = B_\alpha$ be the $(\alpha+1) \times (\alpha+1)$ matrix defined in lemma 6. Then BS has zeros outside of the rows indexed $1, \ldots, \beta - 1$, and

$$(BS)_{i,j} = \binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j}$$

for $i \in \{1, \dots, \beta - 1\}$. Let $\overline{R}$ denote the $(\alpha+1) \times (\alpha+1)$ matrix over $\mathbb{F}_p$ obtained from $\overline{BN}$ by replacing the rows indexed $1, \dots, \beta - 1$ with the corresponding rows of $\overline{BS}$. As in the proof of theorem 17 in [Ars21] we can compute

$$\begin{aligned}(\overline{BN})_{i,j} = \textstyle\sum_{l,v=0}^{\alpha} (-1)^{i+l+v} \binom{l}{i} \binom{j-v}{l-v} \binom{s-\alpha-\beta+j}{v}^{\partial} \binom{\overline{s-\alpha+j-v}}{\underline{j-v}}^{\partial} \\ - [i=0] \binom{s-\alpha-\beta+j}{j}^{\partial} - [i=\beta] \binom{s-\alpha-\beta+j}{s-\alpha}^{\partial} \\ - (-1)^i \binom{s-\alpha-\beta+j}{s-\alpha} \textstyle\sum_{l=0}^{\alpha} \binom{l}{i} \binom{l-\beta-1}{l}^{\partial}.\end{aligned}$$

Thus lemma 14 implies that

$$\overline{R}(C_0, C_1, \dots, C_\alpha)^T = \left(\frac{(-1)^{\alpha+\beta+1}(s-\alpha)(\alpha-\beta+1)}{\beta^2(2\alpha-s+1)\binom{\alpha}{\beta}} \binom{\alpha}{s-\alpha}, 0, \dots, 0 \right)^T.$$

So the conditions we need to apply corollary 19 are indeed satisfied, and that completes the proof. ∎

Proof of proposition 24. This is the first time that we consider an α such that $\alpha \geqslant s$. The major difference in this scenario is that s is not the "correct" remainder of r to work with and instead we should consider the number that is congruent to r mod $p-1$ and belongs to the set $\alpha+1, \dots, p-\alpha-1$. Let us therefore define $s_\alpha = \overline{r-\alpha} + \alpha$, and in particular let us note that $s_\alpha = s$ for $s > \alpha$ (which has hitherto always been the case). Then the computations in the proof of theorem 17 in [Ars21] work out exactly the same if we replace every instance of s with s_α (and the restricted sum "$\sum_{i>0}$" with "$\sum_{0<i(p-1)<r-\alpha}$" when $s_\alpha = p-1$). The sufficient condition for these computations to work is

$$\binom{s_\alpha - \alpha}{2\nu - \alpha} \in \mathbb{Z}_p^\times,$$

which is indeed the case since $s_\alpha - \alpha = p - 1 + s - \alpha \geqslant 2\nu - \alpha$. So there is an analogous version of theorem 17 in [Ars21], and we can conclude the desired result—as the proof of theorem 17 in [Ars21] works nearly without modification, we omit the full details of the arguments. ∎

Proof of proposition 25. Let us write $\alpha = \frac{s}{2} + 1$ and, as the claim we want to prove is vacuous for $s = 2$, let us assume that $s \geqslant 4$ and in particular $\alpha \geqslant 3$. We apply part (3) of corollary 19 with v chosen in the open interval $(v_p(a) - \alpha, t)$ and

$$C_j = \begin{cases} 0 & \text{if } j \in \{-1, 0\}, \\ (-1)^j \binom{\alpha-2}{j} + (-1)^{j+1}(\alpha-2)\binom{\alpha-2}{j-1} + pC_j^* & \text{if } j \in \{1, \dots, \alpha\}, \end{cases}$$

for some constants $C_1^*, \dots, C_\alpha^*$ yet to be chosen. The conditions necessary for the lemma to be applicable are satisfied if $\check{C} = \sum_j C_j \binom{r-\alpha+j}{j} \in \mathbb{Z}_p^\times$ and

$$\vartheta_w(D_\bullet) = \mathsf{O}(\epsilon)$$

for $0 \leqslant w < 2\nu - \alpha$. We have

$$\begin{aligned}\check{C} &= \textstyle\sum_j C_j \binom{s-\alpha-\beta+j}{s-\alpha-\beta} + \mathsf{O}(p) \\ &= -1 + \textstyle\sum_j \left((-1)^j \binom{\alpha-2}{j} + (-1)^{j+1}(\alpha-2)\binom{\alpha-2}{j-1} \right) \binom{s-\alpha-\beta+j}{s-\alpha-\beta} + \mathsf{O}(p) \\ &= -1 + \mathsf{O}(p) \in \mathbb{Z}_p^\times\end{aligned}$$

by (*c*-*e*) since $\alpha - 2 > s - \alpha - \beta$. And, since

$$j \leqslant s - \alpha - \beta + j \leqslant s - \beta < p - i,$$

we also have

$$\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} = \binom{\beta}{i}\binom{s-\alpha-\beta+j}{j-i} + \mathsf{O}(p).$$

Thus the equality $\vartheta_w(D_\bullet) = \mathsf{O}(p)$ follows from the fact that

$$\sum_j (-1)^j \binom{\alpha-2}{j-2}\binom{s-\alpha-\beta+j}{s-\alpha-\beta+i} = 0,$$

which follows from (*c*-*e*) since $\alpha - 2 > \alpha - 2 - \beta + i = s - \alpha - \beta + i$. Moreover, we can choose

$$C_1^*, \dots, C_\alpha^*$$

in a way that $\vartheta_w(D_\bullet) = 0$ for $0 \leqslant w < 2\nu - \alpha$ similarly as in the proof of theorem 17 in [Ars21] since the reduction modulo p of the matrix

$$\left(\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j}\right)_{1\leqslant i,j<\beta} = \left(\binom{\beta}{i}\binom{s-\alpha-\beta+j}{j-i} + \mathsf{O}(p)\right)_{1\leqslant i,j<\beta}$$

is upper triangular with units on the diagonal. Thus the conditions we need to apply corollary 19 are satisfied and we can conclude that $\widehat{N}_{s/2+1}$ is trivial modulo $\mathscr{I}_a$. ∎

Proof of proposition 26. Let us write $\alpha = \frac{s}{2} - 1$ and, as the claim we want to prove is vacuous for $s = 2$, let us assume that $s \geqslant 4$ and in particular $\alpha \geqslant 3$. The only obstruction in the proof of proposition 22 that prevents us from concluding that $\widehat{N}_{s/2-1}$ is trivial modulo $\mathscr{I}_a$ is that the dominant terms are

$$E_\xi \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\xi h_\xi$$

for $\frac{s}{2} < \xi \leqslant 2\nu - \frac{s}{2}$ rather than H. We can see from proposition 25 that

$$E_{s/2+1} \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s/2+1} h_{s/2+1} = x_1 + x_2,$$

with $v_p(x_1) \geqslant t+1$, and with $x_2 \in \operatorname{im}(T-a)$. Since the valuation of the coefficient of H is less than $t+1$, we can remove the obstruction coming from

$$E_{s/2+1} \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s/2+1} h_{s/2+1}$$

by replacing it with x_1. If $s = 2\nu - 2$ then this is the only obstruction and we can conclude that $\widehat{N}_{s/2-1}$ is trivial modulo $\mathscr{I}_a$. Now suppose that $s < 2\nu - 2$. Then just as in the proof of theorem 17 in [Ars21] we can apply part (1) of corollary 19 and conclude that $\widehat{N}_\alpha$ is trivial modulo $\mathscr{I}_a$ as long as $(\epsilon, 0, \dots, 0)^T$ is in the image of the matrix $A = (A_{w,j})_{0\leqslant w,j\leqslant\alpha}$ that has integer entries

$$A_{w,j} = \sum_{i>0} \binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = S_{w,j} + \epsilon N_{w,j} + \mathsf{O}(\epsilon p)$$

with S and N as in proposition 20. However, this time we can deduce more than that: since $s < 2\nu - 2$ it follows that

$$1 \bullet_{KZ,\overline{\mathbb{Q}}_p} x^{s/2+1} y^{r-s/2-1}$$

is equal to

$$g_1 \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s/2+1} x^{s/2-n+1} y^{r-np-s/2-1} + x_3$$

for some g_1 with $v_p(g_1) \geqslant v_p(a) - \frac{s}{2} - 1$ and some $x_3 \in \operatorname{im}(T-a)$. This in turn by proposition 25 is equal to

$$g_2 \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s/2+1} h_2 + x_4$$

for some g_2 with $v_p(g_2) \geqslant t$, some h_2, and some $x_4 \in \operatorname{im}(T-a)$. Here we use the fact that the valuation of the constant C_1 from proposition 25 is at least one and therefore the corresponding term H is

$$g_2 \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s/2+1} x^{s/2-n+1} y^{r-np-s/2-1} + x_5 + \mathsf{O}(\epsilon)$$

for some g_3 with $v_p(g_3) = v_p(a) - \frac{s}{2} - 1$ and some $x_5 \in \operatorname{im}(T-a)$. In general the error term would be

$$C_1 a p^{-s/2} g_4 \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{s/2} x^{s/2-n} y^{r-np-s/2} + \mathsf{O}(\epsilon)$$

rather than $\mathsf{O}(\epsilon)$—a description of this error term is given in part (2) of lemma 15. This implies that we can add a constant multiple of

$$1 \bullet_{KZ,\overline{\mathbb{Q}}_p} x^{s/2+1} y^{r-s/2-1}$$

to the element

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

from the proof of lemma 17, and we can translate this back to adding the extra column

$$\left(\tbinom{r-\alpha}{s-\alpha}, \ldots, \tbinom{r}{s}\right)^T$$

to A. As in proposition 20 we can then reduce showing that $(\epsilon, 0, \ldots, 0)^T$ is in the image of A to showing that

$$(1, 0, \ldots, 0)^T$$

is in the image of the $(\alpha+1) \times (\alpha+2)$ matrix $\overline{R}$ which is obtained from the matrix $\overline{Q}$ defined in the proof of theorem 17 in [Ars21] by replacing all entries in the first row with zeros (because this time we do not divide the corresponding row of A by p) and by adding an extra column corresponding to the extra column of A. Thus, if we index the extra column to be the zeroth column, the lower right $\alpha \times \alpha$ submatrix of $\overline{R}$ is upper triangular with units on the diagonal, the first column of $\overline{R}$ is identically zero, and all entries of the first row of $\overline{R}$ except for $\overline{R}_{0,0}$ are zero. As when computing $(\overline{BN})_{i,j}$ in proposition 23 we can find that

$$\overline{R}_{0,0} = \textstyle\sum_{l=0}^{\alpha} \binom{l-\beta-1}{l}^{\partial} = \Phi'(-\beta-1)$$

with

$$\Phi(z) = \textstyle\sum_{l=0}^{\alpha} \binom{z+l}{l} = \binom{z+\alpha+1}{\alpha}.$$

Thus

$$\overline{R}_{0,0} = \binom{\alpha-\beta}{\alpha}^{\partial} = \frac{(-1)^{\beta+1}}{\beta\binom{\alpha}{\beta}} \neq 0,$$

which implies that $(1, 0, \ldots, 0)^T$ is in the image of $\overline{R}$. Thus the conditions we need to apply corollary 19 are satisfied and we can conclude that $\widehat{N}_{s/2-1}$ is trivial modulo $\mathscr{I}_a$. ∎

Proof of proposition 27. Let us write $\alpha = \frac{s}{2} + 1$. The reason why the proof of proposition 25 does not work for $\beta \in \{\alpha-1, \alpha\}$ is because $\check{C} = \mathsf{O}(p)$ for the constructed constants C_j. However, since $t > v_p(a) - \frac{s}{2}$, if $\check{C} \in p\mathbb{Z}_p^\times$ then the dominant term coming from lemma 18 is

$$H = b_H \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} + \mathsf{O}\big(p^{\nu-\alpha+1}\big)$$

for the constant

$$b_H = \frac{ap^{-\alpha}}{1-p} \check{C}$$

which has valuation $v_p(a)-\alpha+1$. As in proposition 26 it is crucial here that $C_1=\mathsf{O}(p)$. Just as in the proof of proposition 25 we can reduce the claim we want to show to proving that there exist constants $C_1,\dots,C_\alpha\in\mathbb{Z}_p$ such that $C_1=\mathsf{O}(p)$ and

$$\left(\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j}\right)_{0\leqslant i<\beta,0<j\leqslant\alpha}(C_1,\dots,C_\alpha)^T=(p,0,\dots,0)^T.$$

Therefore it is enough to show that the square matrix

$$A_0=\left(p^{[j=1]-[i\leqslant\beta-\alpha+1]}\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j}\right)_{0\leqslant i<\beta,\,\alpha-\beta<j\leqslant\alpha}$$

has integer entries and is invertible (over $\mathbb{Z}_p$), as then we can recover

$$\begin{cases} C_1=0 \text{ and } (C_2,\dots,C_\alpha)^T=A_0^{-1}(1,0,\dots,0)^T & \text{if } \beta=\alpha-1,\\ (C_1/p,\dots,C_\alpha)^T=A_0^{-1}(1,0,\dots,0)^T & \text{if } \beta=\alpha.\end{cases}$$

This follows from lemma 13. So the conditions we need to apply corollary 19 are satisfied and we can conclude that $\widehat{N}_{s/2+1}$ is trivial modulo $\mathscr{I}_a$. ∎

Proof of proposition 28. Let us write $\alpha=\frac{s}{2}+1$. This time the proofs of both parts (25) and (27) break down since $\check{C}=\mathsf{O}(p)$ and the dominant term is no longer H. Let us slightly tweak these constants and instead use

$$C_j=\begin{cases}(-1)^\alpha\epsilon & \text{if } j=-1,\\ (-1)^{\alpha+j+1}\alpha\binom{\alpha-2}{j-2} & \text{if } j\in\{0,\dots,\alpha\}.\end{cases}$$

Let $\overline{R}$ be the matrix constructed in proposition 23. Then just as in the proof of proposition 25 we can show that $\check{C}=\mathsf{O}(p)$, and just as in the proof of proposition 20 we can show that the dominant term coming from equation (3) in lemma 18 is

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

(and therefore that $\mathrm{ind}_{KZ}^G\,\mathrm{sub}(\frac{s}{2}+1)$ is trivial modulo $\mathscr{I}_a$) as long as

$$\overline{R}(C_0,\dots,C_\alpha)^T=(0,\dots,0,1)^T.$$

This follows from lemma 12. Thus the conditions we need to apply corollary 19 are satisfied and we can conclude that $\mathrm{ind}_{KZ}^G\,\mathrm{sub}(\frac{s}{2}+1)$ is trivial modulo $\mathscr{I}_a$. ∎

References

[Ars21] Bodan Arsovski, *On the reductions of certain two-dimensional crystalline representations*, Documenta Mathematica **26** (2021), 1929–1979.

[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.

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

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

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

[Bre03b] ———, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbb{Q}_p)$*, II*, Journal of the Institute of Mathematics of Jussieu **2** (2003), no. 1, 23–58.

[BG09] Kevin Buzzard and Toby Gee, *Explicit reduction modulo p of certain two-dimensional crystalline representations*, International Mathematics Research Notices **12** (2009), 2303–2317.

[BG13] ———, *Explicit reduction modulo p of certain two-dimensional crystalline representations, II*, Bulletin of the London Mathematical Society **45** (2013), no. 4, 779–788.

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

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