ON THE REDUCTIONS OF CERTAIN
TWO-DIMENSIONAL CRYSSTALLINE
REPRESENTATIONS, III

BODAN ARSOVSKI

Abstract. A conjecture of Breuil, Buzzard, and Emerton says that the slopes of certain reducible \( p \)-adic Galois representations must be integers. In [Ars] we showed this conjecture for representations that lie over certain “non-subtle” components of weight space. This article is a continuation of [Ars] in which we also show the conjecture for 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 \( k \geq 2 \) be an integer, and let \( a \) be an element of \( \mathbb{Z}_p \) 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 [Ars], and we define \( V_{k,a} \) as the semi-simplification of the reduction modulo the maximal ideal \( m \) of \( \mathbb{Z}_p \) of a Galois stable \( \mathbb{Z}_p \)-lattice in \( V_{k,a} \) (with the resulting representation being independent of the choice of lattice). The question of computing \( V_{k,a} \) has been studied extensively, and we refer to the introduction of [Ars] 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 \( V_{k,a} \) is irreducible.

The main result of [Ars] 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

\[
 k \neq 3, 4, \ldots, 2\nu, 2\nu + 1 \mod p - 1.
\]

Thus there are \( \max\{\frac{p-1}{2} - \nu + 1, 0\} \) many “non-subtle” components of weight space. This article is a continuation of [Ars] 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 \( \frac{p-1}{2} \).

Date: February 2021.
2. Computing \( \nabla_{k,a} \) by computing \( \mathcal{O}_{k,a} \)

From now on we assume the notation from sections 2, 3, 4, and 6 of \( \text{[Ars]} \). Moreover, we assume that \( k > p^{100} \) as in section 5 of \( \text{[Ars]} \). Theorem 2 in \( \text{[Ars]} \) 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 \( v_{p}(a) \in (0, \frac{p-1}{2}) \setminus \mathbb{Z} \) then \( \mathcal{O}_{k,a} \) is irreducible.

Thus our task is to prove theorem 2.

3. Combinatorics

Throughout the proof we will refer to the combinatorial results in section 8 of \( \text{[Ars]} \). For convenience, we reproduce the statements here in the form we will use.

**Lemma 3.** Suppose throughout this lemma that
\[
n, t, y \in \mathbb{Z}, \quad b, d, k, l, w \in \mathbb{Z}_{\geq 0}, \quad m, u, v \in \mathbb{Z}_{\geq 1}.
\]

(1) If \( u \equiv v \mod (p-1)p^{m-1} \) then
\[
M_{u,n} \equiv M_{v,n} \mod p^{m}.
\]

(2) Suppose that \( u = t_{u}(p-1) + s_{u} \) with \( s_{u} = \mathcal{O}_{u} \), so that \( s_{u} \in \{1, \ldots, p-1\} \) and \( u_{n} \in \mathbb{Z}_{\geq 0} \). Then
\[
M_{u} = 1 + [u \equiv_{p-1} 0] + \frac{m}{m} p + O(t_{u}p^{2}).
\]

(3) If \( n \leq 0 \) then
\[
M_{u,n} = \sum_{i=0}^{-n} (-1)^{i}\binom{-n}{i}M_{u-n,i,0}.
\]

(4) If \( n \geq 0 \) then
\[
M_{u,n} \equiv (1 + [u \equiv_{p-1} n \equiv_{p-1} 0])p \mod p.
\]

(5) If \( u \geq (b + l)d \) and \( l \geq w \) then
\[
\sum_{j} (-1)^{j-b} \binom{l}{j-b} \binom{w-d}{j} = [w = l]d^{t}.
\]

(6) If \( X \) is a formal variable then
\[
\binom{X}{w} = \sum_{v} (-1)^{w-v}\binom{1}{w} \binom{l}{w} \binom{X-v}{l-v}.
\]

Consequently, if \( b + l \geq d + w \) then
\[
\sum_{i} \binom{b-d+i}{i}\binom{a(p-1)+l}{w} = \sum_{a} (-1)^{w-v}\binom{1}{w} \binom{l-w-1}{w-v}\binom{b-d+i}{w}M_{b-d-l-v, l-v}.
\]

(7) We have
\[
\sum_{j} (-1)^{j}\binom{w+l-j}{w-j} = (-1)^{w}\binom{w-l-1}{w}.
\]

(8) We have
\[
\sum_{j} \binom{u-1}{j-w} \binom{-l}{j-w} = (-1)^{u-w}\binom{l-w}{u-w}.
\]

(9) We have
\[
\sum_{j} (-1)^{j}\binom{b}{j-w} \binom{l}{j-w} = (-1)^{l+w}\binom{l+w-b}{l+w}.\]
Lemma 4. Let \( \alpha \in \mathbb{Z} \cap [0, \ldots, \frac{p^r}{p-1}] \) and let \( \{D_i\}_{i \in \mathbb{Z}} \) be a family of elements of \( \mathbb{Z}_p \) such that \( D_i = 0 \) for \( i \not\in [0, \frac{p^r}{p-1}] \) and \( \vartheta_w(D_\bullet) = 0 \) for all \( 0 \leq w < \alpha \). Then
\[
\sum_i D_i x^{i(p-1)+\alpha} y^{-i(p-1)-\alpha} = \theta^\alpha h
\]
for some polynomial \( h \) with integer coefficients.

Lemma 5. For \( \alpha, \lambda, \mu \in \mathbb{Z}_{\geq 0} \) let
\[
L_{\alpha}(\lambda, \mu)
\]
be the \((\alpha + 1) \times (\alpha + 1)\) matrix with entries
\[
L_{i,j} = \sum_{k=0}^{\alpha} \frac{d}{d^k} \left( \frac{X}{\alpha} \right)^k \ s_1(l, k)s_2(k, j),
\]
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
\[
L_{\alpha}(\lambda, \mu) \left( \begin{array}{c} \lambda X \\ \alpha \end{array} \right) = \left( \begin{array}{c} \mu X \\ \alpha \end{array} \right).
\]

Lemma 6. For \( \alpha \in \mathbb{Z}_{\geq 0} \) let \( B_\alpha \) be the \((\alpha + 1) \times (\alpha + 1)\) matrix with entries
\[
B_{i,j} = j! \sum_{k,l=0}^{\alpha} \frac{(-1)^{i+k}}{k!} \binom{l}{1} (1-p)^{-k} s_1(l, k)s_2(k, j),
\]
where \( s_1(i, j) \) and \( s_2(k, j) \) are the Stirling numbers of the first and second kind, respectively. Let \( \{X_{i,j}\}_{i,j \geq 0} \) be formal variables. For \( \beta \in \mathbb{Z}_{\geq 0} \) such that \( \alpha \geq \beta \) let
\[
S(\alpha, \beta) = (S(\alpha, \beta)_{w,j})_{0 \leq w, j \leq \alpha}
\]
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 \( 1, \ldots, \beta \) and
\[
(B_\alpha S(\alpha, \beta))_{i,j} = X_{i,j}
\]
for \( i \in \{1, \ldots, \beta\} \).

Lemma 7. For \( u, v, c \in \mathbb{Z} \) let us define
\[
F_{u,v,c}(X) = \sum_w (-1)^w c \binom{X}{w} (X^{v-c})^\partial (X^{v-c}) \in \mathbb{Q}_p[X].
\]
Then
\[
F_{u,v,c}(X) = \binom{X}{c} (X^v)^\partial - \binom{X}{u} (X^c)^\partial.
\]

Lemma 8. Let \( X \) and \( Y \) denote formal variables, and let
\[
c_j = (-1)^j \alpha! \binom{X+j+1}{j+1} \binom{Y+j+1}{j+1} \binom{Y+j-1}{j+1} \in \mathbb{Q}[X, Y] \subset \mathbb{Q}(X, Y)
\]
be polynomials over \( \mathbb{Q} \) of degrees \( \alpha - j \), for \( 1 \leq j \leq \alpha \). Let
\[
M = (M_{w,j})_{0 \leq w, j \leq \alpha}
\]
be the \((\alpha + 1) \times (\alpha + 1)\) matrix over \( \mathbb{Q}(X, Y) \) with entries
\[
M_{w,0} = (-1)^w \frac{Y-X}{Y^{w+1}} X_w,
\]
\[
M_{w,j} = \sum_v (-1)^{w-v} \binom{X+j}{w-v-1} \binom{Y+j}{j-v} \binom{Y+j-1}{j-v} \binom{Y+j-1}{j-v} - \binom{X+j}{j-v} \binom{Y+j-1}{j-v},
\]
for \( 0 \leq w \leq \alpha \) and \( 0 < j \leq \alpha \). Then the first \( \alpha - 1 \) entries of
\[
M_c = (M_{\alpha, c_1}, \ldots, c_\alpha)^T = (d_0, \ldots, d_\alpha)^T
\]
are zero, and \( d_\alpha = \frac{(Y-X)_{\alpha+1}}{Y_{\alpha+1}} \).
Lemma 9. Suppose that $s, \alpha, \beta \in \mathbb{Z}$ are such that

$$1 \leq \beta \leq \alpha \leq \frac{s}{2} - 2 \leq \frac{p-5}{2}.$$  

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

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

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

$$p^{-|i|} \sum_{\nu=0}^{\alpha} B_{i,\nu} \sum_{v} (-1)^{w-v} (j+w-v-1) (s+\beta(p-1)-\alpha+j)^{\nu} \cdot \sum_{\nu=0}^{\beta} (s+\beta(p-1)-\alpha+j-v)^{\nu}.$$

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 $s, \alpha \in \mathbb{Z}_{\geq 0}$ are such that

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

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

$$\sum_{\nu} (-1)^{w-v} (j+w-v-1) (z^{2+\nu}) (s-\alpha+2+\nu) (z^{2+\nu}) - (z^{-\alpha+1}) (z^{\nu}) - (z^{-\alpha+1}) (z^{s-2}).$$

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

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

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

$$F_1(z) = \sum_{j=0}^{\alpha} C_j(z) F_{w,j}(z),$$

$$F_2(z) = -[w = 0] (\frac{s-1}{\alpha+1}).$$

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

Proof. Let us first show that

$$(1) \quad C_0(z) \binom{\frac{s-\alpha}{\alpha}}{s-\alpha} + \sum_{j=1}^{\alpha} C_j(z) \binom{\frac{s-\alpha+j}{s-\alpha}}{s-\alpha} = \frac{(-1)^{s+1}(z-\alpha)}{s-\alpha}.$$  

Since

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

this is equivalent to

$$\binom{\frac{\alpha}{s-\alpha-1}}{s-\alpha} - \frac{z^{-\alpha-1}}{s-\alpha-1} + \sum_{j=1}^{\alpha} \frac{(-1)^{\nu+1}(\alpha-1)}{\nu+1} \binom{\frac{s-\alpha}{\alpha-j}}{s-\alpha}(z^{-\alpha+j}) = (-1)^{s+1}.$$
The polynomial on the left side has degree at most \(s - \alpha\). The coefficient of \(z^{s-\alpha}\) in it is \(\frac{2s-1}{(s-\alpha)!}\) plus
\[
\sum_j \frac{(s-\alpha-1)}{j+1} \frac{(-1)^{j+1}}{(\alpha-j)} (s-\alpha-1)^{(\alpha-j)} \in \mathbb{Z}.
\]

The third equality follows from the fact that \(\gamma\) is even. Therefore it is enough to show that the two polynomials are equal when evaluated at \(z \in \{\alpha + 1, \ldots, s\}\). At these points the polynomial on the left side is equal to
\[
(s-\alpha) \sum_j \frac{(-1)^{j+1}}{j+1} \frac{(s-\alpha-1)}{\alpha-j} (s-\gamma)^{(\alpha-j)}
\]
for \(\gamma \in \{0, \ldots, s - \alpha - 1\}\). We have
\[
\sum_j \frac{(-1)^{j+1}}{j+1} \frac{(s-\alpha-1)}{\alpha-j} (s-\gamma)^{(\alpha-j)} = \sum_j \frac{(-1)^{j-\alpha+j+1}}{j+1} \frac{(s-\alpha-1)}{\alpha-j} (s-\gamma)^{(\alpha-j)}
\]
\[
= \sum_u \binom{s}{u} \sum_j \frac{(-1)^{j-\alpha+j+1}}{j+1} \frac{(s-\alpha-1)}{\alpha-j} (s-\gamma)^{(\alpha-j)}
\]
\[
= \sum_u \binom{s}{u} \sum_j \frac{(-1)^{j-\alpha+j+1}}{s-\alpha-u} (s-\gamma)^{(\alpha-j)}
\]
\[
= \sum_u \binom{s}{s-\alpha-u} \binom{s-\alpha-1}{\alpha-j} \sum_j (s-\alpha-1)^{(\alpha-j)}
\]
\[
= \sum_u \binom{s}{s-\alpha-u} \binom{s-\alpha-1}{\alpha-j} = \frac{(-1)^{s-\alpha}}{(\alpha+1)!}.
\]

The third equality follows from \(\binom{s}{u} = 0\) for \(u > s - \alpha - 1\), and the last equality follows from \(\binom{s-\alpha-1}{\alpha+1} = 0\) for \(u \in \{1, \ldots, s - \alpha - 1\}\). 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
\[
z \in \{s + \gamma(p-1) | \gamma \in \{0, \ldots, \alpha + 1\}\}.
\]

It is easy to verify that \(F_1(s) = F_2(s)\), and when
\[
z \in \{s + \gamma(p-1) | \gamma \in \{1, \ldots, \alpha + 1\}\}
\]
the fact that
\[
\sum_{j=0}^{\gamma-1} \binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j} F_{w,j} = \binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j}
\]
(due to (c-g)) implies that the equation \(F_1(s + \gamma(p-1)) = F_2(s + \gamma(p-1))\) is equivalent to
\[
\sum_{j=0}^{\gamma-1} C_j(s + \gamma(p-1)) \sum_{i=1}^{\gamma-1} \binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j} (s-\gamma)^{(\gamma-j-1)} = [w = 0] (-\gamma(p-1)-1).
\]

Note that \((-\gamma(p-1)-1) = (-\gamma-1) = 0\) and therefore the right side vanishes. Let us reiterate that all computations done in this proof are over \(\mathbb{F}_p\). Let us write \(C_j = C_j(s + \gamma(p-1))\). The desired identity
\[
\sum_{j=0}^{\gamma-1} C_j(s + \gamma(p-1)) \sum_{i=1}^{\gamma-1} \binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j} (s-\gamma)^{(\gamma-j-1)} = 0
\]
follows if
\[
\sum_{j=0}^{\gamma-1} C_j \sum_{i=1}^{\gamma-1} \binom{s+\gamma(p-1)-\alpha+j}{i(p-1)+j} (s-\gamma)^{(\gamma-j-1)} = 0
\]
for all \(i \in \{1, \ldots, \gamma - 1\}\). If \(j > 0\) and \(C_j \neq 0\) then
\[
j \geq 2\alpha - s + 1 \geq \alpha + \gamma - s
\]
and consequently
\[
(s^{+\gamma(p-1)-\alpha+j})_{i(p-1)+j} = \begin{cases} 
(s^{-\alpha-\gamma+j}) & \text{if } s-\alpha-\gamma+i \geq 0 \\
(s^{-\alpha-\gamma+j})_{j-1} & \text{if } s-\alpha-\gamma+i < 0 
\end{cases}
\]
\[
= (\gamma)_{i(p-1)-1}^{\alpha-\gamma+j}.
\]
On the other hand,
\[
(s^{+\gamma(p-1)-\alpha})_{i(p-1)-1}^{\alpha-\gamma} = (\gamma)_{i(p-1)-1}^{\alpha-\gamma+j}.
\]
Since
\[
(\gamma^{-1})_{i(p-1)-1}^{\alpha-\gamma+j} \in \mathbb{F}_p^{	imes}
\]
(as that \(0 < i < \gamma \leq \alpha + 1\)), what we want to show is that
\[
C_0^{\gamma} = \frac{1}{\gamma} \sum_{j=1}^{\alpha} (s^{-\alpha-\gamma+j}) \left( s^{-\alpha-1}(\gamma^{-1}j+1) \right)
\]
for all \(i \in \{1, \ldots, \gamma - 1\}\). That is equivalent to
\[
F_3(s + \gamma(p-1)) = 0,
\]
where \(F_3(z) \in \mathbb{F}_p[z]\) is defined as
\[
F_3(z) = (s^{-\alpha-1})_{s-\alpha-1}^{\alpha+1}(s^{-\alpha-1}w) + \sum_{j=1}^{\alpha} \frac{(-1)^{i+j}i(\gamma^{-1}j+1)}{(\alpha-j)!} (s^{-\alpha-1})_{s-\alpha-1}^{\alpha+1}(s^{-\alpha-1}w)
\]
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 \(-\sum_{j=1}^{\alpha} \frac{(-1)^{i+j}i(\gamma^{-1}j+1)}{(\alpha-j)!} (s^{-\alpha-1})_{s-\alpha-1}^{\alpha+1}(s^{-\alpha-1}w)\) plus
\[
\frac{1}{(s-\alpha-w-1)!} \sum_{j=1}^{\alpha} \frac{(-1)^{i+j}i(\gamma^{-1}j+1)}{(\alpha-j)!} (s^{-\alpha-1})_{s-\alpha-1}^{\alpha+1}(s^{-\alpha-1}w),
\]
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
\[
z \in \{\alpha + 1, \ldots, s - w\}.
\]
At these points \(F_3(z)\) is equal to
\[
(s - \alpha - w) \sum_{j} \frac{(-1)^{i+j}}{(\alpha-j)!}(s^{-\alpha-1})(s^{-\alpha-\gamma+j})
\]
for \(\gamma \in \{w, \ldots, s - \alpha - 1\}\). We have
\[
\sum_{j} \frac{(-1)^{i+j}(s^{-\alpha-1})(s^{-\alpha-\gamma+j})}{(\alpha-j)!}(s^{-\alpha-1})_{s-\alpha-1}^{\alpha+1}(s^{-\alpha-1}w) = \sum_{j} \frac{(-1)^{i+j}(s^{-\alpha+j-w+1})(s^{-\alpha-1})_{s-\alpha-1}^{\alpha+1}(s^{-\alpha-1}w)}{(\alpha-j)!}(\gamma^{-1}j+1)
\]
\[
= \sum_{u} (\gamma^{-1}u) \sum_{j} \frac{(-1)^{i+j+w-1}(s^{-\alpha-1})(s^{-\alpha-j-1})}{(\alpha-j)!}(s^{-\alpha-1}w)
\]
\[
= \sum_{u} (\gamma^{-1}u) \sum_{j} \frac{(-1)^{i+j+w-1}(s^{-\alpha-1})(s^{-\alpha-j-1})}{(\alpha-j)!}(s^{-\alpha-1}w)
\]
\[
= \sum_{u} \frac{(-1)^{u+w}}{(\gamma^{-1}u)} \sum_{j} \frac{(s^{-\alpha-1})(s^{-\alpha-j-1})}{(\alpha-j)!}(s^{-\alpha-1}w)
\]
\[
= 0.
\]
The last equality follows from \(\sum_{u} (\gamma^{-1}u) = 0\) for
\[
u \not\in \{0, \ldots, s - \alpha - w - 1\}.
\]
This proves that indeed \(F_3(z) = 0\) and therefore that \(F_3(z) = F_2(z)\).

Lemma 11. Suppose that \(\alpha \in \mathbb{Z}_{\geq 0}\). For \(w, j \in \{0, \ldots, \alpha\}\) let
\[
F_{w,j}(z, \psi) \in \mathbb{F}_p[z, \psi]
\]
declare the polynomial
\[
\sum_{v} (-1)^{v}((w-v-1)(\psi-v) + (w-v-1)(\psi-v)) = (z^{-\alpha+j-v})
\].
Note that this depends on $\alpha$. Then
\[
\sum_{j=1}^{\alpha} (-1)^{\alpha-j} \binom{\alpha-j}{\gamma} F_{w,j}(z,\psi) = (-1)^{\alpha} ([w = \alpha] - [w = 0]) \binom{\alpha-j}{\gamma}.
\]

Proof. Both sides of the equation we want to prove have degree $\alpha$ and the coefficient of $z^\alpha$ 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 $(z, \psi)$ such that
\[
(z, \psi) \in \{(u + \gamma(p-1) + \alpha, u + \alpha) \mid u \in \{0, \ldots, \alpha\}, \gamma \in \{0, \ldots, \alpha-1\}\}.
\]
The right side is zero when evaluated at these points, and
\[
F_{w,j}(u + \gamma(p-1) + \alpha, u + \alpha) = \sum_{i=1}^{\gamma} \binom{u+\gamma(p-1)+j}{i} \binom{i(p-1)}{w}
\]
by (7.30). Thus we want to show that
\[
\sum_{j=1}^{\alpha} (-1)^{\alpha-j} \binom{\alpha-j}{\gamma} \sum_{i=1}^{\gamma} \binom{u+\gamma(p-1)+j}{i} \binom{i(p-1)}{w} = O(p)
\]
for $0 \leq u, w \leq \alpha$ and $0 \leq \gamma < \alpha$. Since
\[
\binom{u+\gamma(p-1)+j}{i} \binom{i(p-1)}{w} = \binom{\gamma}{i} \binom{u+j-\gamma}{i} \binom{-1}{w} + O(p),
\]
that is equivalent to
\[
\sum_{i,j>0} (-1)^{\alpha+w-i} \binom{u+1}{i} \binom{\gamma-u-i-1}{j} \binom{i+w-1}{w} = O(p).
\]
This follows from the facts that
\[
\sum_{j>0} \binom{u+1}{i} \binom{\gamma-u-i-1}{j} = \binom{\gamma-i}{\alpha-i}
\]
for $i > 0$ by Vandermonde’s convolution formula, and
\[
\binom{\gamma}{i} \binom{\gamma-i}{\alpha-i} = \binom{\gamma}{\alpha} \binom{\gamma-i}{\alpha-i} = 0
\]
since $\gamma \in \{0, \ldots, \alpha-1\}$.

\[\square\]

Lemma 12. Suppose that $s, \alpha, \beta \in \mathbb{Z}$ are such that
\[
s \in \{2, 4, \ldots, p-3\} \quad \text{and} \quad \alpha = \beta = \frac{s}{2} + 1.
\]
Let $M$ denote the $(\alpha+1) \times (\alpha+1)$ matrix with entries in $\mathbb{F}_p$ defined in lemma [14]. Suppose that $C_0, \ldots, C_\alpha \in \mathbb{F}_p$ are defined as
\[
C_j = (-1)^{\alpha+j+1} \alpha \binom{\alpha-2}{j-2}.
\]
Then
\[
M(C_0, \ldots, C_\alpha)^T = (0, \ldots, 0, 1)^T.
\]

Proof. The equation associated with the $i$th row of $M$ is straightforward if $i \not\in \{0, \alpha\}$. Since $M_{0,j}$ is equal to
\[
\sum_{j=0}^{\alpha} \binom{\alpha}{j} (-1)^{\alpha+j+1} \binom{\alpha-2}{j-2} \binom{\alpha-j-2}{\alpha-2} \binom{1 + [\alpha = 2 \& j = v]}{j-v} = \binom{\alpha-j-2}{\alpha-2} \binom{\alpha-2}{\alpha}.
\]
and since
\[ \sum_j (-1)^j \binom{\alpha-2}{j-2} \frac{1}{i(j-1)} = \frac{1}{\alpha}, \]
\[ \sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{j-2}{\alpha}^{\theta} = (-1)^{\alpha} \binom{0}{\alpha}^{\theta} = -\frac{1}{\alpha}, \]
\[ \sum_i (-1)^i \binom{\alpha-2}{\alpha-i} \binom{\alpha-i}{\alpha-2} \binom{\alpha}{\alpha-i}^{\theta} = -\frac{1}{\alpha}, \]
\[ \sum_i (-1)^i \binom{\alpha-2}{\alpha-i} \binom{\alpha-i}{\alpha-2} \binom{\alpha}{\alpha-i}^{\theta} = -\frac{1}{\alpha}, \]
the equation associated with the zeroth row is
\[ \sum_j (-1)^j \binom{\alpha-2}{j-2} \sum_{i,v=0}^{\alpha} (-1)^{i+j} \binom{i}{\alpha} \binom{j-v}{\alpha} = -\frac{1}{\alpha}, \]
and it follows from the fact that
\[ \sum_{i=0}^{\alpha} (-1)^i \binom{i}{\alpha} = (-1)^j \binom{v}{\alpha} \]
for \(0 \leq v \leq j \leq \alpha\). This shows the equation associated with the zeroth row. Since \(M_{\alpha,j}\) is equal to
\[ |j = 2| \binom{0}{\alpha}^{\theta} + |j = \alpha| F_{\alpha,\alpha,0} (\alpha - 2) - (\binom{j-2}{\alpha}^{\theta} - (-1)^{\alpha} \binom{j-2}{\alpha}^{\theta} \binom{1}{\alpha}^{\theta}), \]
the equation associated with the \(\alpha\)th row is
\[ \binom{0}{\alpha}^{\theta} - \sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{j-2}{\alpha}^{\theta} = (-1)^{\alpha} \binom{1}{\alpha}^{\theta} - (-1)^{\alpha} F_{\alpha,\alpha,0} (\alpha - 2) + \frac{(-1)^{\alpha+1}}{\alpha}, \]
and it follows from the facts that
\[ F_{\alpha,\alpha,0} (\alpha - 2) = F_{\alpha,\alpha,0} (\alpha - 1) = (-1)^{\alpha} \binom{1}{\alpha}^{\theta} \]
and that the polynomial \((X_{\alpha-2})^{\theta} \in \mathbb{F}_p[X]\) has degree less than \(\alpha - 2\) (and is zero if \(\alpha = 2\) and therefore
\[ \sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{j-2}{\alpha}^{\theta} = 0. \]
This shows the equation associated with the \(\alpha\)th row and concludes the proof. ■

**Lemma 13.** Suppose that \(s, \alpha, \beta \in \mathbb{Z}\) are such that
\(s \in \{2, 4, \ldots, p-3\}\) and \(\alpha = \frac{s}{2} + 1\) and \(\beta \in \{\frac{s}{2}, \frac{s}{2} + 1\}\).
Let \(A_0\) denote the \(\beta \times \beta\) matrix with entries in \(\mathbb{Q}_p\) defined as
\[ A_0 = \left( \binom{p}{j-1} \sum_{i=0}^{\beta} \left( \binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} \right) \right)_{0 \leq i < \beta, \alpha - \beta < j < \alpha}. \]
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
\[ s - \alpha - \beta + j \geq 0 \]
and therefore
\[ \binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} = \binom{\beta}{i}(s+\alpha-\beta+j) + O(p) = O(p) \]
for \(i \leq \beta - \alpha + 1\). 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 \(c_2, \ldots, c_\alpha\). The bottom left \((\alpha-3) \times (\alpha-3)\) submatrix of \(\overline{A}_0\) is upper triangular with units on the diagonal. Moreover, since
\[ \sum_j (-1)^j \binom{s+\beta-1}{\alpha-i-j-1} \binom{\alpha-2}{j} = \sum_j (-1)^j \binom{\beta-1}{i-1} \binom{\beta-1}{j} = 0, \]
\[ \sum_j (-1)^j \binom{j-1}{\alpha-i-j-1} \binom{\alpha-1}{j} = \sum_j (-1)^j \binom{\beta-1}{i-1} \binom{\beta-1}{j} = 0, \]
all but the top two entries of each of the vectors
\[ c_{\alpha-1} - \binom{\alpha-2}{1} c_{\alpha-2} + \cdots + (-1)^{\alpha-3} \binom{\alpha-2}{3} c_2, \]
\[ c_{\alpha} - \binom{\alpha-1}{2} c_{\alpha-2} + \cdots + (-1)^{\alpha-3} \binom{\alpha-1}{3} c_2 \]
are zero. Thus it is easy to show that the \(2 \times 2\) matrix consisting of those four entries is invertible (over \(\mathbb{F}_p\)). This \(2 \times 2\) matrix is
\[
\begin{pmatrix}
  e_{0,0} & e_{0,1} \\
  (-1)^{\beta} e_{0,0} & (-1)^{\beta} e_{0,1}
\end{pmatrix}
\]
with
\[
e_{0,0} = \beta \sum_{j=0}^{\beta-1} (-1)^j \binom{\beta-1}{j} \binom{\beta-j-1}{\beta-j} = \sum_{j=0}^{\beta-1} \frac{(-1)^j \beta}{\beta-j} \left( \binom{\beta-1}{j} \right),
\]
\[
e_{0,1} = \beta \sum_{j=0}^{\beta} (-1)^j (j-1) \binom{\beta-j}{\beta-j} \frac{\beta}{\beta-j+1} (\binom{\beta+1}{j}) = \sum_{j=0}^{\beta} \frac{(-1)^{j-1}}{\beta-j+1} \left( \frac{\beta}{(j)} \right),
\]
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 \(c_1, \ldots, c_\alpha\). The bottom left \((\alpha-1) \times (\alpha-1)\) submatrix of \(A_0\) is upper triangular with units on the diagonal, all but the top entry of the vector
\[ c_{\alpha} - \binom{\alpha-2}{1} c_{\alpha-1} + \cdots + (-1)^{\alpha-2} \binom{\alpha-2}{\alpha-2} c_2 \]
are zero, and that top entry is
\[ \beta \sum_{j=0}^{\beta-2} (-1)^j \binom{\beta-2}{j} \binom{\beta-j-2}{\beta-j} = \sum_{j=0}^{\beta-2} \frac{(-1)^j}{\beta-j+1} \left( \binom{\beta-1}{j} \right) = (-1)^{\beta} \in \mathbb{F}_p^\times. \]
Therefore \(A_0\) is invertible.

\[ \textbf{Lemma 14.} \] Suppose that \(s, \alpha, \beta \in \mathbb{Z}\) are such that
\[ s \in \{2, 4, \ldots, p-3\} \text{ and } \frac{s}{\alpha} \leq s \leq \text{ and } 1 \leq \beta \leq \alpha. \]
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
\[ M_{i,j} = \binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j}, \]
and if \(i \in \{0, \ldots, \alpha\}\setminus\{1, \ldots, \beta-1\}\) and \(j \in \{0, \ldots, \alpha\}\) then
\[ M_{i,j} = \sum_{l,v=0}^{\alpha} (-1)^{1+l+v} \binom{l}{j} \binom{\alpha-v}{l-v} \binom{s+\beta-j}{v} \binom{\alpha-v}{v} - \sum_{l=0}^{\alpha} \binom{l}{j} \binom{\alpha-v}{l} - [i=0] \binom{s+\beta-j}{j} - [i=\beta] \binom{s+\beta-j}{s+\beta-j} - \binom{-1}{\beta} \binom{s+\beta-j}{s-\alpha} \sum_{l=0}^{\alpha} \binom{l}{j} \binom{\alpha-v}{j}. \]
Suppose that \(C_0, \ldots, C_\alpha \in \mathbb{F}_p\) are defined as
\[ C_j = \begin{cases} 
1 & \text{if } j = 0, \\
(-1)^{i+1}(s+\beta)(\alpha+j) & \text{if } j \in \{1, \ldots, \alpha\}. 
\end{cases} \]
Then
\[ M(C_0, C_1, \ldots, C_\alpha)^T = \left( \frac{(-1)^{p+\beta+1}(s+\beta)(\alpha+j)}{\beta^2(2\alpha-\beta+1)} \binom{\alpha}{s} \right)^T. \]
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

\[ \binom{s - \alpha + j - v}{j - v} = \binom{s - \alpha + j - v}{j - v}. \]

We have the following string of equations:

\[
\sum_{j \geq 0} (-1)^{j+1} \binom{j}{2\alpha - s + 1} \binom{\alpha + 1}{j + 1} \binom{s - \alpha - \beta + j}{s - \alpha} = \\
\sum_u \binom{j}{\alpha + u} \sum_{j \geq 0} (-1)^{\alpha - j + 1} \binom{j}{2\alpha - s + 1} \binom{\alpha + 1}{j + 1} \binom{s - \alpha - \beta + j}{s - \alpha - u}
\]

\[
= \sum_u \binom{j}{\alpha + u} \sum_{j \geq 0} (-1)^{j + u + 1} \binom{\alpha + 1}{j + 1} \binom{s - \alpha + j - u}{\alpha - u + 1}
\]

\[
= \sum_u \binom{j}{\alpha + u} (-1)^{u + 1} \binom{s - \alpha - u + 1}{\alpha - u + 1} + \sum_j (-1)^{j + u + 1} \binom{\alpha + 1}{j + 1} \binom{s - \alpha + j - u}{\alpha - u + 1}
\]

\[
= \sum_u \binom{j}{\alpha + u} (-1)^{u + 1} \binom{s - \alpha - u + 1}{\alpha - u + 1} + [u = 0] (-1)^{\alpha + 1}
\]

\[
= (-1)^\alpha \binom{\beta}{\alpha} - \binom{\alpha + 1}{\alpha + 1}.
\]

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

\[ \sum_{j=0}^\alpha C_j \binom{s - \alpha - \beta + j}{s - \alpha} = (-1)^{\alpha + 1} \binom{s - \alpha - \beta}{\alpha + 1}. \]

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

\[ \sum_{l=0}^\alpha (-1)^l \binom{l}{j - v} = (-1)^j \binom{v}{j - v} \]

for \(0 \leq v \leq j \leq \alpha\) and therefore

\[
M_{0,j} = \sum_{l=0}^\alpha (-1)^{l+v} \binom{l}{j - v} \binom{s - \alpha - \beta}{s - \alpha - v} \binom{s - \alpha - \beta + v}{s - \alpha - v} - \binom{s - \alpha - \beta}{s - \alpha} \sum_{l=0}^\alpha \binom{l - \beta - 1}{l}^\alpha
\]

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

\[
M_{0,0} = \sum_{l=0}^\alpha (-1)^{l+v} \binom{l}{j - v} \binom{s - \alpha - \beta}{s - \alpha - v} \binom{s - \alpha - \beta + v}{s - \alpha - v} - \binom{s - \alpha - \beta}{s - \alpha} \sum_{l=0}^\alpha \binom{l - \beta - 1}{l}^\alpha
\]

\[
= \sum_{l=0}^\alpha (-1)^{\alpha + l+v} \binom{l}{j - v} \binom{s - \alpha - \beta}{s - \alpha} \binom{s - \alpha - \beta + v}{s - \alpha} - \binom{s - \alpha - \beta}{s - \alpha} \sum_{l=0}^\alpha \binom{l - \beta - 1}{l}^\alpha
\]

\[
= \sum_{l=0}^\alpha (-1)^{\alpha + l+v} \binom{l}{j - v} \binom{s - \alpha - \beta}{s - \alpha} \binom{s - \alpha - \beta + v}{s - \alpha} + \binom{s - \alpha - \beta}{s - \alpha} \sum_{l=0}^\alpha (-1)^l \sum_v (-1)^{v+1} \binom{s - \alpha - \beta}{s - \alpha - v} \binom{s - \alpha - \beta}{s - \alpha - v}. \]
The third equality follows from lemma [7]. Thus \( r_0(C_0, \ldots, C_a)^T \) is equal to
\[
\sum_{i,v=0}^\alpha (-1)^{\alpha+i+v} (s-a-\beta)^\vartheta \left( \binom{\alpha}{i} \binom{v}{v} \right) (s-a)^{i-v} + \frac{s-a-\beta}{\vartheta} (s-a)^i \binom{1}{i-v}
\]
\[
= (-1)^\alpha \sum_{i=0}^\alpha (s-a-\beta)^\vartheta \left( \binom{\alpha}{i} \binom{\alpha+1}{s-a} \right) + \frac{s-a-\beta}{\vartheta} (s-a)^i \binom{1}{2a-s}
\]
\[
= \left( \frac{\alpha}{(s-a)} + \frac{s-a-\beta}{\vartheta} (s-a)^i \binom{\alpha+1}{s-a} \right) \sum_{v=0}^\alpha (-1)^v (s-a-\beta)^\vartheta (s-a-v-1)
\]
\[
= \frac{(-1)^{a+\beta+1}}{\beta^2 (2a-s+1)} \binom{\alpha}{s-a}.
\]

The third equality follows from lemma [7]. Thus we have computed
\[
r_0(C_0, \ldots, C_a)^T = \frac{(-1)^{a+\beta+1}(s-a)(a-\beta+1)}{\beta^2(2a-s+1)} \binom{\alpha}{s-a}.
\]

- **Computing** \( r_i(C_0, C_1, \ldots, C_a)^T \) for \( i \in \{1, \ldots, \beta-1\} \). Let \( w \in \mathbb{Z} \) be such that \( i = \beta - w \in \{1, \ldots, \beta-1\} \). Then
\[
\sum_{j\geq 0} \binom{s-a-\beta}{\beta} \binom{j}{2a-s+1} (s-a-\omega)^j
\]
\[
= \sum_u \binom{\alpha-\beta+1}{\beta} \sum_{j\geq 0} \frac{(-1)^{j+1}(s-a-\beta)}{2a-s} \binom{j}{2a-s+1} (s-a-\omega)^j
\]
\[
= \sum_u \binom{\alpha-\beta+1}{\beta} (s-a-\omega+1) \sum_{j\geq 0} \frac{(-1)^{j+1}(s-a-\beta)}{2a-s} \binom{j}{2a-s+1} (s-a-\omega+1)^j
\]
\[
= (-1)^{s-a-\omega+1} \sum_{u} \binom{\alpha-\beta+1}{\beta} (s-a-\omega+1)^u
\]
\[
= \frac{s-a-\beta}{\beta} (s-a-\beta+1) (s-a-\omega)^\beta = \frac{1}{\beta} (s-a-\beta).
\]

The third equality follows from (22-23). Consequently, if \( i \in \{1, \ldots, \beta-1\} \) then
\[
r_i(C_0, \ldots, C_a)^T = 0.
\]

- **Computing** \( r_i(C_0, C_1, \ldots, C_a)^T \) for \( i \in \{\beta, \alpha\} \). For these \( i \) we have
\[
M_{i,0} = \sum_{i,v=0}^\alpha (-1)^{i+\alpha+i+v} (s-a-\beta)^\vartheta \left( \binom{\alpha}{i} \binom{v}{v} \right) \binom{1}{i-v}
\]
\[
- [i = \beta] \binom{s-a-\beta}{\beta} (s-a-\beta)^\vartheta - (-1)^i (s-a-\beta)^\vartheta \sum_{l=0}^\alpha \binom{\alpha}{l} (l-\beta-1)^\vartheta,
\]
and for \( j > 2a-s \) we also have
\[
M_{i,j} = \sum_{i,v=0}^\alpha (-1)^{i+j+v} (s-a-\beta)^\vartheta \left( \binom{\alpha}{i} \binom{v}{v} \right) \binom{1}{j-v}
\]
\[
- [i = \beta] (s-a-\beta)^\vartheta - (-1)^i (s-a-\beta)^\vartheta \sum_{l=0}^\alpha \binom{\alpha}{l} (l-\beta-1)^\vartheta.
\]

The identity
\[
\sum_{j=0}^\alpha (-1)^{j+1} (2a-s) (s-a)^j \binom{\alpha+1}{j+1} (s-a)^j
\]
\[
= \frac{\vartheta}{\beta} \left( \sum_{j=0}^\alpha (-1)^{j+1} (2a-s) (s-a)^j \binom{j+1}{j+1} (s-a)^j \right)
\]
\[
= \frac{\vartheta}{\beta} \left( (z+s-a+1) - (s-2a-2) \right)
\]
\[
= (z+s-a-1)^\vartheta.
\]
is true over $\mathbb{Q}_p[z]$. By evaluating at $z = -\beta$ we get
\[
\sum_{j=1}^{\alpha} C_j \frac{(s - \alpha - \beta + j)}{s - \alpha} \frac{\partial}{\partial (s - \alpha - \beta + 1)} \frac{\partial}{\partial (s - \alpha - \beta - 1)} \frac{\partial}{\partial (s - \alpha - \beta - 1)},
\]
and consequently
\[
\Phi(z) = (\alpha - s)\Phi_1(z) - \Phi_2(z) + (z + s - \alpha)(\Phi_3(z) + \Phi_4(z))
\]
and
\[
\Phi_1(z) = \sum_{l,v=0}^{\alpha} (-1)^{l+v+1} (s - \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha},
\]
\[
\Phi_2(z) = \left( \frac{\alpha}{s - \alpha - 1} \right) \left( \frac{\alpha}{i - 1} \right),
\]
\[
\Phi_3(z) = \sum_{l,v=0}^{\alpha} (-1)^{s+j+l+v+1} (s - \alpha)_v (z + s - \alpha)_v (z + s + j - v),
\]
\[
\Phi_4(z) = \left( \frac{\alpha + 1}{s - \alpha} \right) \left( \frac{\alpha}{i - 1} \right).
\]
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
\[
\beta \Phi_1'(-\beta) = \beta \sum_{l,v=0}^{\alpha} (-1)^{l+v+1} (s - \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha}
\]
\[
= \sum_{l,v=0}^{\alpha} (-1)^{i}\beta (s - \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha}
\]
\[
= \sum_{l,v=0}^{\alpha} (-1)^{i} (l - \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha}
\]
\[
= \sum_{l,v=0}^{\alpha} (l = 0) (-1)^{\beta + l+1} + [l = \beta] (-1)^l (l - \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha}
\]
\[
= (-1)^\beta (l - \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha}
\]
\[
= (-1)^\beta (l + \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha}
\]
\[
= (-1)^\beta (l + \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha}
\]
\[
= \Phi_2(-\beta).
\]
Now suppose that $s \neq \alpha + \beta$. As in the proof of lemma [7] we can simplify $\Phi_1(z)$ to
\[
\Phi_1(z) = - (z + s - \alpha) \sum_{l=0}^{\alpha} (l + \alpha)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha},
\]
We can also simplify $\Phi_3(z)$ to
\[
\Phi_3(z) = \sum_{j,v=0}^{\alpha} (-1)^{s+j+l+v+1} (2s - \alpha)_v (z + s - \alpha)_v (z + s + j - v)
\]
\[
= \left( \frac{z + s - \alpha}{z + s - \alpha} \right) \left( \frac{z + s + j - v}{z + s - \alpha} \right),
\]
Suppose first that $i > \beta$. Then
\[
\Phi_1'(-\beta) = - \sum_{l=0}^{\alpha} (l - \beta)_v (z + s - \alpha)_v (z - \alpha)_{l-\alpha},
\]
\[
\Phi_2(-\beta) = 0,
\]
\[
\Phi_3'(-\beta) = \sum_{j=0}^{\alpha} (-1)^{s+j+1} (z + s + j + 1)_v (z + s - \alpha)_v (z - \alpha)_{j-\alpha},
\]
\[
\Phi_4'(-\beta) = (-1)^{\beta}(z + s - \alpha)_v (z - \alpha)_{l-\alpha}.
\]
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

$$L_1 := \sum_{l=0}^{\alpha} \binom{l}{i-\beta-1} \binom{l-\beta-1}{s-\alpha-\beta-1},$$

$$R_1 := \binom{s-\alpha}{\beta+1} \sum_{j=0}^{s-\alpha-i+1} \binom{j+1}{s-j+i} \binom{\alpha+1}{j+1} \binom{\alpha-\beta}{j-i}.$$  

Let us in fact show that

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

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

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

since both sides are zero, and

$$R_1(u + 1, v + 1, w, t) - R_1(u, v, w, t) - L_1(u + 1, v + 1, w, t) + L_1(u, v, w, t)$$

$$= \left(\frac{u-v}{u+v+1}\right)^{u-v} \sum_{j=0}^{u-v} (-1)^j \binom{j}{v+1} \binom{v+1}{j} \binom{v-w+j}{u-v-w+t}$$

$$- \left(\frac{u-v}{u+v+2}\right)^{u-v} \sum_{j=0}^{u-v} (-1)^j \binom{j}{v+1} \binom{v+1}{j} \binom{v-w+j}{u-v-w+t}$$

$$+ \left(\frac{u-v}{u+v+2}\right)^{u-v} \sum_{j=0}^{u-v} (-1)^j \binom{j}{v+1} \binom{v+1}{j} \binom{v-w+j}{u-v-w+t}.$$

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

$$\sum_j (-1)^j \binom{j}{v+1} \binom{v+1}{j} \binom{v-w+j}{u-v-w+t}$$

$$= \sum_{j, e} (-1)^j \binom{v-w+1}{u-v-w+i-e} \binom{j}{v+1} \binom{v-w+1}{u-v-w+i-e} \binom{v-w+1}{u-v-w-t+e}$$

$$= \sum_{j, e} (-1)^j \binom{v-w+1}{u-v-w+i-e} \binom{j}{v+1} \binom{v-w+1}{u-v-w+i-e} \binom{v+1}{u-v-w-t+e}$$

$$= \sum_{j, e} (-1)^j \binom{v-w+1}{u-v-w+i-e} \binom{j}{v+1} \binom{v-w+1}{u-v-w+i-e} \binom{v+1}{u-v-w-t+e}$$

$$= (-1)^{v+1} \binom{v-w+1}{u-v} \binom{v+1}{u-v}.$$  

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

$$L_2 := \sum_{i=\alpha+1}^{\alpha} \binom{i-\beta-1}{l-\beta-1},$$

$$R_2 := \sum_{j=0}^{s-\alpha-i+1} \binom{j+1}{s-j+i} \binom{\alpha+1}{j+1} \binom{\alpha-\beta}{s-\alpha-\beta} + \binom{s+1}{\alpha-\beta}.$$  

Let us in fact show that

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

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

$$L_2(u, t, w, t) = R_2(u, t, w, t),$$
and
\[ R_2(u + 1, v + 1, w, t) - R_2(u, v, w, t) - L_2(u + 1, v + 1, w, t) + L_2(u, v, w, t) = \frac{u-v}{2v-u+2} \sum_{j=0}^{u} (-1)^{v+j} \binom{j}{v} \left( \binom{v+1}{j} - \binom{1}{j} \binom{u-v-w}{j-1} \right), \]
which is zero by (2). Finally, suppose that \( i = \beta \). Then
\[
\Phi_1'(-\beta) = - \sum_{l=0}^{\alpha} \binom{l}{j} \left( \binom{s-\alpha-\beta}{s-\alpha} \binom{l-\beta-1}{l+\alpha-s} + \binom{s-\alpha-\beta}{s-\alpha} \binom{l-\beta-1}{l+\alpha-s} \right),
\]
\[
\Phi_2'(-\beta) = (-1)^{\beta+1} \binom{s-\alpha-1}{s-\alpha},
\]
\[
\Phi_3'(-\beta) = \sum_{j=0}^{\alpha} (-1)^{\alpha+\beta+j+1} \binom{j}{2\alpha-s+1} \binom{\alpha+1}{j+1} \binom{\alpha+s-\beta}{s-\alpha} \binom{j+1}{s-\alpha} h_\beta,
\]
\[
\Phi_4'(-\beta) = (-1)^{\beta} \binom{s+1}{s-\alpha} (h_\alpha - h_\beta),
\]
where \( h_t = 1 + \cdots + \frac{1}{t} \) is the harmonic number for \( t \in \mathbb{Z}_{>0} \) and \( h_0 = 0 \) for \( t \in \mathbb{Z}_{\leq 0} \).

Since
\[
\sum_{j=0}^{\alpha} (-1)^{\alpha+\beta+j+1} \binom{j}{2\alpha-s+1} \binom{\alpha+1}{j+1} \binom{\alpha+s-\beta}{s-\alpha} \binom{\alpha+1}{j+1} (\frac{s+\alpha+s-j}{s-\alpha}) = (-1)^{\alpha+\beta} (\frac{s+\alpha+s-1}{s-\alpha} - \frac{s+2\alpha-2}{s-\alpha}),
\]
we can simplify \( \Phi_4'(-\beta) \) to
\[
\Phi_4'(-\beta) = \sum_{j=0}^{\alpha} (-1)^{\alpha} \binom{j}{2\alpha-s+1} \binom{\alpha+s-1}{s-\alpha} \binom{j+1}{s-\alpha} (-1)^{\beta} \binom{\alpha+1}{s-\alpha} h_\beta.
\]
The equation \( \Phi(-\beta) = 0 \) is therefore equivalent to
\[
L_3(s, \alpha, \beta) = R_3(s, \alpha, \beta)
\]
with
\[
L_3 := \beta \Phi_1'(-\beta),
\]
\[
R_3 := (s-\alpha-\beta) (\Phi_3'(-\beta) + \Phi_4'(-\beta)) - \Phi_2'(-\beta).
\]
Let us show that \( L_3(u, v, w) = R_3(u, v, w) \) for all \( u > v \geq w > 0 \). For \( v = w \) this is
\[
(-1)^w \left( \frac{w-1}{u-w} \right)^{\beta} \binom{1}{2w-u} - \left( \frac{w-1}{u-w} \right)^{\beta} \binom{1}{2w-u} = (2w-u) (\frac{w}{u-w} h_w + (\frac{w-1}{2w-u})).
\]
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 \( w(h_{u-1} + \frac{1}{2w-u}) \). 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 \( u > v \geq w > 0 \). By using the equation
\[
\sum_{j=0}^{\alpha} (-1)^j \binom{j}{2\alpha-s+1} \binom{\alpha+s-1}{s-\alpha} \binom{j+1}{s-\alpha} (\frac{s+\alpha+s-j}{s-\alpha}) = (-1)^{\alpha+\beta} \binom{s+1}{s-\alpha} (h_{\alpha} - h_\beta),
\]
we can get rid of the sum \( \sum_{j} \) and, after some simple algebraic manipulations, simplify this to
\[
\left( \frac{w-1}{u-w} \right)^{\beta} \binom{1}{2w-u} - \left( \frac{w-1}{u-w} \right)^{\beta} \binom{1}{2w-u} = \frac{(w+1)(w-w-1)}{w(w-w-1)} (\frac{w-1}{u-v}).
\]
We omit the full tedious details and just mention that since we are able to get rid of the sums \( \sum_i \) and \( \sum_j \) the aforementioned algebraic manipulations amount to simple cancellations. If \( u \geq v + w \) then
\[
\begin{align*}
\frac{(v+1)}{w} \left( \left( \frac{u-v-w}{u-v} \right)^\beta \left( \frac{v-w}{2v-u+1} \right) + \left( \frac{u-v-w}{u-v} \right) \left( \frac{v-w}{2v-u+1} \right)^\beta \right)
&= \frac{(-1)^{v+1}(v+1)!(u-w)!((u-v-w)!(w-1))!}{u(w-v+1)!(u-v-w)!(2v-u+1)!}
\end{align*}
\]
and if \( u < v + w \) then
\[
\begin{align*}
\frac{(v+1)}{w} \left( \left( \frac{u-v-w}{u-v} \right)^\beta \left( \frac{v-w}{2v-u+1} \right) + \left( \frac{u-v-w}{u-v} \right) \left( \frac{v-w}{2v-u+1} \right)^\beta \right)
&= \frac{(-1)^{v+1}(v+1)!(u-v-w)!(v-w)!(v+1)!}{u(w-v+1)!(u-v-w)!(2v-u+1)!}
\end{align*}
\]
We have finally shown that if \( i \in \{\beta, \ldots, \alpha\} \) then
\[
\mathbf{r}_i(C_0, \ldots, C_{\alpha})^T = 0.
\]

\[\blacksquare\]

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

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

Lemma 15. Suppose that \( \alpha \in \{0, \ldots, \nu - 1\} \).

(1) We have
\[
(T - a) \left( 1 \bullet_{KZ} x_\nu \theta^{a+n} y^{r-np-\alpha} \right)
= \sum_j (-1)^j \binom{j}{\nu} \theta^{p(j+1)+\alpha \theta} \bullet_{KZ} x^{j(p+1)+\alpha} y^{r-j(p-1)-\alpha}
- a \sum_j (-1)^j \binom{n-\alpha}{j} \bullet_{KZ} x^{\theta^\beta(p+1)} y^{r-j(p-1)-\alpha(p+1)} + O(p^n).
\]

(2) The submodule \( \text{im}(T - a) \subset \text{ind}_{KZ}^{\mathbb{Z}} \sum_r \) contains
\[
\sum_i \left( \sum_{i=\beta-\gamma}^{i=\beta-l} C_l \right) \bullet_{KZ} x^{i(p+1)+\beta} y^{r-i(p-1)-\beta}
+ O(ap^{\beta+\nu} + p^{p-1})
\]
for all \( 0 \leq \beta \leq \gamma < \nu \) and all families \( \{C_l\} \) of elements of \( \mathbb{Z}_p \), where
\[
v_C = \min_{\beta-\gamma \leq i \leq \beta} (v_\mu(C_l) + l).
\]
The \( O(ap^{\beta+\nu} + p^{p-1}) \) term is equal to \( O(p^{p-1}) \) plus
\[
-\frac{ap^{\beta}}{p-1} \sum_{i=\beta-\gamma}^{i=\beta-l} C_l \sum_{\nu \neq \mu \in \mathbb{Z}_p} \left[ \mu \right]^{-1} \binom{p}{\mu} \theta^{n\beta - l - n} y^{r-np-\beta + l}.
\]
Lemma 16. Suppose that $\alpha \in \mathbb{Z}$ and $v \in \mathbb{Q}$ are such that

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

$$
v \leq v_p(\vartheta_\alpha(D_\bullet)),
$$

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

$$
v' < v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leq w < \alpha.
$$

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

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

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

$$
\sum_i(\Delta_i - D_i) \cdot KZ \cdot x\gamma(p-1) + \alpha y\gamma(p-1) - \alpha
$$

$$
= [\alpha \leq s](1)^{n+1}D_{\theta}\cdot KZ \cdot \theta^\alpha y^{r-s+\alpha} - D_{0} \cdot KZ \cdot \theta^\alpha y^{r-s+\alpha}
$$

$$
+ E \cdot KZ \cdot \theta^\alpha h + F \cdot KZ \cdot \theta^\alpha h' + \text{ERR}_1 + \text{ERR}_2,
$$

for some ERR\(_1\) and ERR\(_2\) such that

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

some polynomials $h$ and $h'$, and some $E, F \in \mathbb{K}_p$ such that $v_p(E) \geq v'$ and $v_p(F) > v'$.

Lemma 17. Let $\{C_i\}_{i \in \mathbb{Z}}$ be any family of elements of $\mathbb{Z}_p$. Suppose that $\alpha \in \{0, \ldots, \nu - 1\}$ and $v \in \mathbb{Q}$, and suppose that the constants

$$
D_i := \lfloor i = 0 \rfloor C - 1 + [0 < i(p-1) < r - 2\alpha] \sum_{i=0}^\alpha C_i(r - \alpha + i)
$$

satisfy the conditions of lemma 16, i.e.

$$
v \leq v_p(\vartheta_\alpha(D_\bullet)),
$$

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

$$
v' < v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leq w < \alpha.
$$

Moreover, suppose that $C_0$ is a unit. Let

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

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

(1) If $v_p(\vartheta') \leq v'$ then there is some element $\text{gen}_1 \in \mathcal{I}_a$ that represents a generator of $\tilde{N}_\alpha$.

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

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

where $T$ denotes the endomorphism of $\text{ind}_{KZ}^G \text{quot}(\alpha)$ corresponding to the double coset of $(\text{gen}_2)$.

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

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

are such that

\[
\alpha \in \{0, \ldots, \nu - 1\},
\]

\[
v \leq v_p(\vartheta(D_\#)),
\]

\[
v' := \min \{v_p(a) - \alpha, v\} < v_p(\vartheta_w(D_\#)) \text{ for } 0 \leq w < \alpha.
\]

Let

\[
\vartheta' := (1 - p)^{-\alpha} \vartheta(D_\#) - C_{-1}.
\]

Then \( \text{im}(T - a) \) contains

\[
(\vartheta' + C_{-1}) \cdot KZ_{\mathbb{F}_p} \theta^{n \cdot x^{p-1} y^{r - \alpha(p + 1) - p - 1}} + C_{-1} \cdot KZ_{\mathbb{F}_p} \theta^{n \cdot x^{\alpha - n} y^{r - np - \alpha}}
\]

(3)

\[
+ \sum_{2\nu - \alpha - 1}^{2\nu - \alpha + 1} E_\xi \cdot KZ_{\mathbb{F}_p} \theta^\xi h_\xi + F \cdot KZ_{\mathbb{F}_p} h' + H,
\]

for some \( h_\xi, h', E_\xi, F, H \) such that

1. \( E_\xi = \vartheta(D_\#) + \mathcal{O}(p^\nu) \cup \mathcal{O}(\vartheta_{\alpha + 1}(D_\#)) \cup \cdots \cup \mathcal{O}(\vartheta_{\xi - 1}(D_\#)), \)

2. if \( \xi + \alpha - s \leq 2\xi - s \neq 0 \) then the reduction modulo \( \mathfrak{m} \) of \( \theta^\xi h_\xi \) generates \( N_\xi, \)

3. \( v_p(F) > v', \) and

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

\[
\frac{1 - p}{p - \alpha} H = g \cdot KZ_{\mathbb{F}_p} \theta^{n \cdot x^{\alpha - n} y^{r - np - \alpha}} + \mathcal{O}(p^{\nu - v_p(a)})
\]

with

\[
g = \sum_{\lambda \in \mathbb{F}_p} C_0(p^{\lambda |\lambda|}) + A(p^{0 \lambda}) + [r \equiv 1 \pmod{p - 1}] B(p^{0 \lambda}),
\]

where

\[
A = -C_{-1} + \sum_{l=1}^{\alpha} C_l \binom{r - \alpha + l}{i}
\]

and

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

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

\[
(\vartheta' + C_{-1}) \cdot KZ_{\mathbb{F}_p} \theta^{n \cdot x^{p-1} y^{r - \alpha(p + 1) - p - 1}} + C_{-1} \cdot KZ_{\mathbb{F}_p} \theta^{n \cdot x^{\alpha - n} y^{r - np - \alpha}}
\]

by \( \vartheta' \). 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 \( h_\xi, E_\xi, F, H, A, \) and \( B \) claimed in (1), (2), (3), and (4). The \( h_\xi \) and \( E_\xi \) come from the proof of lemma [16] and \( E_\xi \cdot KZ_{\mathbb{F}_p} \theta^\xi h_\xi \) is

\[
X_\xi \cdot KZ_{\mathbb{F}_p} \sum_{\lambda \neq 0} (-\lambda)^r \theta^{n \cdot x^{r - np - \xi} y^{s - n}},
\]
with the notation for \(X_ξ\) from the proof of lemma 16. Let \(E_ξ = (-1)^{ξ+1}X_ξ\). Then condition (1) is satisfied directly from the definition of \(X_ξ\). Let

\[
h_ξ = (-1)^{ξ+1} \sum_{λ \neq 0} (-λ)^{r-α-ξ(1_0 \ 1)}(-θ)^{α,r-yp-ξy^{ξ−n}}.
\]

This reduces modulo \(m\) to the element

\[
(-1)^{ξ} \sum_{λ \neq 0} (-λ)^{r-α-ξ(1_0 \ 1)}Y^{2ξ−r} = (-1)^{s−α+1}X^{ξ+α−s}Y^{ξ−α}
\]

of

\[
σ_{2ξ−r}(r − ξ) ∼ I_{r−2ξ}(ξ)/σ_{r−2ξ}(ξ) = quot(ξ).
\]

This element is non-trivial and generates \(N_ξ\) if \(ξ + α − s ≤ 2ξ − s ≠ 0\), since then \(X^{ξ+α−s}Y^{ξ−α}\) generates \(N_ξ\). This verifies condition (2). Condition (3) follows from the assumption \(v' < v_p(\vartheta_w(D_*)\)) for \(0 ≤ w < α\), 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 \(\{C_i\}_{i ∈ \mathbb{Z}}\) be any family of elements of \(\mathbb{Z}_p\). Suppose that \(α ∈ \{0, \ldots, ν − 1\}\) and \(v ∈ \mathbb{Q}\), and suppose that the constants

\[
D_i := [i = 0]|C_{i+1}| + [0 < i(p − 1) < r − 2α]\sum_{l=0}^{α} C_i \binom{r−α+l}{i−l}
\]

are such that

\[
v ≤ v_p(\vartheta_α(D_*)\)),
\]

\[
v' := \min\{v_p(α − α, v) ≤ v_p(\vartheta_w(D_*)\))\ for \(α < w < 2ν − α\),
\]

\[
v' < v_p(\vartheta_w(D_*)\)) \ for \(0 ≤ w < α\).
\]

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

\[
\vartheta' := (1 − p)^{−α}\vartheta_α(D_*) − C_{−1},
\]

\[
\tilde{C} := −C_{−1} + \sum_{l=1}^{α} C_i \binom{r−α+l}{i−l}.
\]

If \(*\) then \(*\) is trivial modulo \(\mathcal{F}_a\), for each of the following pairs

\[
(*, *) = \text{(condition, representation)}.
\]

1. \((v_p(\vartheta')) ≤ \min\{v_p(C_{−1}), v', \tilde{N}_{a}\}\).
2. \((v = v_p(C_{−1}) < \min\{v_p(\vartheta'), v_p(α − α), \ ind_{K^{G}}^{G} \ sub(α)\}\).
3. \((v_p(α) − α < v ≤ v_p(C_{−1}) \ni C \in \mathbb{Z}_p^\times \ni C_0 \notin \mathbb{Z}_p^\times \ni 2α − r > 0, \tilde{N}_{a}\))
4. \((v_p(α) − α < v ≤ v_p(C_{−1}) \ni C \in \mathbb{Z}_p^\times, \ ind_{K^{G}}^{G} \ quot(α)\))
5. \((v_p(α) − α < v ≤ v_p(C_{−1}) \ni C_0 \in \mathbb{Z}_p^\times, r_1\), where

\[
r_1
\]

is a finite-codimensional submodule of

\[
T(\ind_{K^{G}}^{G} \ quot(α)).
\]
Proof. There is one extra condition imposed in addition to the conditions from lemma 18 that
\[ v' := \min \{ v_p(\alpha) - \alpha, v \} \leq v_p(\partial_w(D_\ast)) \text{ for } \alpha < w < 2\nu - \alpha, \]
and it ensures that \( v_p(E_\xi) \geq v' \) for all \( \alpha < \xi < 2\nu - \alpha \). Lemma 18 implies that the element in (3) is in \( \text{im}(T - a) \). Let us call this element \( \gamma \).

(1) The condition \( v_p(\partial') \leq \min \{ v_p(C_{-1}), v' \} \) ensures that if we divide \( \gamma \) by \( \partial' \) then the resulting element reduces modulo \( m \) to a representative of a generator of \( N_\alpha \).

(2) The condition \( v = v_p(C_{-1}) < \min \{ v_p(\partial'), v_p(\alpha) \} \) ensures that if we divide \( \gamma \) by \( C_{-1} \) then the resulting element reduces modulo \( m \) to a representative of a generator of \( \text{ind}^G_K \text{sub}(\alpha) \).

(3) [4] [5] The condition \( v_p(\alpha) - \alpha < v \leq v_p(C_{-1}) \) ensures that the term with the dominant valuation in (3) is \( H \), so we can divide \( \gamma \) by \( ap^{-\alpha} \) and obtain the element \( L + O(p^\nu v_p(\alpha)) \), where \( L \) is defined by
\[
L := \left( \sum_{\lambda \in \mathbb{F}_p} C_0(\frac{p^{|\lambda|}}{0 1}) + A(\frac{0 0}{0 1}) + [r \equiv_{p-1} 2\alpha]B(\frac{0 0}{0 1}) \right) \cdot K_{Z,\mathbb{F}_p} \cdot \theta^n x^{a - n} y^{x - np - \alpha}
\]
with \( A \) and \( B \) as in lemma 18. This element \( L \) is in \( \text{im}(T - a) \), and it reduces modulo \( m \) to a representative of
\[
\left( \sum_{\lambda \in \mathbb{F}_p} C_0(\frac{p^{|\lambda|}}{0 1}) + A(\frac{0 0}{0 1}) + [r \equiv_{p-1} 2\alpha](-1)^{r - \alpha}B(\frac{1 0}{0 1}) \right) \cdot K_{Z,\mathbb{F}_p} X^{2\alpha - r}.
\]
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 \( T(\text{ind}^G_K \text{quot}(\alpha)) \), and if additionally \( A \neq 0 \) (over \( \mathbb{F}_p \)) then in fact we have the stronger conclusion that it generates \( \text{ind}^G_K \text{quot}(\alpha) \).

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

5. Proof of theorem 2

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

We assume that
\[ r = s + \beta(p - 1) + u_0 p^t + O(p^{t+1}) \]
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 [Ars] implies theorem 2 for \( s \geq 2\nu \), we may assume that
\[ s \in \{2, \ldots, 2\nu - 2\}. \]
Recall also that we assume \( \nu - 1 < v_p(a) < \nu \) for some \( \nu \in \{1, \ldots, \frac{p^t - 1}{p} \} \), 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
\[
\begin{cases}
\hat{N}_{\alpha} & \text{if } \beta \in \{0, \ldots, \alpha - 1\} \text{ and } \alpha > v_p(a) - t, \\
\text{ind}^G_{KZ} \text{sub}(\alpha) & \text{otherwise}
\end{cases}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 21. If $\frac{s}{2} \leq \alpha < s$ and $\beta \notin \{1, \ldots, \alpha + 1\}$ then
\[
\hat{N}_{\alpha}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 22. If $0 < \alpha < \frac{s}{2}$ then
\[
\begin{cases}
T(\text{ind}^G_{KZ} \text{quot}(\alpha)) & \text{if } \beta \in \{0, \ldots, \alpha\} \text{ and } \alpha > v_p(a) - t, \\
\hat{N}_{s-\alpha} & \text{if } \beta \in \{0, \ldots, \alpha\} \text{ and } \alpha < v_p(a) - t, \\
\hat{N}_{\alpha} & \text{if } \beta \in \{\alpha + 1, \ldots, s - \alpha\}, \\
\hat{N}_{s-\alpha} & \text{if } \beta > s - \alpha
\end{cases}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 23. If $\frac{s}{2} \leq \alpha < s$ and $(\alpha, \beta) \neq (\frac{s}{2}, \frac{s}{2} + 1)$ then
\[
\begin{cases}
T(\text{ind}^G_{KZ} \text{quot}(\alpha)) & \text{if } \beta \in \{1, \ldots, s - \alpha\} \text{ and } s - \alpha > v_p(a) - t, \\
T(\text{ind}^G_{KZ} \text{quot}(\alpha)) & \text{if } \beta \in \{s - \alpha + 1, \ldots, \alpha\} \text{ and } \alpha > v_p(a) - t, \\
\hat{N}_{\alpha} & \text{otherwise}
\end{cases}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 24. If $\alpha \geq s$ then
\[
\begin{cases}
T(\text{ind}^G_{KZ} \text{quot}(\alpha)) & \text{if } \alpha = \max\{\nu - t - 1, \beta - 1\}, \\
\hat{N}_{\alpha} & \text{otherwise}
\end{cases}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 25. If $\beta \in \{1, \ldots, \frac{s}{2} - 1\}$ and $t > \nu - \frac{s}{2} - 2$ then
\[
\hat{N}_{s/2 + 1}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 26. If $\beta \in \{1, \ldots, \frac{s}{2} - 1\}$ and $t = \nu - \frac{s}{2}$ then
\[
\hat{N}_{s/2 - 1}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 27. If $\beta \in \{\frac{s}{2}, \frac{s}{2} + 1\}$ and $t > \nu - \frac{s}{2} - 1$ then
\[
\hat{N}_{s/2 + 1}
\]
is trivial modulo $\mathcal{A}_a$.

Proposition 28. If $\beta = \frac{s}{2} + 1$ and $t = \nu - \frac{s}{2} - 1$ then
\[
\text{ind}^G_{KZ} \text{sub}(\frac{s}{2} + 1)
\]
is trivial modulo $\mathcal{A}_a$. 
Proof that propositions 20–28 imply theorem 2. Let us assume that \( \Sigma_{k,a} \) is reducible with the goal of reaching a contradiction. The classification given by theorem 2 in [Ars] implies that \( \Sigma_{k,a} \) has two infinite-dimensional factors, each of which is a quotient of a representation in the set

\[
\{ \text{ind}_{KZ}^G \text{sub}(\alpha) \mid 0 \leq \alpha < \nu \} \cup \{ \text{ind}_{KZ}^G \text{quot}(\alpha) \mid 0 \leq \alpha < \nu \},
\]

and moreover that the following classification is true.

1. If the two representations are \( \text{ind}_{KZ}^G \text{sub}(\alpha_1) \) and \( \text{ind}_{KZ}^G \text{sub}(\alpha_2) \) then
   \[\alpha_1 + \alpha_2 \equiv_{p-1} s + 1.\]

2. If the two representations are \( \text{ind}_{KZ}^G \text{sub}(\alpha_1) \) and \( \text{ind}_{KZ}^G \text{quot}(\alpha_2) \) then
   \[\alpha_1 - \alpha_2 \equiv_{p-1} 1.\]

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

The facts that

\[
\alpha_1 + \alpha_2 \in \{0, \ldots, 2\nu - 2\} \subseteq \{0, \ldots, p - 3\},
\]

\[
\alpha_1 - \alpha_2 \in \{1 - \nu, \ldots, \nu - 1\} \subseteq \{-\frac{p-3}{2}, \ldots, \frac{p-3}{2}\},
\]

\[
s \in \{2, \ldots, 2\nu - 2\} \subseteq \{2, \ldots, p - 3\}
\]

imply that the following classification is true as well.

1. If the two representations are \( \text{ind}_{KZ}^G \text{sub}(\alpha_1) \) and \( \text{ind}_{KZ}^G \text{sub}(\alpha_2) \) then
   \[\alpha_1 + \alpha_2 = s + 1.\]

2. If the two representations are \( \text{ind}_{KZ}^G \text{sub}(\alpha_1) \) and \( \text{ind}_{KZ}^G \text{quot}(\alpha_2) \) then
   \[\alpha_1 = \alpha_2 + 1.\]

3. If the two representations are \( \text{ind}_{KZ}^G \text{quot}(\alpha_1) \) and \( \text{ind}_{KZ}^G \text{quot}(\alpha_2) \) 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 \( \text{ind}_{KZ}^G \text{sub}(\frac{s}{2}) \) or \( \text{ind}_{KZ}^G \text{quot}(\frac{s}{2}) \), and in that case the other representation is either

\[\text{ind}_{KZ}^G \text{sub}(\frac{s}{2} + 1)\]

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

\[\text{ind}_{KZ}^G \text{quot}(\frac{s}{2} - 1)\]

(which can only happen if \( s = 2 \) or \( \beta \in \{1, \ldots, \frac{s}{2} - 1\} \) and \( t = \nu - \frac{s}{2} \)). In the latter case if \( s = 2 \) then either \( 1 \bullet_{KZ} \alpha, x^2 y^{s-2} \in \mathcal{A}_{a} \) generates \( \text{ind}_{KZ}^G \text{quot}(0) \), or \( \nu \leq 2 \) in which case \( V_{k,a} \) is known to be irreducible. Propositions 23, 25, 26, 27, and 28 exclude all of the remaining possibilities. Thus if we assume that \( \Sigma_{k,a} \) is reducible we reach a contradiction, so \( \Sigma_{k,a} \) must be irreducible. \( \blacksquare \)
Proof of proposition 20. First suppose that $\beta \geq \alpha$. 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

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

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

$$\sum_{j=1}^{\alpha} (-1)^{\alpha-j} \binom{s-\alpha+1}{\alpha-j} \sum_{i>0} \binom{r-\alpha+j}{i(p-1)+j} \binom{i(p-1)}{w} = (-1)^\alpha ([|w| = 0] - [w = 0]) \binom{s-r}{\alpha} + O(p)$$

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

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

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

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

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

and in fact we can conclude that $\tilde{N}_{a}$ is trivial modulo $\mathcal{I}_{a}$. 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

$$t < v_p(\vartheta'),$$

$$t < v_p(\vartheta_w(D_*)) \text{ for } \alpha \leq w < 2\nu - \alpha,$$

$$t < v_p(\vartheta_w(D_*)) \text{ for } 0 \leq w < \alpha.$$

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

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

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

$$A = S + \epsilon N + O(\epsilon p),$$
Then to the single equation which is itself equivalent to 
\[ v \] for some trivial modulo \( I \) and therefore we can choose \( \beta, \ldots, \beta \) ones indexed 1 where the only entries of the vector on the right that can possibly be non-zero are the \( w \) when 
\[ v \] can apply part (2) of corollary 19 with \( \text{lemma 9} \) and is therefore upper triangular with units on the diagonal. Thus we
\[ \text{with zeros outside the rows indexed 1, \ldots, \beta}, \] \( B \) implies that 
\[ B \]
\[ \text{Let we have} \]
\[ \text{We still have equation 4 since the constants are the same, and since} \]
\[ (^{\ast - r}_{\alpha}) = O(p), \]
we have 
\[ S(C_0, \ldots, C_\alpha)^T = (O(p), \ldots, O(p))^T. \]
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, \ldots, \beta and such that 
\[ (BS)_{w,j} = p^{-[j=0]} (^{\ast + \beta(p-1)-\alpha+j}_{w(p-1)+j}) \]
when \( w \in \{1, \ldots, \beta\} \). We thus have 
\[ BS(C_0, \ldots, C_\alpha)^T = (0, O(p), \ldots, O(p), 0, \ldots)^T, \]
where the only entries of the vector on the right that can possibly be non-zero are the ones indexed 1, \ldots, \beta. As in the proof of theorem 17 in [Ars] we note that \( S \) has rank \( \beta \) and therefore we can choose \( C^*_1, \ldots, C^*_\alpha \) in a way that \((C_0, \ldots, C_\alpha)^T \in \ker BS \). Then \( \partial_w(D_\alpha) = O(\epsilon) \) for all \( w \), and the conditions that need to be satisfied are 
\[ \partial'_w(D_\alpha) = O(\epsilon p) \text{ for } 0 \leq w < \alpha \text{ and } \partial'' = O(\epsilon p). \]
These two conditions are equivalent to the single equation 
\[ A(C_0, \ldots, C_\alpha)^T = (-C_{-1}, 0, \ldots, 0, C_{-1}) + O(\epsilon p), \]
which is itself equivalent to 
\[ BN(C_0, \ldots, C_\alpha)^T \]
\[ = (0, -\binom{\alpha}{1}(C_{-1}^{-1} \ldots, (-1)^{\alpha} \binom{\alpha}{\beta})(C_{-1}^{-1})^T + BSv + O(p) \]
for some \( v \). Thus, if \( \overline{T} \) is the \( \alpha \times \alpha \) matrix over \( \mathbb{F}_p \) obtained from \( \overline{BN} \) by replacing the rows indexed 1, \ldots, \beta with the corresponding rows of \( BS \) and then discarding the zeroth row and the zeroth column, the condition that needs to be satisfied is equivalent to the claim that 
\[ \left((-1 - [1 < \beta]) \binom{\alpha}{1}, \ldots, (-1)^{\alpha} (1 - [\alpha < \beta]) \binom{\alpha}{\beta} \right)^T \]
is in the image of \( \overline{T} \) (since \( C_0 = O(p) \) and \( C_{-1}^{-1} \in \mathbb{Z}_p^\times \)). This is indeed the case since \( \overline{T} \) is the lower right \( \alpha \times \alpha \) submatrix of the matrix \( \overline{Q} \) defined in the proof of theorem 17 in [Ars] (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 \( \text{ind}_{KZ}^{\alpha} \text{sub}(\alpha) \) is trivial modulo \( \mathcal{F}_a \).
Proof of proposition 22. Let us define $C_{-1}(z), \ldots, C_{\alpha}(z) \in \mathbb{Z}_p[z]$ as

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

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

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

The two conditions we need to verify are $v_p(\vartheta_w(D^*_\alpha)) > 0$ for $0 \leq w < \alpha$ and $v_p(\vartheta') = 0$.

These two conditions follow from the system of equations

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

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

$$\sum_{v=0}^{\alpha} (-1)^{w-v}(\frac{\alpha}{w-v})(\frac{s-z+v}{v}) + (\frac{z-s}{w-v})(\frac{z-s}{w-v}) - (\frac{z-s}{w}) = F_{w,j}(r),$$

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

Proof of proposition 22. First let us assume that $\beta \in \{0, \ldots, \alpha\}$. If we attempt to copy the proof of theorem 17 in [Arso] 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

$$pN_{w,0} = (s^\beta \frac{(p-1)-\alpha-\alpha}{w}) \frac{\alpha}{i_{(p-1)-\alpha-w}} + O(p),$$

where the second term is $O(p)$ because it is still true that

$$\sum_{i>0} \left(\frac{r-\alpha-w}{i(p-1)-\alpha-w}\right) - \sum_{i>0} \left(\frac{s^\beta(p-1)-\alpha-\alpha}{i(p-1)-\alpha-w}\right) = O(\epsilon p).$$

On the other hand,

$$\sum_{i>0} \left(\frac{s^\beta(p-1)-\alpha-\alpha}{i(p-1)-\alpha-w}\right) = \sum_{i=0}^{\alpha} \left(\frac{-1}{i}\right) \sum_{i>0} \left(\frac{s^\beta(p-1)-\alpha-\alpha}{i(p-1)-\alpha-w}\right)
= (-1)^{s-\alpha} \left(\frac{w}{s-\alpha}\right) + O(p).$$

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

$$A_{w,0} = S_{w,0} + (-1)^{s-\alpha} \left(\frac{w}{s-\alpha}\right) \left(s^\beta \frac{w-1}{w-1}\right) \epsilon p^{-1} + O(\epsilon)$$

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

$$(s-\alpha-\beta)^\theta = \frac{(-1)^{s-\alpha-\beta-w}}{w} \in \mathbb{Z}_p^\times.$$
What this means is that if we proceed with the proof of theorem 17 in [Ars] and apply lemma [18] with the constants \((C_{-1}, C_0, \ldots, C_\alpha)\) constructed there such that \(C_0\) is a unit, then we obtain an element

\[
(\vartheta' + C_{-1}) \ast KZ_{p_{\xi}} \theta^\alpha x^{p-1} y^{-\alpha(p+1)-p+1} + C_{-1} \ast KZ_{p_{\xi}} \theta^\alpha x^{\alpha-n} y^{r-np-\alpha} + \sum_{\xi=\alpha+1}^{2\nu-\alpha-1} E_{\xi} \ast KZ_{p_{\xi}} \theta^\alpha x^{\alpha-n} y^{r-np-\alpha}
\]

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

\[
v_p(C_{-1}) = v_p(\vartheta') = t + 1, \quad v_p(E_{\xi}) \geq t + 1 \text{ for } \alpha + 1 \leq \xi < s - \alpha, \quad v_p(F) > t + 1,
\]

and with \(H\) as in lemma [18]. However, \(v_p(E_{s-\alpha}) = t\) and \(v_p(E_{\xi}) \geq t\) 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 \(T(\text{ind}_{KZ}^G \text{quot}(\alpha))\) is trivial modulo \(\mathcal{J}_\alpha\), and if \(t < v_p(a) - \alpha\) then the dominant term is

\[
E_{s-\alpha} \ast KZ_{p_{\xi}} \theta^{s-\alpha} h_{s-\alpha}
\]

and hence \(\tilde{N}_{s-\alpha}\) is trivial modulo \(\mathcal{J}_\alpha\) 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 [Ars], and we apply lemma [18]. This gives an element

\[
\vartheta' \ast KZ_{p_{\xi}} \theta^\alpha x^{p-1} y^{-\alpha(p+1)-p+1} + \sum_{\xi=\alpha+1}^{2\nu-\alpha-1} E_{\xi} \ast KZ_{p_{\xi}} \theta^\alpha x^{\alpha-n} y^{r-np-\alpha} + \sum_{\xi=\alpha+1}^{2\nu-\alpha-1} E_{\xi} \ast KZ_{p_{\xi}} \theta^\alpha x^{\alpha-n} y^{r-np-\alpha}
\]

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

\[
v_p(\vartheta') = 1, \quad v_p(E_{\xi}) \geq 1 \text{ for } \alpha + 1 \leq \xi < s - \alpha, \quad v_p(F) > 1, \quad v_p(E_{s-\alpha}) = v_p((r - \alpha)_{s-\alpha}),
\]

and with \(H\) as in lemma [18]. This time the dominant term is either

\[
\vartheta' \ast KZ_{p_{\xi}} \theta^\alpha x^{p-1} y^{-\alpha(p+1)-p+1}
\]

or

\[
E_{s-\alpha} \ast KZ_{p_{\xi}} \theta^{s-\alpha} h_{s-\alpha}
\]

depending on whether \(\beta \in \{\alpha + 1, \ldots, s - \alpha\}\) or \(\beta > s - \alpha\). Thus in the former case \(\tilde{N}_\alpha\) is trivial modulo \(\mathcal{J}_\alpha\), and in the latter case \(\tilde{N}_{s-\alpha}\) is trivial modulo \(\mathcal{J}_\alpha\).

**Proof of proposition [23]** By proposition [21] we may assume that \(\beta \not\in \{1, \ldots, \alpha + 1\}\), and by proposition [22] we may assume that \(\beta \neq \alpha + 1\). If \(\alpha \neq \frac{7}{2}\) and \(\beta \in \{1, \ldots, s - \alpha\}\) and \(s - \alpha < v_p(a) - t\) then the claim follows from proposition [22]. Thus it is enough to show that if \(\beta \in \{1, \ldots, \alpha\}\) then

\[
\begin{cases}
T(\text{ind}_{KZ}^G \text{quot}(\alpha)) & \text{if } \alpha > v_p(a) - t, \\
\tilde{N}_\alpha & \text{if } \alpha < v_p(a) - t
\end{cases}
\]
is trivial modulo $\mathcal{A}_a$. 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

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

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

- $t \leq v_p(\partial_w(D_{\alpha}))$ for $\alpha \leq w < 2\nu - \alpha$,
- $t < v_p(\partial_w(D_{\alpha}))$ for $0 \leq w < \alpha$,
- $\vartheta' = -C_{-1} + O(\epsilon p)$.

Let us consider the matrix

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

that has integer entries

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

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

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

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

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

where

$$S_{w,j} = \sum_{i=1}^{\beta} \binom{s+\beta}{i(p-1)+j} \binom{i(p-1)}{w} - \binom{s+\beta}{i(p-1)+j} \binom{\beta}{w},$$

$$N_{w,j} = \sum_{v=0}^{\beta} \binom{\beta}{w} \binom{s+\beta}{i(p-1)+j} \binom{s+\beta}{w} \sum_{i=0}^{\beta} \binom{s+\beta}{i(p-1)+j} \binom{s+\beta}{w}.$$

The first condition follows from an argument similar to the one in the fourth bullet point in the proof of theorem 17 in [Ars]: 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 $A \equiv S \mod \epsilon$ and so we can replace $A$ with $S + O(\epsilon)$, and $\vartheta_w(D_{\alpha})$ for each $\alpha \leq w < 2\nu - \alpha$ is a $\mathbb{Z}_p$-linear combination of $\vartheta_0(D_{\alpha}) = O(\epsilon)$, $\ldots$, $\vartheta_{\alpha}(D_{\alpha}) = O(\epsilon)$. And, as in the proof of theorem 17 in [Ars], the second and third conditions follow if

$$S(C_0, \ldots, C_{\alpha})^T = 0,$$

$$N(C_0, \ldots, C_{\alpha})^T = (-C_1 \epsilon^{-1}, 0, \ldots, 0)^T + Sv + O(p)$$

for some $v$.

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

$$(BS)_{i,j} = \binom{s+\beta}{i(p-1)+j}$$
for \( i \in \{1, \ldots, \beta - 1\} \). Let \( \mathbf{R} \) denote the \((\alpha + 1) \times (\alpha + 1)\) matrix over \( \mathbb{F}_p \) obtained from \( \mathbf{BN} \) by replacing the rows indexed 1, \ldots, \beta - 1 with the corresponding rows of \( \mathbf{BS} \). As in the proof of theorem 17 in [Ars], we can compute

\[
(BN)_{i,j} = \sum_{i,v=0}^{\alpha} (-1)^i j^v \left( \binom{i}{v} \right) \binom{(s-\alpha-\beta+j)}{v} \binom{(s-\alpha+j-v)}{j-v}
- \left[ i = 0 \right] \binom{(s-\alpha-\beta+j)}{j} - \left[ i = \beta \right] \binom{(s-\alpha-j)}{j}
- (-1)^i \binom{(s-\alpha-\beta+j)}{s-\alpha} \sum_{i=0}^{\alpha} \left( \binom{i}{\beta} \right) \binom{(s-\alpha+j-i)}{i} \binom{(s-\alpha+j-v)}{j-v}.
\]

Thus lemma [14] implies that

\[
\mathbf{R}(C_0, C_1, \ldots, C_\alpha)^T = \left( \frac{(-1)^{\alpha+1}(s-\alpha)(\alpha-\beta+1)}{\beta^2(2\alpha-s+1)(\alpha)} \right) (\alpha, 0, \ldots, 0)^T.
\]

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 \( \alpha \) such that \( \alpha \geq s \). The major difference in this scenario is that \( \alpha \) 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 \( \alpha+1, \ldots, p-\alpha-1 \). Let us therefore define \( s_\alpha = r - \alpha + \alpha \), 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 [Ars] work out exactly the same if we replace every instance of \( s \) with \( s_\alpha \) (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

\[
\left( \frac{s_\alpha-\alpha}{s_\alpha} \right) \in \mathbb{Z}_p^\times,
\]

which is indeed the case since \( s_\alpha - \alpha = p-1 + s - \alpha \geq 2\nu - \alpha \). So there is an analogous version of theorem 17 in [Ars], and we can conclude the desired result—as the proof of theorem 17 in [Ars] 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 \( s \geq 4 \) and in particular \( \alpha \geq 3 \). We apply part (3) of corollary [19] with \( v \) chosen in the open interval \((\nu_0(\alpha) - \alpha, 0)\) and

\[
C_j = \begin{cases} 
0 & \text{if } j \in \{-1, 0\}, \\
(-1)^j \left( \binom{\alpha-2}{j} \right) + (-1)^{j+1}(\alpha-2)\binom{\alpha-2}{j-1} + pC^*_j & \text{if } j \in \{1, \ldots, \alpha\},
\end{cases}
\]

for some constants \( C^*_1, \ldots, C^*_\alpha \) yet to be chosen. The conditions necessary for the lemma to be applicable are satisfied if \( \tilde{C} = \sum_j C_j \left( \frac{r-\alpha+j}{\alpha+j} \right) \in \mathbb{Z}_p^\times \) and

\[
\vartheta_w(D_\bullet) = O(\epsilon)
\]

for \( 0 \leq w < 2\nu - \alpha \). We have

\[
\tilde{C} = \sum_j C_j \left( \frac{s-\alpha-\beta+j}{s-\alpha-\beta} \right) + O(p)
= -1 + \sum_j \left( (-1)^j \left( \binom{\alpha-2}{j} \right) + (-1)^{j+1}(\alpha-2)\binom{\alpha-2}{j-1} \right) \left( \frac{s-\alpha-\beta+j}{s-\alpha-\beta} \right) + O(p)
= -1 + O(p) \in \mathbb{Z}_p^\times
\]

by \([c-z]\) since \( \alpha - 2 > s - \alpha - \beta \). And, since

\[
j \leq s - \alpha - \beta + j \leq s - \beta < p - i,
\]
we also have
\[
\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} = \binom{\beta}{i} \binom{s-\alpha-\beta+j}{j-i} + O(p).
\]
Thus the equality \( \vartheta_w(D_\bullet) = O(p) \) follows from the fact that
\[
\sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{s-\alpha-\beta+j}{s-\alpha-\beta+i+j} = 0,
\]
which follows from (c-e) since \( \alpha - 2 > \alpha - 2 - \beta + i = s - \alpha - \beta + i \). Moreover, we can choose
\[
C^*_1, \ldots, C^*_\alpha
\]
in a way that \( \vartheta_w(D_\bullet) = 0 \) for \( 0 \leq w < 2\nu - \alpha \) similarly as in the proof of theorem 17 in [Ars] since the reduction modulo \( p \) of the matrix
\[
\begin{pmatrix}
\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} \\
\end{pmatrix}
\]
\[\text{is upper triangular with units on the diagonal. Thus the conditions we need to apply corollary 19 are satisfied and we can conclude that } N_{s/2+1} \text{ is trivial modulo } \mathcal{J}_a. \]

**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 \( s \geq 4 \) and in particular \( \alpha \geq 3 \). The only obstruction in the proof of proposition 22 that prevents us from concluding that \( N_{s/2-1} \) is trivial modulo \( \mathcal{J}_a \) is the dominant terms are
\[
E_\xi \cdot KZ_{\mathfrak{p}} \theta^\xi h_\xi
\]
for \( \frac{s}{2} < \xi \leq 2\nu - \frac{s}{2} \) rather than \( H \). We can see from proposition 25 that
\[
E_{s/2+1} \cdot KZ_{\mathfrak{p}} \theta^{s/2+1} h_{s/2+1} = x_1 + x_2,
\]
with \( v_p(x_1) \geq t + 1 \), and with \( x_2 \in \text{im}(T - a) \). Since the valuation of the coefficient of \( H \) is less than \( t + 1 \), we can remove the obstruction coming from
\[
E_{s/2+1} \cdot KZ_{\mathfrak{p}} \theta^{s/2+1} h_{s/2+1}
\]
by replacing it with \( x_1 \). If \( s = 2\nu - 2 \) then this is the only obstruction and we can conclude that \( N_{s/2-1} \) is trivial modulo \( \mathcal{J}_a \). Now suppose that \( s < 2\nu - 2 \). Then just as in the proof of theorem 17 in [Ars] we can apply part (1) of corollary 19 and conclude that \( N_a \) is trivial modulo \( \mathcal{J}_a \) as long as \( (\epsilon, 0, \ldots, 0)^T \) is in the image of the matrix \( A = (A_{w,j})_{0 \leq w, j \leq \alpha} \) that has integer entries
\[
A_{w,j} = \sum_{i>0} \binom{r-\alpha+j}{i(p-1)+j} \binom{s-1}{w} = S_{w,j} + \epsilon N_{w,j} + O(\epsilon p)
\]
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
\[
1 \cdot KZ_{\mathfrak{p}} \theta^{s/2+1} y^{r-s/2-1}
\]
is equal to
\[
g_1 \cdot KZ_{\mathfrak{p}} \theta^{s/2+1} x^{r/2-2-n+1} y^{r-np-s/2-1} + x_3
\]
for some \( g_1 \) with \( v_p(g_1) \geq v_p(\alpha) - \frac{s}{2} - 1 \) and some \( x_3 \in \text{im}(T - a) \). This in turn by proposition 25 is equal to
\[
g_2 \cdot KZ_{\mathfrak{p}} \theta^{s/2+1} h_2 + x_4
\]
for some \( g_2 \) with \( v_p(g_2) \geq t \), some \( h_2 \), and some \( x_4 \in \text{im}(T-a) \). 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

\[
g_2 \cdot KZ_{\mathbb{Q}_p} \cdot \theta^{s/2+1} x^{s/2-n+1} y^{r-np-s/2-1} + x_5 + O(\epsilon)
\]

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

\[
C_1 a p^{-s/2} g_4 \cdot KZ_{\mathbb{Q}_p} \cdot \theta^{s/2} x^{s/2-n} y^{r-np-s/2} + O(\epsilon)
\]

rather than \( O(\epsilon) \)—a description of this error term is given in part (2) of lemma 13. This implies that we can add a constant multiple of

\[
1 \cdot KZ_{\mathbb{Q}_p} \cdot x^{s/2+1} y^{r-s/2-1}
\]

to the element

\[
\sum_i D_i \cdot KZ_{\mathbb{Q}_p} \cdot x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} + O(ap^{-\alpha})
\]

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

\[
\left( (\frac{r-\alpha}{s-\alpha}), \ldots, (\frac{t}{s}) \right)^T
\]

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 [Ar5] 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 \((BN)_{i,j}\) in proposition 25 we can find that

\[
\overline{R}_{0,0} = \sum_{i=0}^{\alpha} (l-\beta-1) \partial = \Phi'(-\beta - 1)
\]

with

\[
\Phi(z) = \sum_{i=0}^{\alpha} \left( \frac{z+i}{l} \right) = \left( \frac{z+\alpha+1}{l} \right).
\]

Thus

\[
\overline{R}_{0,0} = \left( \frac{\alpha-\beta}{l} \right)^\partial = \frac{(-1)^{\beta+1}}{\beta(\beta)} \neq 0,
\]

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 \( \tilde{N}_{s/2^{-1}} \) is trivial modulo \( \mathcal{F}_a \).

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

\[
H = b_H \cdot KZ_{\mathbb{Q}_p} \cdot x^{\alpha-n} y^{r-np-\alpha} + O(p^{\alpha+1})
\]

for the constant

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

\[
\left( \begin{array}{c}
(\alpha+1)^{(p-1)\alpha+j} \\
(\alpha+1)^{(p-1)\alpha+j}
\end{array} \right)_{0 \leq i < \beta, 0 \leq j \leq \alpha} (C_1, \ldots, C_\alpha)^T = (p, 0, \ldots, 0)^T.
\]

Therefore it is enough to show that the square matrix

\[
A_0 = \left( \begin{array}{c}
\alpha+1 \end{array} \right)_{0 \leq i < \beta, 0 \leq j \leq \alpha}
\]

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

\[
\left\{ \begin{array}{l}
C_1 = 0 \text{ and } (C_2, \ldots, C_\alpha)^T = A_0^{-1}(1, 0, \ldots, 0)^T \text{ if } \beta = \alpha - 1, \\
(C_1/p, \ldots, C_\alpha)^T = A_0^{-1}(1, 0, \ldots, 0)^T \text{ if } \beta = \alpha.
\end{array} \right.
\]

This follows from lemma \([13]\). So the conditions we need to apply corollary \([19]\) are satisfied and we can conclude that \( \tilde{N}_{s/2+1} \) is trivial modulo \( \mathcal{F}_a \). \( \blacksquare \)

**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 \( \tilde{C} = O(p) \) and the dominant term is no longer \( H \). Let us slightly tweak these constants and instead use

\[
C_j = \left\{ \begin{array}{l}
(\alpha+1)^{\alpha+1} \text{ if } j = -1, \\
(\alpha+1)^{\alpha+1} \text{ if } j \in \{0, \ldots, \alpha\}.
\end{array} \right.
\]

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

\[
(\vartheta^p + C_{-1}) = K Z \vartheta^{\alpha+1} y^r - \alpha + (p-1)^{p+1} + C_{-1} = K Z \vartheta^{\alpha+1} y^r - \alpha + n - p - \alpha
\]

(and therefore that \( \text{ind}_{K Z} G \text{sub}(\frac{s}{2} + 1) \) is trivial modulo \( \mathcal{F}_a \)) as long as

\[
\overline{R}(C_0, \ldots, C_\alpha)^T = (0, \ldots, 0, 1)^T.
\]

This follows from lemma \([12]\). Thus the conditions we need to apply corollary \([19]\) are satisfied and we can conclude that \( \text{ind}_{K Z} G \text{sub}(\frac{s}{2} + 1) \) is trivial modulo \( \mathcal{F}_a \). \( \blacksquare \)

**References**

[Ber10] Laurent Berger, *Représentations modulaires de 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 GL_2(\mathbb{Q}_p)*, I, Compositio Mathematica 138 (2003), no. 2, 165–188.

[Bre03b] , *Sur quelques représentations modulaires et p-adiques de 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] Abhijit Ganguli and Eknath Ghate, *Reductions of Galois representations via the mod p local Langlands correspondence*, Journal of Number Theory 147 (2015), 250–286.