On the locally reducible part of the eigencurve

a thesis presented for the degree of

Doctor of Philosophy of Imperial College London

and the

Diploma of Imperial College

by

Bodan Arsovski

Department of Mathematics

Imperial College

180 Queen's Gate, London SW7 2BZ

January 2019

I certify that this thesis, and the research to which it refers, are the product of my own work, and that any ideas or quotations from the work of other people, published or otherwise, are fully acknowledged in accordance with the standard referencing practices of the discipline.

Signed: _____

Copyright

Abstract

This thesis studies crystalline Galois representations, which are certain constructions in p-adic Hodge theory whose most interesting property is that they arise as representations associated with modular forms. The main theorems proved in this thesis are partial results towards a conjecture about crystalline representations which dates back to computational observations by Buzzard and Gouvêa. Among the curiosities they noticed when computing the p-adic slopes of modular forms (i.e. the p-adic valuations of their pth coefficients) was that, for a certain class of so-called $\Gamma_0(N)$-regular primes when the level N is coprime to p, the p-adic slopes of eigenforms of level $\Gamma_0(N)$ are always integers. Since, at least when $p > 2$, the reductions modulo p of the Galois representations associated with such modular forms are always reducible, this eventually pointed to a more general conjecture that the "locally reducible" eigenforms—i.e. those eigenforms of level coprime to p which have associated Galois representations whose reductions modulo p are reducible—always have integer slopes. In fact, while all representations associated with the aforementioned modular forms are crystalline, the class of all crystalline representations is larger and constructed entirely locally via p-adic Hodge theory (and therefore does not need any of the global structure coming from the world of modular forms). Thus the main conjecture tackled in this thesis is an entirely local statement saying that the slopes of locally reducible crystalline representations of even weight are always integers. The main result we prove in this thesis is that this conjecture is true when the slope is less than $\frac{p-1}{2}$. We additionally classify the reductions modulo p for a large class of crystalline representations.

Acknowledgments

I would first and foremost like to thank my advisors, Kevin Buzzard and Ana Caraiani, for suggesting the topic of this thesis, for numerous discussions on the topic, and for excellent guidance and support in general. I would like to thank the Department of Mathematics at Imperial College London; this work was supported by its President's PhD Scholarship.

Contents

1

Introduction and statements of the main results

1.1 Background and motivation behind the main conjecture

Throughout this thesis we assume that p is an odd prime number. Many of the computations crucially make the assumption that $p \neq 2$, and in fact the main conjecture is not true for $p = 2$. The main objects of study are two-dimensional crystalline representations of the absolute Galois group of $\mathbb{Q}_p$, which are representations that are up to a twist parametrized by an integer $k \geqslant 2$ and an element $a \in \overline{\mathbb{Z}}_p$ such that $v_p(a) > 0$. We denote by $V_{k,a}$ the crystalline representation corresponding to the parameters (k, a), so that all crystalline representations are of the form $V_{k,a} \otimes \eta$ for some character η of $G_{\mathbb{Q}_p}$ that is the product of an unramified character and a power of the cyclotomic character. The construction of $V_{k,a}$ is outlined in section 2.1. The core property of crystalline representations is that the representation associated with a non-ordinary finite slope classical eigenform

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

of weight $k \geqslant 2$, level $\Gamma_0(N)$ such that $(N, p) = 1$, and character χ, is crystalline and equal to $V_{k,a_p\sqrt{\chi}(p)} \otimes \sqrt{\chi}$, where $\sqrt{\chi}$ is an unramified character of $G_{\mathbb{Q}_p}$ whose square is χ. By the "slope" of f we mean the p-adic valuation of the eigenvalue of the Hecke operator T_p which corresponds to the eigenvector f. By the "slope" of an eigenform of level $\Gamma_0(Np)$ we mean the p-adic valuation of the corresponding eigenvalue of the Atkin–Lehner operator U_p. Each newform of level $\Gamma_0(N)$ maps onto a pair of oldforms f_1, f_2 of level $\Gamma_0(Np)$ via the maps defined on q-expansions that send $q \mapsto q$ and $q \mapsto q^p$. If the slope of f is α, then the slopes of f_1, f_2 are α and $k - 1 - \alpha$; moreover, every newform of level $\Gamma_0(Np)$ has slope $\frac{k-2}{2}$ (see section 1 of [Gou01]). Thus finding the slopes of newforms of level $\Gamma_0(N)$ is equivalent to finding the slopes of eigenforms of level $\Gamma_0(Np)$.

The motivation behind the main conjecture tackled in this thesis comes from computational observations made by Buzzard and Gouvêa in [Buz05] and [Gou01] about a certain class of primes which Buzzard subsequently termed "$\Gamma_0(N)$-regular". These computational observations were about the slopes of newforms of level $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$, and consisted of the following:

1. In most cases, the slopes were at most $\frac{k-1}{p+1}$. The exceptions occurred for $p = 59, 79, 2411, 3371, \ldots$

2. In almost all cases, the slopes were integers. The exceptions occurred for $p = 59, 79$.

Subsequently, Buzzard introduced the notion of "$\Gamma_0(N)$-regularity": a prime $p > 2$ is called $\Gamma_0(N)$-regular if and only if any eigenform of level $\Gamma_0(N)$ and weight in $\{2, \ldots, \frac{p+3}{2}\}$ has slope equal to zero. There is an algorithm which can be used to verify whether a prime is $\Gamma_0(N)$-regular. The list of $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$-regular primes begins with $59, 79, 107, 131, 139, 151, 173, \ldots$, so one might ask if all exceptions to the above two observations happen only when the prime is regular.

The main connection between this and the theory of Galois representations is that a prime $p > 2$ is $\Gamma_0(N)$-regular if and only if, for all weights $k \geqslant 2$ and all $f \in S_k(\Gamma_0(N))$, the mod p representation associated with f is reducible

(see [Buz05] and [BG16]). This naturally leads to the more general conjecture that all exceptions to the above two observations happen only when the associated mod p representation is reducible.

In this thesis we only concern ourselves with the second observation, and the main conjecture we consider is the following one, which was made by Breuil, Buzzard, and Emerton (see conjecture 4.1.1 in [BG16]):

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

Here $\overline{V}_{k,a}$ is a mod p representation, and it defined 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 $V_{k,a}$. Since the weights of non-trivial modular forms of level $\Gamma_0(N)$ are even, and since the representation associated with a level $\Gamma_0(N)$ eigenform is crystalline as we have mentioned, this conjecture, if true, would imply that indeed all exceptions to the second observation above happen when the associated mod p representation is reducible.

1.2 Prior results

The question of computing $\overline{V}_{k,a}$ has been studied extensively:

- $\overline{V}_{k,a}$ has been computed when $k \leqslant 2p+1$ by the work of Berger and Breuil, in [Ber10], [Bre03a], and [Bre03b].
- $\overline{V}_{k,a}$ has been computed when the slope $v_p(a)$ is greater than $\lfloor \frac{k-2}{p-1} \rfloor$ by the work of Berger, Li, and Zhu, in [BLZ04].
- Outside of a small region where the slope is $\frac{3}{2}$, $\overline{V}_{k,a}$ has been computed when $v_p(a) < 2$, by the work of Buzzard, Gee, Ganguli, Ghate, Bhattacharya, and Rozensztajn in [BG15], [BGR18], [BG09], [BG13], and [GG15].
- Algorithms have been developed that allow one to compute $\overline{V}_{k,a}$ for given p, k, a, and to find the locus of all a such that $\overline{V}_{k,a} = \overline{\rho}$ for given p, k, and a mod p representation $\overline{\rho}$, by the work of Rozensztajn in [Roz18] and [Roz].

1.3 New results

There are three main results in this thesis: theorems 1, 2, and 3. The first two theorems compute $\overline{V}_{k,a}$ in about half of all cases when the slope is less than $\frac{p-1}{2}$. The third theorem builds on the first two theorems and proves that conjecture A is true when the slope is less than $\frac{p-1}{2}$.

The statements of theorems 1 and 2 are somewhat complicated: for example, if the valuation of a is a positive integer $\nu - 1 \in \mathbb{Z}_{>0}$, then there are about $\frac{1}{2}\nu^2 p$ different possibilities for what $\overline{V}_{k,a}$ can be depending on the congruence class of k modulo p^ν. Perhaps the most natural way to state these theorems is to fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}_p$ and to look at the space of continuous homomorphisms $\mathscr{W} = \hom_{cts}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$. We have $\mathbb{Z}_p^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z}) \times \mathbb{Z}_p$, and $\hom_{cts}(\mathbb{Z}_p, \mathbb{C}_p^\times)$ is isomorphic to the open disk in $\mathbb{C}_p$ with center 0 and radius 1, via the identification $\chi \leftrightarrow \chi(1) - 1$. Thus $\mathscr{W}$ is the disjoint union of $p-1$ open disks of radii 1. We identify the weight $k \geqslant 2$ with the continuous homomorphism $x \mapsto x^{k-2}$, so that $k \geqslant 2$ is a point on the disk indexed by $k - 2 \bmod p - 1$. We say a point of $\mathscr{W}$ is "integral" if it is associated with a weight in this fashion.

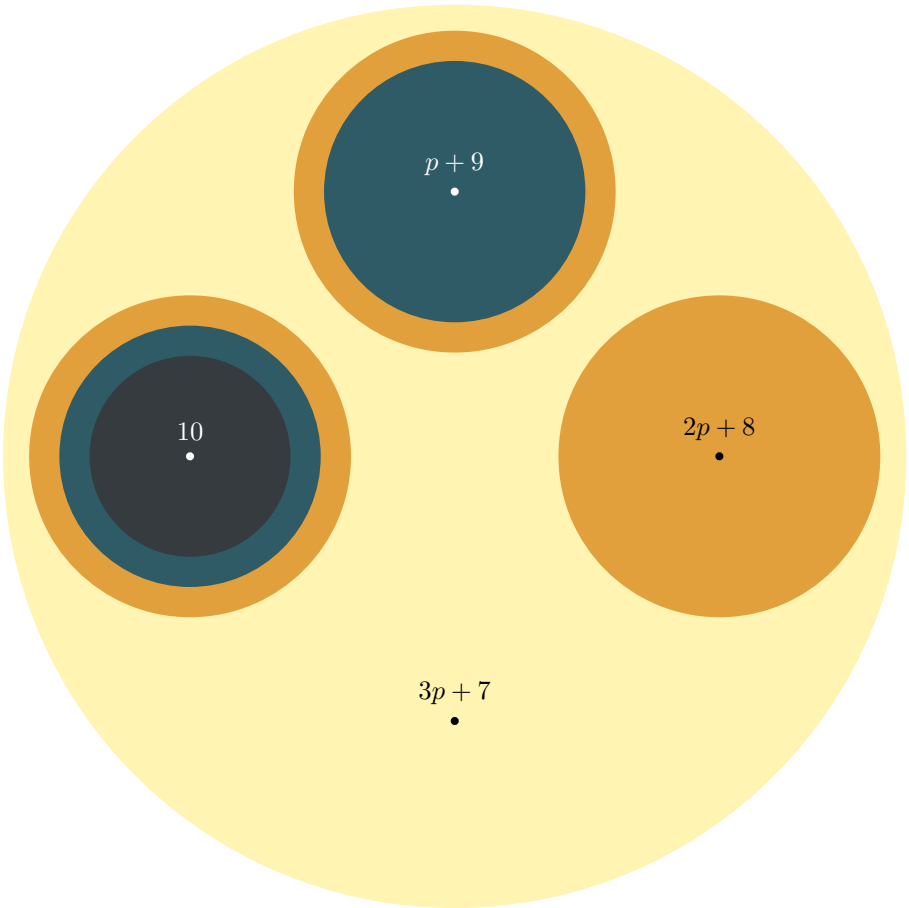
The most general result about $\overline{V}_{k,a}$ to date is the main theorem in [BLZ04] which says that

$$\overline{V}_{k,a} \cong \overline{V}_{k,0} \cong \begin{cases} \operatorname{ind}(\omega_2^{k-1}) & \text{if } p+1 \nmid k-1, \\ (\mu_{\sqrt{-1}} \oplus \mu_{-\sqrt{-1}}) \otimes \omega^{\frac{k-1}{p+1}} & \text{if } p+1 \mid k-1, \end{cases}$$

whenever $v_p(a) > \lfloor \frac{k-2}{p-1} \rfloor$. This theorem tells us what $\overline{V}_{k,a}$ is at a discrete set of points in the aforementioned $p-1$ disks. It is expected that the bound $\lfloor \frac{k-2}{p-1} \rfloor$ is not optimal: there is a prediction in subsection 2.1 of [BG16] that the bound can be replaced with $\frac{k-1}{p+1}$, and this prediction is motivated by the first of the two observations in section 1.1. However, there seems to be an inherent increase in difficulty in finding $\overline{V}_{k,a}$ at these extra points.

The theorems we prove indicate that these points play a fundamental role: it seems that the $p-1$ open disks can be split into regions by concentric circles centered at these points in a way that $\overline{V}_{k,a}$ depends on the region

k belongs to. For example, the following diagram illustrates how the disk containing the weight 10 is split into regions when $p \geqslant 11$ and $3 < v_p(a) < 4$. There are four centers of the bundles of concentric circles, and they are exactly the points k belonging to the disk (i.e. such that $k \equiv 10 \bmod p-1$) and such that $v_p(a) > \lfloor \frac{k-2}{p-1} \rfloor$ (i.e. $\lfloor \frac{k-2}{p-1} \rfloor < 4$). In fact, they are the same as the points satisfying $\frac{k-1}{p+1} < 4$. By [BLZ04], at these four points we have $\overline{V}_{k,a} \cong \mathrm{ind}(\omega_2^{k-1})$. The diagram illustrates closed disks around the points, of radii p^{-1}, p^{-2}, and p^{-3}. As we show in theorem 1, in this situation $\overline{V}_{k,a}$ is always one of these four representations, depending on the color of the region that k belongs to, as illustrated.



Theorems 1 and 2 prove a general version of this, in the case when the corresponding disk is what we label "non-subtle": this label depends on the slope $v_p(a)$ and roughly means that the bound $\lfloor \frac{k-2}{p-1} \rfloor$ is optimal for any k belonging to that disk, i.e. that there are no additional points k on that disk satisfying the improved bound $v_p(a) > \frac{k-1}{p+1}$ but not $v_p(a) > \lfloor \frac{k-2}{p-1} \rfloor$ at which the associated representation is distinct from the "typical" one, which in the context of the diagram on the previous page means the representation corresponding to the yellow region.

Theorem 3 is simpler to state because it is not a complete classification like theorems 1 and 2 are—in proving it we show just enough to conclude that $\overline{V}_{k,a}$ is irreducible when $k \in 2\mathbb{Z}$ and $v_p(a) \notin \mathbb{Z}$ and $v_p(a) < \frac{p-1}{2}$.

1.4 Statements of the main results

Recall that we assume that $p > 2$ is an odd prime number. Let $k \geqslant 2$ be an integer, and let a be an element of $\overline{\mathbb{Z}}_p$ such that $v_p(a) > 0$. With this data we associate a mod p representation $\overline{V}_{k,a}$—the full details are given in section 2.1. Let us write $\overline{h}$ for the number in $\{1, \ldots, p-1\}$ which is congruent to h mod $p-1$. Let $\nu = \lfloor v_p(a) \rfloor + 1 \in \mathbb{Z}_{>0}$, and let s be the number in $\{1, \ldots, p-1\}$ which is congruent to $k-2$ mod $p-1$. Let us say that k is "subtle" if $s \in \{1, \ldots, 2\nu - 1\}$, and k is "non-subtle" if $s \notin \{1, \ldots, 2\nu - 1\}$. An open disk of $\mathscr{W}$ consists either entirely of "subtle" points or entirely of "non-subtle" points, so we can also refer to the $p-1$ open disks of $\mathscr{W}$ as either "subtle" or "non-subtle". In particular, the $\min\{p-1, 2\nu-1\}$ disks containing $3, \ldots, 2\nu+1$ are "subtle", and all other disks are "non-subtle". Note that whether a weight is "subtle" or not depends on the value of ν.

Let $\mathscr{D}_s$ denote the open disk of radius 1 around $s + 2 \in \mathscr{W}$, and let us consider the set

$$B_{s,\nu} = \{s + \beta(p-1) + 2 \,|\, \beta \in \{0, \ldots, \nu - 2\}\}.$$

In particular, if $\nu = 1$ then $B_{s,\nu} = \varnothing$, and in general $B_{s,\nu}$ is a set of $\nu - 1$ points in $\mathscr{D}_s$. Let

$$b_0 < \cdots < b_{\nu-2}$$

be the elements of $B_{s,\nu}$ in increasing order. Therefore if $i \in \{0, \dots, \nu-2\}$ then $b_i = s + i(p-1) + 2$ and, by the main result of [BLZ04],

$$\overline{V}_{b_i,a} \cong \mathrm{ind}(\omega_2^{b_i-1}).$$

Let us also define $b_{\nu-1} = s + (\nu-1)(p-1) + 2$. For $i \in \{0, \dots, \nu-2\}$ and $j \in \mathbb{Z}_{>0}$, let

$$\mathscr{R}_{i,j}^{s,\nu} = \{t \in \mathscr{D}_s \,|\, j \leqslant v_p(t - b_i) < j+1\}$$

be the half-open annulus which is the complement of the closed disk of radius p^{-j-1} around b_i in the closed disk of radius p^{-j} around b_i. The integral points in $\mathscr{R}_{i,j}^{s,\nu}$ are the points on the circle of radius p^{-j} around $b_i = s + i(p-1) + 2$. Finally, let

$$\mathscr{R}_0^{s,\nu} = \mathscr{D}_s \setminus \cup_{i \in \{0,\dots,\nu-2\},\, j>0} \mathscr{R}_{i,j}^{s,\nu},$$

so that $\mathscr{D}_s$ is partitioned into the disjoint sets

$$\{\mathscr{R}_0^{s,\nu}\} \cup \{\mathscr{R}_{i,j}^{s,\nu} \,|\, i \in \{0, \dots, \nu-2\},\, j \in \mathbb{Z}_{>0}\}. \qquad (\mathscr{R}^{s,\nu})$$

Note that the definition of this partition depends on both s and ν. For $l \in \mathbb{Z}$ and $\lambda \in \overline{\mathbb{F}}_p^\times$ let us define

$$\mathrm{Irr}(l) = \mathrm{ind}(\omega_2^{l-1}) \text{ and } \mathrm{Red}_{s,\nu}(l,\lambda) = \mu_\lambda \omega^{s+l-\nu+2} \oplus \mu_{\lambda^{-1}} \omega^{\nu-l-1}.$$

The first result is a complete classification of $\overline{V}_{k,a}$ over the "non-subtle" components of weight space for $v_p(a) \notin \mathbb{Z}$.

Theorem 1. *Recall that $k \geqslant 2$ is an integer and that s is defined as the integer in $\{1, \dots, p-1\}$ which is congruent to $k-2 \bmod p-1$. Suppose that k is "non-subtle", i.e.*

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

Suppose also that the open disk $\mathscr{D}_s$ of radius 1 around $s+2 \in \mathscr{W}$ is partitioned

into disjoint sets as in $(\mathscr{R}^{s,\nu})$. *If* $v_p(a) \notin \mathbb{Z}$ *then*

$$\overline{V}_{k,a} \cong \begin{cases} \mathrm{Irr}(b_{\nu-1}) & \text{if } k \in \mathscr{R}_0^{s,\nu}, \\ \mathrm{Irr}(b_{\max\{i,\nu-j-1\}}) & \text{if } k \in \mathscr{R}_{i,j}^{s,\nu}. \end{cases}$$

This result is known for $\nu = 1$ by the work of Buzzard and Gee in [BG09] and for $\nu = 2$ by the work of Bhattacharya and Ghate in [BG15].

We also prove a similar theorem for $v_p(a) \in \mathbb{Z}$. The precise statement of this is the following theorem, which is a complete classification of $\overline{V}_{k,a}$ over the "non-subtle" components of weight space for $v_p(a) \in \mathbb{Z}$.

Theorem 2. *Recall that* $k \geqslant 2$ *is an integer and that* s *is defined as the integer in* $\{1, \ldots, p-1\}$ *which is congruent to* $k - 2 \bmod p - 1$. *Suppose that* k *is "non-subtle", i.e.*

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

Suppose also that the open disk $\mathscr{D}_s$ *of radius 1 around* $s + 2 \in \mathscr{W}$ *is partitioned into disjoint sets as in* $(\mathscr{R}^{s,\nu})$. *If* $v_p(a) = \nu - 1 \in \mathbb{Z}_{>0}$ *then*

$$\overline{V}_{k,a} \cong \begin{cases} \mathrm{Red}_{s,\nu}(0, \lambda_{k,\nu}) & \text{if } k \in \mathscr{R}_0^{s,\nu}, \\ \mathrm{Red}_{s,\nu}(j, \lambda_{k,\nu,i,j}) & \text{if } k \in \mathscr{R}_{i,j}^{s,\nu} \text{ and } i + j < \nu - 1, \\ \mathrm{Irr}(b_i) & \text{if } k \in \mathscr{R}_{i,j}^{s,\nu} \text{ and } i + j \geqslant \nu - 1, \end{cases}$$

where

$$\lambda_{k,\nu} = \tfrac{\binom{s-\nu+2}{\nu-1} a}{\binom{s-k+2}{\nu-1} p^{\nu-1}} \in \overline{\mathbb{F}}_p^{\times},$$
$$\lambda_{k,\nu,i,j} = \tfrac{(-1)^{\nu+i+j+1}(\nu-j-1)\binom{\nu-j-2}{i}\binom{s-\nu+j+2}{\nu-j-1} a}{(k-s-i(p-1)-2)p^{\nu-j-1}} \in \overline{\mathbb{F}}_p^{\times}.$$

Note that $\lambda_{k,\nu,i,j}$ is indeed a unit (and therefore we can think of it as an element of $\overline{\mathbb{F}}_p^{\times}$) since the integral points in $\mathscr{R}_{i,j}^{s,\nu}$ consist precisely of those points on the circle of radius p^{-j} around $b_i = s + i(p-1) + 2$ and so

$$v_p((k - s - i(p-1) - 2)p^{\nu-j-1}) = \nu - 1.$$

This result is known for $\nu = 2$ by the work of Bhattacharya, Ghate, and Rozensztajn in [BGR18].

Building on theorems 1 and 2, we also prove the following theorem.

Theorem 3. *Conjecture A is true when the slope is less than* $\frac{p-1}{2}$.

This is relatively more difficult and the ad hoc nature of the proof involving many case studies means that we cannot (yet) deduce a full classification as in theorems 1 and 2.

The proofs are based on the method (developed by Breuil, Buzzard, and Gee) of using the local Langlands correspondence and its compatibility with reduction modulo p to compute the representations of $G_{\mathbb{Q}_p}$ by computing certain corresponding representations of $\mathrm{GL}_2(\mathbb{Q}_p)$. We give further outlines of the proofs in chapters 2, 5, 6, and 7.

Finally, we note that there is nothing to prevent the method from working when $\nu > \frac{p-1}{2}$ other than the complexity of the computations, and we believe that it is possible to write a computer program which takes as input a positive integer m and verifies conjecture A for slopes up to m by verifying it for the primes that are less than $2m$.

1.5 Verifying theorems 1 and 2 by a computer

The paper [Roz18] gives an algorithm which takes as input a prime p, a weight k, an eigenvalue a, and a parameter called "radius" which determines the precision of the computations, and if the radius is large enough it computes $\overline{V}_{k,a}$.[1] An implementation of the algorithm in `SageMath` is available at

`http://perso.ens-lyon.fr/sandra.rozensztajn/software/index.html`

As theorems 1 and 2 give complete classifications of $\overline{V}_{k,a}$, one can use this algorithm to verify them for any given triple (p, k, a). The complexity of the

[1] The algorithm actually computes the $\mathrm{GL}_2(\mathbb{Q}_p)$-representation associated with $\overline{V}_{k,a}$ via the bijective correspondence given in theorem 4 in section 2.2, and one can use theorem 4 to then compute $\overline{V}_{k,a}$.

algorithm depends on the size of the extension field generated by a, so in practice it is much faster to verify theorem 2. Additionally, the statement of theorem 2 is more complicated, especially the formulas for $\lambda_{k,\nu}, \lambda_{k,\nu,i,j}$, so it is better suited for this type of computer verification. We have verified theorem 2 for the triples in the following table.

p	k	a	"radius"	$\overline{V}_{k,a}$
7	8	49	3	$\mathrm{ind}(\omega_2^7)$
7	14	49	3	$\mathrm{ind}(\omega_2^{13})$
7	20	49	4	$\mu_3\omega^5 \oplus \mu_5\omega^2$
7	26	49	3	$\mu_1\omega^5 \oplus \mu_1\omega^2$
7	32	49	3	$\mu_4\omega^5 \oplus \mu_2\omega^2$
7	38	49	3	$\mu_1\omega^5 \oplus \mu_1\omega^2$
7	44	49	3	$\mu_3\omega^5 \oplus \mu_5\omega^2$
7	50	49	3	$\mu_6\omega \oplus \mu_6$
7	56	49	3	$\mathrm{ind}(\omega_2^{13})$
11	38	121	3	$\mu_7\omega^5 \oplus \mu_8\omega^2$
11	39	121	3	$\mu_5\omega^6 \oplus \mu_9\omega^2$
11	40	121	3	$\mu_7\omega^7 \oplus \mu_8\omega^2$
11	41	121	3	$\mu_2\omega^8 \oplus \mu_6\omega^2$
11	42	121	3	$\mu_1\omega^9 \oplus \mu_1\omega^2$

2

Assumptions and definitions

This chapter introduces all of the objects studied in this thesis. In section 2.1 we refer to a definition of the crystalline Galois representations $V_{k,a}$ and their reductions $\overline{V}_{k,a}$. In section 2.2 we state a bijective correspondence between these reductions and certain $\mathrm{GL}_2(\mathbb{Q}_p)$-representations $\overline{\Theta}_{k,a}$. The main results in this thesis are about computing $\overline{V}_{k,a}$, and the main recipe to do so is by computing the bijectively associated $\overline{\Theta}_{k,a}$. In section 2.3 we use the bijective correspondence between $\overline{V}_{k,a}$ and $\overline{\Theta}_{k,a}$ to rephrase theorems 1, 2, and 3 into the equivalent theorems 5, 6, and 7. Thus our task for the remainder of this thesis becomes proving the latter three theorems, and we do that in chapters 5, 6, and 7. In sections 2.4 and 2.5 we introduce some notation and all of the assumptions we make throughout this thesis, most notably that $k > p^{100}$. In section 2.6 we introduce some combinatorial definitions. Finally, in section 2.7 we collate all of the new assumptions, definitions, and notation in a convenient table.

2.1 Crystalline representations

Recall that we assume that $k \geqslant 2$ is an integer and $a \in \overline{\mathbb{Z}}_p$ is such that $v_p(a) > 0$. The representation $V_{k,a}$ is defined in subsection 3.1 of [Bre03b] as the representation of $G_{\mathbb{Q}_p}$ that is crystalline on $\mathbb{Q}_p$ and such that

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

for the weakly admissible filtered φ-module

$$D_{k,a} = \overline{\mathbb{Q}}_p e_1 \oplus \overline{\mathbb{Q}}_p e_2$$

which has Hodge–Tate weights $(0, k-1)$, a filtration

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

and a Frobenius map φ such that

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

All crystalline representations are of the form $V_{k,a} \otimes \eta$ (see proposition 3.1 in [Bre03b]). We define $\overline{V}_{k,a}$ to be 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 $V_{k,a}$.

Let us denote $\nu = \lfloor v_p(a) \rfloor + 1 \in \mathbb{Z}_{>0}$. Since the theorems we prove in this thesis are vacuous for $\frac{p-1}{2} \leqslant v_p(a)$, we assume that $\nu \in \{1, \ldots, \frac{p-1}{2}\}$. And, since $\overline{V}_{k,a}$ has been described completely for $k \leqslant 2p+1$, we also assume that

$$a^2 \neq 4p^{k-1} \text{ and } a \neq \pm(1 + p^{-1})p^{k/2}.$$

2.2 The p-adic and mod p local Langlands correspondences

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

$$\mathrm{ind}_H^G W := \{\text{l.a. maps } G \to W \mid f(hg) = hf(g) \ \&\ \mathrm{supp}\, f \text{ is compact in } H\backslash G\}.$$

Let B be the Borel subgroup of G consisting of those elements that are upper triangular, let $K = \mathrm{GL}_2(\mathbb{Z}_p) \subset G$, and let Z be the center of G. Let $\mathbb{F} \in \{\overline{\mathbb{Q}}_p, \overline{\mathbb{F}}_p\}$. For an open subgroup H of G, a locally algebraic finite-dimensional representation W of H, and elements $g \in G$ and $w \in W$, let $g \bullet_{H,\mathbb{F}} w$ be the unique element of $\mathrm{ind}_H^G W$ that is supported on Hg^{-1} and maps g^{-1} to w. Since $H\backslash G$ is discrete, every element of $\mathrm{ind}_H^G W$ can be written as a finite linear combination of functions of the type $g \bullet_{H,\mathbb{F}} w$. It is easy to check that

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

For $\xi \in \mathbb{F}$, let $\xi \bullet_{H,\mathbb{F}} w$ denote $\xi(\mathrm{id} \bullet_{H,\mathbb{F}} w)$. Let μ_x be the unramified character of the Weil group that sends the geometric Frobenius to x. Write λ for one of the roots of $X^2 - aX + p^{k-1}$, so that the other root is $\lambda^{-1}p^{k-1}$. Let $\rho : B \to \overline{\mathbb{Q}}_p^\times$ be the character defined by

$$B \ni \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \mapsto \mu_{\lambda p^{1-k}}(x)\mu_{\lambda^{-1}}(z)|x/z|^{1/2}.$$

We can view $\mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2)$ as the G-module of homogeneous polynomials in x and y of total degree $k-2$ with coefficients in $\overline{\mathbb{Q}}_p$, with G acting by

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

for $\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in G$ and $v(x,y) \in \mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2)$. Similarly, if $R \in \{\overline{\mathbb{Z}}_p, \overline{\mathbb{F}}_p\}$, we can view $\mathrm{Sym}^{k-2}(R^2)$ as the KZ-module of homogeneous polynomials in x and y of total degree $k-2$ with coefficients in R, with KZ acting by

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

for $\left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in KZ$ and $v(x,y) \in \mathrm{Sym}^{k-2}(R^2)$. Let

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

In particular, $\left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$ acts on $\mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2)$ as multiplication by p^{k-2} and it acts on $\widetilde{\Sigma}_{k-2}$ trivially. Let Σ_{k-2} be the reduction of $\mathrm{Sym}^{k-2}(\overline{\mathbb{Z}}_p^2) \otimes |\det|^{\frac{k-2}{2}}$ modulo $\mathfrak{m}$. Let us consider the $\overline{\mathbb{Q}}_p$-representation

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

Here the Borel subgroup B is seen as a parabolic subgroup of G and ind_B^G denotes parabolic induction (as opposed to the compact induction we defined above). Let us fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Then π corresponds to a principal series representation which is the admissible representation of G associated with $V_{k,a}$ via the classical local Langlands correspondence. In section 3.2 of [Bre03b], Breuil defines the $\mathrm{GL}_2(\mathbb{Q}_p)$-representation

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

where $T \in \mathrm{End}_G(\mathrm{ind}_{KZ}^G \widetilde{\Sigma}_{k-2})$ is the Hecke operator corresponding to the double coset of $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and proves that

$$\Pi_{k,a} \cong \mathrm{Sym}^{k-2}(\overline{\mathbb{Q}}_p^2) \otimes |\det|^{-\frac{1}{2}} \otimes \pi. \tag{2.1}$$

Here π is the parabolic representation we defined above. He also defines

$$\Theta_{k,a} = \mathrm{im}\left(\mathrm{ind}_{KZ}^G(\mathrm{Sym}^{k-2}(\overline{\mathbb{Z}}_p^2) \otimes |\det|^{\frac{k-2}{2}}) \longrightarrow \Pi_{k,a}\right),$$

and $\overline{\Theta}_{k,a} = \Theta_{k,a} \otimes \overline{\mathbb{F}}_p$. In section 2.1 of [Bre03b], Breuil proves the explicit formula

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

where $[\xi]$ is the Teichmüller lift of $\xi \in \mathbb{F}_p$ to $\mathbb{Z}_p$. Let us write $\sigma_t = \mathrm{Sym}^t(\overline{\mathbb{F}}_p^2)$. For $t \in \{0, \dots, p-1\}$, $\lambda \in \overline{\mathbb{F}}_p$, and a character $\psi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$, let $\pi(t, \lambda, \psi)$ denote the representation

$$\pi(t, \lambda, \psi) = (\mathrm{ind}_{KZ}^G \sigma_t/(T - \lambda)) \otimes \psi,$$

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

In [Ber10], Berger proves the following correspondence between $\overline{V}_{k,a}$ and $\overline{\Theta}_{k,a}$, which was conjectured by Breuil (conjecture 3.3.5 in [Bre03b]).[1]

Theorem 4. *There are $t \in \{0, \dots, p-1\}$ and $\psi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$ such that either*

$$\overline{\Theta}_{k,a} \cong \left(\mathrm{ind}_{KZ}^G \sigma_t/T\right) \otimes \psi$$

or

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

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

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

and in the latter case we have

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

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

Moreover, since $\overline{\Theta}_{k,a}$ has finite length as a $\overline{\mathbb{F}}_p[G]$-module, we have $\overline{\Theta}_{k,a}^{\mathrm{ss}} \cong \overline{\Pi}_{k,a}^{\mathrm{ss}}$ by lemma 3.3.4 in [Bre03b], so we may replace $\Theta_{k,a}$ with $\Pi_{k,a}$ in theorem 4. Theorem 4 is the mod p local Langlands correspondence, which associates with $\overline{V}_{k,a}$ a $\mathrm{GL}_2(\mathbb{Q}_p)$-representation over $\overline{\mathbb{F}}_p$, and equation 2.1 implies that it is compatible with the p-adic local Langlands correspondence, which associates with $V_{k,a}$ a principal series representation over $\mathbb{Q}_p$.

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

For $l \in \mathbb{Z}$ let us define

$$\Theta\mathrm{Irr}(l) = \left(\mathrm{ind}_{KZ}^{G} \sigma_{l_1}/T\right) \otimes \omega^{l_2},$$

where l_1 and l_2 are the unique integers such that $l = l_1 + (p+1)l_2 + 2$ and $l_1 \in \{0, \ldots, p-1\}$. For $l \in \mathbb{Z}$ and $\lambda \in \overline{\mathbb{F}}_p^{\times}$ let us define

$$\begin{aligned}&\Theta\mathrm{Red}_{s,\nu}(l,\lambda)\\ &\quad = \pi(\underline{s+2l-2\nu+2}, \lambda, \omega^{\nu-l-1}) \oplus \pi(\underline{2\nu-s-2l-4}, \lambda^{-1}, \omega^{s+l-\nu+2}).\end{aligned}$$

Theorem 4 implies that the three theorems in section 1.4 can be rewritten in the following equivalent forms. Recall that we assume $p > 2$ throughout.

Theorem 5. *Recall that $k \geqslant 2$ is an integer and that s is defined as the integer in $\{1, \ldots, p-1\}$ which is congruent to $k-2 \bmod p-1$. Suppose that k is "non-subtle", i.e.*

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

Suppose also that the open disk $\mathscr{D}_s$ of radius 1 around $s+2 \in \mathscr{W}$ is partitioned into disjoint sets as in $(\mathscr{R}^{s,\nu})$. If $v_p(a) \notin \mathbb{Z}$ then

$$\overline{\Theta}_{k,a} \cong \begin{cases} \Theta\mathrm{Irr}(b_{\nu-1}) & \text{if } k \in \mathscr{R}_0^{s,\nu}, \\ \Theta\mathrm{Irr}(b_{\max\{i,\nu-j-1\}}) & \text{if } k \in \mathscr{R}_{i,j}^{s,\nu}. \end{cases}$$

Theorem 6. *Recall that $k \geqslant 2$ is an integer and that s is defined as the integer in $\{1, \dots, p-1\}$ which is congruent to $k-2 \bmod p-1$. Suppose that k is "non-subtle", i.e.*

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

Suppose also that the open disk $\mathscr{D}_s$ of radius 1 around $s+2 \in \mathscr{W}$ is partitioned into disjoint sets as in $(\mathscr{R}^{s,\nu})$. If $v_p(a) = \nu - 1 \in \mathbb{Z}_{>0}$ then

$$\overline{\Theta}_{k,a}^{\mathrm{ss}} \cong \begin{cases} \Theta\mathrm{Red}_{s,\nu}(0, \lambda_{k,\nu})^{\mathrm{ss}} & \text{if } k \in \mathscr{R}_0^{s,\nu}, \\ \Theta\mathrm{Red}_{s,\nu}(j, \lambda_{k,\nu,i,j})^{\mathrm{ss}} & \text{if } k \in \mathscr{R}_{i,j}^{s,\nu} \text{ and } i+j < \nu-1, \\ \Theta\mathrm{Irr}(b_i) & \text{if } k \in \mathscr{R}_{i,j}^{s,\nu} \text{ and } i+j \geqslant \nu-1, \end{cases}$$

where

$$\lambda_{k,\nu} = \tfrac{\binom{s-\nu+2}{\nu-1}a}{\binom{s-k+2}{\nu-1}p^{\nu-1}} \in \overline{\mathbb{F}}_p^{\times},$$
$$\lambda_{k,\nu,i,j} = \tfrac{(-1)^{\nu+i+j+1}(\nu-j-1)\binom{\nu-j-2}{i}\binom{s-\nu+j+2}{\nu-j-1}a}{(k-s-i(p-1)-2)p^{\nu-j-1}} \in \overline{\mathbb{F}}_p^{\times}.$$

Theorem 7. *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 theorems 5, 6, and 7. We do this in chapters 5, 6, and 7, respectively.

2.4 Notation

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

$$\alpha \operatorname{ind}_{KZ}^{G}\left(\mathrm{Sym}^{k-2}(\overline{\mathbb{Z}}_p^2) \otimes |\det|^{\frac{k-2}{2}}\right) \subseteq \operatorname{ind}_{KZ}^{G}\left(\mathrm{Sym}^{k-2}(\overline{\mathbb{Z}}_p^2) \otimes |\det|^{\frac{k-2}{2}}\right).$$

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

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

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

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

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

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ and let V be an $\overline{\mathbb{F}}_p[H]$-module. Let $V(m)$ denote the twist $V \otimes \det^m$. Let I_h denote the left $\overline{\mathbb{F}}_p[KZ]$-module of degree h homogeneous functions $\mathbb{F}_p^2 \to \overline{\mathbb{F}}_p$ that vanish at the origin, where Z is defined to act trivially and $\alpha \in K$ is defined to act as $(\alpha f)(x,y) = f((x,y)\alpha)$. Note that if $h_1 \equiv h_2 \bmod p-1$ then $I_{h_1} \cong I_{h_2}$. Let us write $\sigma_h = \mathrm{Sym}^h(\overline{\mathbb{F}}_p^2)$. Then $\sigma_{\overline{h}} \subset I_h$, since any element of $\sigma_{\overline{h}}$ is also a function $\mathbb{F}_p^2 \to \overline{\mathbb{F}}_p$ which is homogeneous of degree h and vanishes at the origin and is therefore an element of I_h. Due to lemma 3.2 in [AS86], there is a map

$$f \in I_h \longmapsto \textstyle\sum_{u,v} f(u,v)(vX-uY)^{\underline{-h}} \in \sigma_{\underline{-h}}(h), \tag{2.2}$$

which gives an isomorphism $I_h/\sigma_{\overline{h}} \cong \sigma_{\underline{-h}}(h)$, and therefore the only two factors of I_h are $\sigma_{\overline{h}}$ ("the submodule") and $\sigma_{\underline{-h}}(h)$ ("the quotient"). If $\overline{h} \neq p-1$ then $\sigma_{\underline{-h}}(h)$ is not a submodule of I_h (since the actions of $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)$ on $\sigma_{\underline{-h}}(h)$ and I_h do not match), and hence $\sigma_{\overline{h}}$ is the only submodule. If $\overline{h} = p-1$ then $\sigma_{\underline{-h}}(h) = \sigma_0$ is also a submodule: the submodule of those functions that are equal to a constant everywhere except at the origin.

Let $\theta = xy^p - x^p y$, and for a polynomial f with coefficients in $\overline{\mathbb{Z}}_p$ let $\overline{f}$ denote its reduction modulo $\mathfrak{m}$. Let $r = k-2 \geqslant 0$ and $s = \overline{r}$ and $t(p-1) = r-s$, and suppose that $r \geqslant \nu(p+1)$. For $\alpha \in \{0, \ldots, \nu-1\}$ let

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

These are the subquotients of the filtration

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

This filtration corresponds to a filtration

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

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

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

there is also a filtration

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

whose subquotients are quotients of $\{\widehat{N}_\alpha\}_{0\leqslant\alpha<\nu}$. More precisely, for each $\alpha \in \{0,\dots,\nu-1\}$ there is a surjection

$$\widehat{N}_\alpha \longrightarrow\!\!\!\!\!\rightarrow \overline{\Theta}_\alpha/\overline{\Theta}_{\alpha+1},$$

and the kernel of this surjection consists of those elements of the subquotient $\widehat{N}_\alpha$ of $\operatorname{ind}_{KZ}^{G}\Sigma_r$ that are represented by an element of $\mathscr{I}_a \subset \operatorname{ind}_{KZ}^{G}\Sigma_r$. In the proofs we compute $\overline{\Theta}_{k,a}$ by eliminating the possible subquotients in this filtration. Therefore, the strategy is to find elements of $\mathscr{I}_a$ that represent non-trivial elements in the subquotients $\{\widehat{N}_\alpha\}_{0\leqslant\alpha<\nu}$.

For a property P let us define $[P]=1$ if P is true and $[P]=0$ if P is false. Lemmas 4.1 and 4.3 and remark 4.4 in [BG09] imply that the ideal

$$\mathscr{I}_a \subseteq \operatorname{ind}_{KZ}^{G}\Sigma$$

contains $1 \bullet_{KZ,\overline{\mathbb{Q}}_p} \overline{\theta}^{\nu}h$ for any polynomial h and $1 \bullet_{KZ,\overline{\mathbb{Q}}_p} x^j y^{r-j}$ for all

$$0 \leqslant j < \lceil v_p(a)\rceil = \nu - [v_p(a)\in\mathbb{Z}],$$

and thus $\overline{\Theta}_{k,a}$ is a subquotient of

$$\operatorname{ind}_{KZ}^{G}(\Sigma_r/\langle y^r,\dots,x^{\nu-1-[v_p(a)\in\mathbb{Z}]}y^{r-\nu+1+[v_p(a)\in\mathbb{Z}]},\overline{\theta}^{\nu}\Sigma_{r-\nu(p+1)}\rangle),$$

a module which has a series whose factors are subquotients of $\widehat{N}_0,\dots,\widehat{N}_{\nu-1}$.

For $\alpha \in \{0, \dots, \nu - 1\}$ let us denote

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

2.5 Assumptions

As the statements of the main theorems are vacuous when $\frac{p-1}{2} < \nu$, let us also assume that $\nu - 1 < v_p(a) < \nu$ for some positive integer $\nu \leqslant \frac{p-1}{2}$.

The modules $\overline{V}_{k,a}$ have been completely described when $k \leqslant 2p+1$ (see for instance theorem 3.2.1 in [Ber10]), so we may assume that $k \geqslant 2p+2$. Moreover, the main theorems are true for $p = 3$ (this follows from the main result of [BG09]), so we may assume that $p \geqslant 5$. In particular, since $v_p(a) < \frac{p-1}{2}$ and $k \geqslant 2p+2$ and $(4p+2)(p^2-3p+1) \geqslant 3(p-1)^3$, we can conclude that $k > 3v_p(a) + \frac{(k-1)p}{(p-1)^2} + 1$. Therefore theorem B in [Ber12] implies that there is a constant $m = m(k,a)$ such that

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

whenever $k' \geqslant k$ and $k' \equiv k \bmod (p-1)p^m$. By using this isomorphism we can conclude that if the main theorems are true for $k > p^{100}$ then they are true for all k. Therefore we assume that $k > p^{100}$.

2.6 Combinatorial definitions

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

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

Therefore

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

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

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

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

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

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

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

and

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

for $b, \epsilon \in \mathbb{Z}_p$ and $m \in \mathbb{Z}_{\geqslant 0}$. Therefore

$$\tbinom{b+\epsilon}{n} = \tbinom{b}{n} + \epsilon\tbinom{b}{n}^{\partial} + \mathsf{O}(\epsilon^2)$$

for $b, \epsilon \in \mathbb{Z}_p$ and $n \in \mathbb{Z}_{<p}$.

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

$$\Big(\tfrac{s_1(i,j)}{i!}\Big)_{0 \leqslant i,j \leqslant m} \cdot (1, \ldots, X^m)^T = \Big(\tbinom{X}{0}, \ldots, \tbinom{X}{m}\Big)^T.$$

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

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

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

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

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

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

Let us also define

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

for $u\in\mathbb{Z}_{\geqslant 0}$ and $n\in\mathbb{Z}$, and let $\mathrm{S}_u=\mathrm{S}_{u,0}$.

We use the convention that when the range of summation is not specified, it is assumed to be over all of $\mathbb{Z}$, so that "$\sum_{m_1,\dots,m_k}$" means "$\sum_{m_1\in\mathbb{Z}}\cdots\sum_{m_k\in\mathbb{Z}}$".

2.7 Table of assumptions and definitions

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

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

3

Combinatorial identities

This is a reference chapter which consists entirely of combinatorial identities, mostly involving binomial sums. The proofs of these identities are standard, so the reader may wish to skip this chapter on initial reading and refer back to it as required.

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

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

This never gives rise to convergence issues as $F(m_1,\ldots,m_k)$ is always supported on a finite subset of $\mathbb{Z}^k$ whenever such a sum appears in this thesis. Finally, let us refer to chapter 2 for any definitions, for example of the Stirling numbers $s_1(n,k)$ and $s_2(n,k)$.

Lemma 8. *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*

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

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

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

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

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

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

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

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*

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

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

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

7. *We have*

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

8. *We have*

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

9. *We have*

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

Proof.

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

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

This is because

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

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

$$x^{1+(p-1)p^{m-1}} \equiv x \bmod p^m$$

for $x \in \{0\}\cup\mathbb{Z}_p^\times$, we can conclude $(c\text{-}a)$.

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

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

Then S_u is equal to

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

It is easy to show that $\binom{t_u}{j}p^j = \mathsf{O}(t_u p^2)$ for $j > 1$ by writing

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

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

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

then

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

Moreover, the constant A_{s_u} is independent of t_u. Since

$$\mathrm{S}_{s_u+p-1} = 1 + [s_u = p-1] + \tbinom{s_u+p-1}{p-1}$$

and

$$\begin{aligned}\tbinom{s_u+p-1}{p-1} &= \tfrac{(s_u+1)\cdots(s_u+p-1)}{(p-1)!} + \mathsf{O}(p)\\ &= \tfrac{(s_u-1)!(s_u+1)\cdots(p-1)}{(p-1)!}p + \mathsf{O}(p) = \tfrac{1}{s_u} + \mathsf{O}(p),\end{aligned}$$

we find that $A_{s_u} = \frac{1}{s_u} + \mathsf{O}(p)$.

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

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

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

4. This follows from the congruence

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

5. Let us denote

$$H_{u,d,l,w} = \textstyle\sum_j (-1)^{j-b}\binom{l}{j-b}\binom{u-dj}{w}.$$

Then

$$H_{u,d,l,w} = H_{u-1,d,l,w} + H_{u-1,d,l,w-1}.$$

Thus it is enough to prove equation (c-e) in the boundary cases, i.e. when either $w = 0$ or $u = (b + l)d$. If $w = 0$ then the equation is trivial as both sides are clearly equal to $[w = l]$. If $u = (b + l)d$ then, after introducing the variable $i = l - j + b$, what we need to show is that

$$\textstyle\sum_i (-1)^{l-i} \binom{l}{i} \binom{di}{w} = [w = l] d^l$$

for $w \leqslant l$. This follows from the facts that

$$\begin{aligned} \textstyle\sum_i (-1)^{l-i} \binom{l}{i} \binom{i}{w'} &= (-1)^{l-w'} \binom{l}{w'} \textstyle\sum_i (-1)^{i-w'} \binom{l-w'}{i-w'} \\ &= \binom{l}{w'} (1-1)^{l-w'} = [w' = l] = [w' = w][w = l] \end{aligned}$$

for all $w' \leqslant w$ and

$$\binom{di}{w} = d^w \binom{i}{w} + h_{w-1} \binom{i}{w-1} + \cdots + h_0 \binom{i}{0}$$

for some $h_{w-1}, \ldots, h_0 \in \mathbb{Z}_p$.

6. We can use

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

to rewrite equation (c-f) as

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

And this equation can be shown to be true by using

$$\binom{t}{w} = \textstyle\sum_v (-1)^{w-v} \binom{l+w-v-1}{w-v} \binom{t+l}{v},$$

which, since

$$(-1)^{w-v} \binom{l+w-v-1}{w-v} = \binom{-l}{w-v},$$

follows from Vandermonde's convolution formula. If we apply (c-f) to $X = b - d + l$ and $t = i(p - 1)$, we get

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

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

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

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

9. If $L(b,l,w)$ denotes the left side and $R(b,l,w)$ denotes the right side,
$$\star\,(b,l,w) + \star\,(b,l,w-1) + \star\,(b-1,l,w-1) = 0$$
for $\star \in \{L,R\}$. This is trivial for $\star = R$ and only slightly more difficult for $\star = L$, but the computation in the latter case is standard and only makes use of the equation
$$\textstyle\sum_j \binom{j}{A}\binom{B}{j} = [A = B],$$
so we omit it. Therefore it is enough to show the boundary cases when $b = 0$ or $w = 0$. If $b = 0$ then both sides are equal to $(-1)^w[l = 0]$, and if $w = 0$ then both sides are equal to $(-1)^b[b = l]$.

∎

Lemma 9. *Let $\alpha \in \mathbb{Z} \cap [0, \ldots, \frac{r}{p+1}]$ 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*
$$\textstyle\sum_i D_i x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha} = \theta^\alpha h$$
for some polynomial h with integer coefficients.

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

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

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

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

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

for all $0 \leqslant w < \alpha$. The coefficients of $\theta^\alpha h$ for any polynomial h (which has degree $r - \alpha(p+1)$) satisfy this set of α equations. We can subtract from

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

a suitable $\theta^\alpha h$ such that the only non-zero coefficients of the resulting polynomial have indices among $0, \ldots, \alpha - 2$, i.e. we can find an h such that

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

and $D'_i = 0$ if $i \notin \{0, \ldots, \alpha - 2\}$. Moreover, the coefficients of this h must be integers since the coefficients $\{D_i\}_{i\in\mathbb{Z}}$ are integers. Since Vandermonde's determinant

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

is 1, we have a set of $\alpha - 1$ constants $D'_0, \ldots, D'_{\alpha-2}$ that satisfy α independent linear equations, so all of them must be zero. Hence

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

■

Lemma 10. *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

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

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

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

and

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

The claim then follows from the fact that

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

■

Lemma 11. *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 (see section 2.7). 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 $i \in \{1,\dots,\beta\}$.

Proof. Let $L = L_\alpha(p-1,1)$ be the matrix defined in lemma 10. Then

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

Let $E = \left(\binom{w}{l}\right)_{0\leqslant l,w\leqslant\alpha}$. Then the claim follows from the fact that

$$B_\alpha = \left((-1)^{i+l}\binom{l}{i}\right)_{0\leqslant i,l\leqslant\alpha} \cdot L = E^{-1}L.$$

■

3.3 Combinatorial identities involving formal variables

Lemma 12. *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

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

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

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

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

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

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

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

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

Lemma 13. *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

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

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

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

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

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

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

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

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

Lemma 14. *Suppose that $s,\alpha\in\mathbb{Z}_{\geqslant 0}$ are such that*

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

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

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

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

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

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

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

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

Proof. Let us first show that

$$C_0(z)\tbinom{z-\alpha}{s-\alpha} + \sum_{j=1}^{\alpha} C_j(z)\tbinom{z-\alpha+j}{s-\alpha} = \tfrac{(-1)^{\alpha+1}(z-\alpha)}{s-\alpha}. \tag{3.1}$$

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

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

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

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

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

$$(s-\alpha) \sum_j \tfrac{(-1)^{j+1}}{j+1} \tbinom{s-\alpha-1}{\alpha-j} \tbinom{s-\alpha-\gamma+j}{s-\alpha}$$

for $\gamma \in \{0, \ldots, s-\alpha-1\}$. 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 $u \in \{1, \ldots, s-\alpha-1\}$. In particular, (3.1) 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

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

(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

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

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

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

and consequently

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

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 $i \in \{1, \ldots, \gamma - 1\}$. That is equivalent to

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

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

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

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

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

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

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

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

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

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

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

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

3.4 Combinatorial identities involving matrices

Lemma 15. *Let X and Y denote formal variables, and let*

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

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*

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

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

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

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

Proof. If $w = 0$ then

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

Thus we have computed the first coordinate of $(d_0, \ldots, d_\alpha)^T$. If $0 < w \leqslant \alpha$ and $0 < j \leqslant \alpha$ then, due to (*c*-*f*),

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

To compute d_w we want to show that

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

where $(Mc)_w$ denotes the wth entry of Mc. The degree of $(Y-\alpha)(Mc)_w$ is at most $\alpha+1$. We are going to show that $(Y-\alpha)(Mc)_w$ belongs to the ideal generated by $Y-X-t$ for $0 \leqslant t \leqslant \alpha$—then it must be a constant multiple of $(Y-X)_{\alpha+1}$ and we can deduce that the constant is indeed $[w=\alpha]$ by comparing the coefficients of $Y^{\alpha+1}$. If $t=0$ then the claim is obvious, so suppose that $0 < t \leqslant \alpha$. In that case $(Mc)_w$ is a polynomial of degree at

most $\alpha - 1$ in the quotient ring

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

By (c-f),

$$M_{w,j} = \sum_l \binom{t}{l}\binom{X+j}{j-l}\binom{-l}{w} = (-1)^w \sum_l \binom{t}{l}\binom{X+j}{j-l}\binom{w+l-1}{w}.$$

So

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

is equal to

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

Here the first equality is a simple rewrite. For the second equality we replace $j+1$ with j in the first term of the inner sum, i.e. we use the equation

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

to rewrite

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

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

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

is zero for $l < 0$ (as then $\binom{t}{l} = 0$), for $l = 0$ (as then $\binom{w+l-1}{w} = 0$), for $l = 1$ (as then $1 - l = 0$), and for $l > 1$ (as then $\binom{X+1}{1-l} = 0$). For the third equality

we use Vandermonde's convolution formula

$$\tbinom{z+m}{n} = \sum_u \tbinom{z}{u}\tbinom{m}{n-u},$$

which holds true for $m \in \mathbb{Z}$ and $n \geqslant 0$ (as both sides are the coefficient of Z^n in $(1+Z)^{z+m}$). To be more precise, we write

$$\tbinom{X+j}{j-l}\tbinom{X+t}{\alpha-j} = \sum_u \tbinom{\alpha-t}{j-l-u}\tbinom{X+t-\alpha+j}{u}\tbinom{X+t}{\alpha-j} = \sum_u \tbinom{\alpha-t}{j-l-u}\tbinom{\alpha-j+u}{u}\tbinom{X+t}{\alpha-j+u}.$$

Finally, the fourth equality is a simple change of variable where we replace $\alpha - j + u$ with u. Since the degree of the polynomial is at most $\alpha - 1$, we can replace the final sum $\sum_u$ with $\sum_{u=0}^{\alpha-1}$, and for u in this range we have

$$\sum_{j>0} \tfrac{(-1)^j}{j}\tbinom{u}{u-\alpha+j} = \sum_j \tfrac{(-1)^{j+\alpha-u}}{j+\alpha-u}\tbinom{u}{j} = \tfrac{(-1)^{\alpha-u}(\alpha-u-1)!u!}{\alpha!}.$$

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

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

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

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

Let us denote the left side by $L(t)$ and the right side by $R(t)$. Then

$$\sum_{j=0}^{m}(-1)^j\tbinom{m}{j}R(j+1) = \tfrac{w_m}{\alpha_{m+1}}\tbinom{Y-m-1}{\alpha-m-1} = \sum_u \tbinom{Y}{u}\tfrac{(-1)^{\alpha-m-u-1}w_m}{\alpha_{m+1}}\tbinom{\alpha-u-1}{\alpha-m-u-1}.$$

To conclude that $L(t) = R(t)$ for $1 \leqslant t \leqslant \alpha$, it is evidently enough to show that

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

for $0 \leqslant m < \alpha$. We can uniquely write each side (as an element of $\mathbb{Q}_p[Y]$) in the form

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

To show that the two sides are equal, it is enough to show that the coefficients of $\binom{Y}{u}$ are the same on both sides, which (after multiplying both coefficients

by $(-1)^{\alpha-m-u-1}\alpha\binom{\alpha-1}{u}$) is equivalent to showing that

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

Let us show that this equation is true more generally for all $\alpha, m, u, w \geqslant 0$. Let $L(\alpha, u)$ denote the left side and let $R(\alpha, u)$ denote the right side. Then

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

for $\star \in \{L, R\}$. Therefore we only need to show the boundary cases, i.e. the ones when $u = 0$ or $\alpha = 0$. If $u = 0$ then, since $l - j - 1 \leqslant 0$, the only terms on the left side that are non-zero are the ones such that $l - 1 = j$. Thus, the equation is

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

This follows from

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

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

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

Let $L(w, m, u)$ denote the left side and let $R(w, m, u)$ denote the right side of this equation. Then the equation follows from the fact that

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

and

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

are both equal to

$$\frac{1}{1-Z_1-Z_3-Z_1Z_2+Z_1Z_3}$$

(as can be found by a routine computation). ∎

Lemma 16. *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 11. 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

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

Then there is a solution of

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

such that $z_0 \neq 0$.

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

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

Since

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

for $l > 0$, it follows that

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

In particular, $\overline{B}_{0,w} = \binom{\alpha}{w}$ and $\sum_{w=0}^{\alpha}(-1)^{w-v}\overline{B}_{i,w}\binom{j+w-v-1}{w-v}$ is equal to

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

The third equality follows from (*c-j*). When $0 \leqslant v \leqslant j \leqslant \alpha$, this is equal to

$$(-1)^{i+j+v}\tbinom{v}{j-i},$$

due to (*c-k*). Hence we can simplify $M_{i,j}$ for $i \notin \{1,\dots,\beta\}$ as

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

Moreover, if $i \in \{\beta+1,\dots,\alpha\}$ then by lemma 12 we have

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

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

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

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

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

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

in the relevant sum

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

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

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

has a solution such that $z_0 \neq 0$ as long as the determinant

$$\det M = M_{0,0} \cdots M_{\alpha,\alpha}$$

is non-zero. Since $\overline{B}_{0,w} = \binom{\alpha}{w}$,

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

Due to (c-i) and lemma 12, that is equal to

$$-\sum_{w>0} \frac{1}{w} \binom{\beta-1-w}{\alpha-w} - \frac{(-1)^\alpha}{\beta} \binom{\alpha-\beta}{\alpha} = (-1)^{\alpha+\beta+1} \sum_w \frac{(-1)^w}{w+\beta} \binom{\alpha-\beta}{w} = \frac{(-1)^{\alpha+\beta+1}}{\beta \binom{\alpha}{\beta}}.$$

The diagonal entries $M_{1,1}, \ldots, M_{\beta,\beta}$ are equal to $\binom{\beta}{1}, \ldots, \binom{\beta}{\beta}$. For $\beta < j$,

$$M_{j,j} = -\sum_{w>0} \frac{1}{w} \binom{\beta-w}{j-w},$$

due to lemma 12, and that is equal to $\frac{(-1)^{\beta+j}}{(\beta+1)\binom{j}{\beta+1}}$. Therefore,

$$\det M = \frac{(-1)^{\alpha+\beta+1}(\alpha-\beta)!\beta!}{(s-\alpha)_{\alpha+1}} \prod_{j=1}^{\beta} \binom{\beta}{j} \prod_{j=\beta+1}^{\alpha} \frac{(-1)^{\beta+j}}{(\beta+1)\binom{j}{\beta+1}} \neq 0,$$

implying that there is indeed a solution of

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

such that $z_0 \neq 0$. ∎

Lemma 17. *Suppose that $s, \alpha, \beta \in \mathbb{Z}$ are such that*

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

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

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

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

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

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

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

Then

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

Proof. Let us denote the rows of M by

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

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

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

We have the following string of equations:

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

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

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

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

have

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

The third equality follows from lemma 12. Thus $\mathbf{r}_0(C_0,\ldots,C_\alpha)^T$ is equal to

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

The third equality follows from lemma 12. Thus we have computed

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

- *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

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

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

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

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

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

The identity

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

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

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

and consequently

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

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

$$\begin{aligned}
\Phi_1(z) &= \textstyle\sum_{l,v=0}^{\alpha}(-1)^{l+v+1}\binom{l}{i}\binom{v}{s-\alpha}\binom{z+s-\alpha}{v}\binom{-v}{l-v},\\
\Phi_2(z) &= \textstyle\binom{i-1}{s-\alpha-1}\binom{z+i-1}{i-1},\\
\Phi_3(z) &= \textstyle\sum_{l,j,v=0}^{\alpha}(-1)^{\alpha+j+l+v+1}\binom{j}{2\alpha-s+1}\binom{\alpha+1}{j+1}\binom{l}{i}\binom{j-v}{l-v}\binom{z+s-\alpha+j}{v}\binom{s-\alpha+j-v}{j-v},\\
\Phi_4(z) &= \textstyle\binom{\alpha+1}{s-\alpha}\sum_{l=0}^{\alpha}\binom{l}{i}\binom{z+l-1}{l} = \binom{\alpha+1}{s-\alpha}\binom{z+\alpha}{\alpha-i}\binom{z+i-1}{i}.
\end{aligned}$$

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

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

Now suppose that $s \neq \alpha + \beta$. As in the proof of lemma 12 we can simplify $\Phi_1(z)$ to

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

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

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

Suppose first that $i > \beta$. Then

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

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

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

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

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

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

$$\begin{aligned}
&\textstyle\sum_j (-1)^j \tbinom{j}{2v-u+1} \tbinom{v+1}{j} \tbinom{u-v-w+j}{u-v-w+t} \\
&\quad = \textstyle\sum_{j,e} (-1)^j \tbinom{v-w+1}{u-v-w+i-e} \tbinom{j}{2v-u+1} \tbinom{v+1}{j} \tbinom{u-2v+j-1}{e} \\
&\quad = \textstyle\sum_{j,e} (-1)^j \tbinom{v-w+1}{u-v-w+i-e} \tbinom{j}{2v-u+e+1} \tbinom{v+1}{j} \tbinom{2v-u+e+1}{e} \\
&\quad = \textstyle\sum_{j,e} (-1)^{u+e+1} \tbinom{v-w+1}{u-v-w+t-e} \tbinom{u-2v-e-2}{j+u-2v-e-1} \tbinom{v+1}{v-j+1} \tbinom{2v-u+e+1}{e} \\
&\quad = \textstyle\sum_{e} (-1)^{u+e+1} \tbinom{v-w+1}{u-v-w+t-e} \tbinom{u-v-e-1}{u-v-e} \tbinom{2v-u+e+1}{e} \\
&\quad = (-1)^{v+1} \tbinom{v-w+1}{t-w} \tbinom{v+1}{u-v}.
\end{aligned} \tag{3.2}$$

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

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

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

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

which is zero by (3.2). Finally, suppose that $i = \beta$. Then

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

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

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

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

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

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

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

with

$$L_3 := \beta\Phi_1'(-\beta),$$
$$R_3 := (s-\alpha-\beta)(\Phi_3'(-\beta)+\Phi_4'(-\beta)) - \Phi_2(-\beta).$$

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

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

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

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

and if $u < v + w$ then

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

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

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

■

Lemma 18. *Suppose that $s, \alpha, \beta \in \mathbb{Z}$ are such that*

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

Let M denote the $(\alpha+1) \times (\alpha+1)$ matrix with entries in $\mathbb{F}_p$ defined in lemma 17. 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 ith row of M is straightforward if $i \notin \{0, \alpha\}$. Since $M_{0,j}$ is equal to

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

and since

$$\begin{aligned}
\textstyle\sum_j (-1)^j \binom{\alpha-2}{j-2} \frac{1}{j(j-1)} &= \tfrac{1}{\alpha}, \\
\textstyle\sum_j (-1)^j \binom{\alpha-2}{j-2} \binom{j-2}{s-\alpha} \binom{0}{\alpha}^{\partial} &= (-1)^{\alpha} \binom{0}{\alpha}^{\partial} = -\tfrac{1}{\alpha}, \\
\textstyle\sum_l^{\alpha} (-1)^{l+\alpha} \binom{2-\alpha}{l-\alpha} \binom{0}{\alpha}^{\partial} \binom{p-1}{\alpha-2} &= -\tfrac{1}{\alpha}, \\
\textstyle\sum_l^{\alpha} (-1)^{l+\alpha} \binom{2-\alpha}{l-\alpha} \binom{0}{\alpha}^{\partial} \binom{0}{\alpha-2} &= -\tfrac{[\alpha=2]}{\alpha},
\end{aligned}$$

the equation associated with the zeroth row is

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

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 19. *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

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

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

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

with

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

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. ∎

4

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

In this chapter we prove six core results that we subsequently use to compute $\overline{\Theta}_{k,a}$. As we remarked in section 2.4, the main strategy for computing $\overline{\Theta}_{k,a}$ is to find elements of $\mathscr{I}_a$ that represent non-trivial elements in the subquotients $\{\widehat{N}_\alpha\}_{0\leqslant\alpha<\nu}$. We refer to section 2.7 for the relevant notation. We recall that $\nu \leqslant \frac{p-1}{2} < p$ and $k > p^{100}$ (and therefore $r > p^{99}$). Let us write $n = p^2$, so that $r > np^2$.

Lemma 20. *Suppose that* $\alpha \in \{0, \dots, \nu - 1\}$.

1. *We have*

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

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

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

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

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

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

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

Proof. (1) Let us recall the formula

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

for T. Directly from the definition of θ we have

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

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

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

can be expanded into

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

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

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

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

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

due to (c-e) applied to $(u, b, w, l) = (r-\alpha, 0, \xi, n)$. The second part of the

formula, the part

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

is precisely

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

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

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

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

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

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

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

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

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

The third equality follows from the fact that

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

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

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

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

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

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

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

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

Lemma 21. *Suppose that $\alpha \in \mathbb{Z}$ and $v \in \mathbb{Q}$ are such that*

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

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

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

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 $v_p(F) > v'$.

Proof. By using the equation

$$v = a^{-1}Tv - (T-a)(a^{-1}v)$$

we can rewrite

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

as

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

where $\mathrm{ERR}_3 + \mathsf{O}(p^{\nu-\alpha}) \in \mathrm{im}(T-a)$. Here

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

The constants Δ_j are precisely designed in a way that $X_\alpha = 0$. We assume

$$v_p(X_\xi) \geqslant v'$$

for $\alpha < \xi < 2\nu - \alpha$, so the part of the sum "$\sum_{\xi=0}^{2\nu-1-\alpha}$" where $\nu \leqslant \xi$ is in

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

Due to part (1) of lemma 20, the part of the sum where $\alpha < \xi < \nu$ is

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

where

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

and h and E are such that $v_p(E) \geqslant v'$ (since $v_p(X_\xi) \geqslant v'$ for all $\alpha < \xi < \nu$). Similarly, the part of the sum where $\xi \leqslant \alpha$ is

$$\textstyle\sum_{\xi=0}^{\alpha-1} F_\xi \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\xi h_\xi + \mathrm{ERR}_5,$$

where

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

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

$$Fh' = \textstyle\sum_{\xi=0}^{\alpha-1} F_\xi \theta^\xi h_\xi$$

for some h' and F. ∎

Lemma 22. *Let $\{C_l\}_{l\in\mathbb{Z}}$ 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*

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

satisfy the conditions of lemma 21, i.e.

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

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* $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Proof. Before proceeding to the proofs of (1) and (2), let us make some initial remarks. Due to part (2) of lemma 20, we know that $\mathrm{im}(T - a)$ contains

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

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

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

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

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

can be factored as $\theta^\alpha h$, due to lemma 9. The general case when $\vartheta_w(D_\bullet) > v'$ for $0 \leqslant w < \alpha$ can be reduced to this special case by adding a term h' such that $v_p(h') > v'$. Then $\overline{\theta}^\alpha \overline{h}$ is an element of N_α, and the number ϑ' is specifically designed in a way that $\overline{\theta}^\alpha \overline{g}$ is precisely $\overline{\vartheta'}$ times a generator of N_α. If ϑ' is a unit then this immediately gives us an element of $\mathrm{im}(T - a)$ whose reduction modulo $\mathfrak{m}$ represents a generator of $\widehat{N}_\alpha$. Note that in general the

valuation of ϑ' is an integer. If that integer is strictly positive then we would like to divide ϑ' by a power of p prior to reducing modulo $\mathfrak{m}$. We cannot do this directly, since almost certainly there exist some D_i whose valuation is strictly smaller than the valuation of ϑ'. Thus we would like to "smoothen" the D_i to better constants Δ_i which have much of the same qualities as the D_i (i.e. satisfy the same conditions) but whose valuations are all at least as large as the valuation of ϑ'. We use the constants Δ_i from lemma 21, and we replace D_i with Δ_i by adding

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

We know, directly from the definition of the constants Δ_i, that

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

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

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

is $\overline{A-B}$ times a generator of $\widehat{N}_\alpha$. We use lemma 21 to deduce that if we add some extra error terms to

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

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

$$\begin{aligned}(\vartheta' + C_{-1}) \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\alpha x^{p-1} y^{r-\alpha(p+1)-p+1} + C_{-1} \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^n x^{\alpha-n} y^{r-np-\alpha} \\ + E \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^{\alpha+1} h + F \bullet_{KZ,\overline{\mathbb{Q}}_p} h' + \mathsf{O}\Big(p^{\nu-v_p(a)+v} + p^{v_p(a)-\alpha}\Big), \qquad (4.1)\end{aligned}$$

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

(1) Suppose that $v_p(\vartheta') \leqslant v'$. Let us note that $v_p(C_{-1}) \geqslant v_p(\vartheta')$. If we multiply (4.1) by $\|\vartheta'\|_p$ and reduce modulo $\mathfrak{m}$ we obtain in $\mathscr{I}_a$ a representative

of a generator of $\widehat{N}_\alpha$. Note that the reductions modulo $\mathfrak{m}$ of the terms in the second row of (4.1) are trivial as $v_p(a) - \alpha > v_p(\vartheta')$ (since, crucially, $v_p(a)$ is not an integer). Thus we define gen_1 to be this element.

(2) Suppose that $v_p(a) - \alpha < v$. Then the dominant term in (4.1) comes from the error term $\mathsf{O}(ap^{-\alpha})$, which is described in the last displayed equation in the statement of lemma 20. Thus after we multiply (4.1) by $\frac{p-1}{ap^{-\alpha}C_0}$ and reduce modulo $\mathfrak{m}$, we get a representative of

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

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

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

and is represented by the reduction modulo $\mathfrak{m}$ of an element of $\mathrm{im}(T-a)$. The classification given in theorem 4 implies that either $T-\lambda$ acts trivially on $\mathrm{ind}_{KZ}^G \mathrm{quot}(\alpha)$ modulo $\mathscr{I}_a$ for some $\lambda \in \overline{\mathbb{F}}_p$, or $s \in \{1, 3, \ldots, 2\nu-1\}$ and $(T-\lambda)(T-\lambda^{-1})$ acts trivially on $\mathrm{ind}_{KZ}^G \mathrm{quot}(\alpha)$ modulo $\mathscr{I}_a$ for some $\lambda \in \overline{\mathbb{F}}_p^\times$, 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 first consider the case when $T-\lambda$ acts trivially. Then

$$\left(A\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right) + \lambda - [r \equiv_{p-1} 2\alpha](1-B)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right)\right) \bullet_{KZ,\overline{\mathbb{F}}_p} X^{\underline{2\alpha-r}} \qquad (4.2)$$

  in $\mathrm{ind}_{KZ}^G \mathrm{quot}(\alpha)$ is represented by an element of $\mathscr{I}_a$. First suppose that $\underline{2\alpha-r} > 0$. If $A \neq 0$ then either $\lambda = 0$ in which case $\mathrm{ind}_{KZ}^G \mathrm{quot}(\alpha)$ is trivial modulo $\mathscr{I}_a$, or $\lambda \neq 0$ in which case we can multiply (4.2) on the left by $[\mu]^{p-2}\left(\begin{smallmatrix} 1 & 0 \\ [\mu] & 1\end{smallmatrix}\right)$ and sum over all $\mu \in \mathbb{F}_p$ to obtain that $\lambda \bullet_{KZ,\overline{\mathbb{F}}_p} X^{\underline{2\alpha-r}-1}Y$ is represented by an element of $\mathscr{I}_a$, so we can take

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

  If $A = 0$ then either $\lambda \neq 0$ in which case $\mathrm{ind}_{KZ}^G \mathrm{quot}(\alpha)$ is trivial modulo

$\mathscr{I}_a$, or $\lambda = 0$ in which case we can take

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

Now suppose that $\underline{2\alpha - r} = 0$. Then we can use the decomposition of G into cosets of KZ given in section 2.1.2 of [Bre03b] together with the fact that 4.2 is trivial modulo $\mathscr{I}_a$ to conclude that any element of $\mathrm{ind}_{KZ}^{G} \mathrm{quot}(\alpha)$ can be written in the form

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

for some h'' which is represented by an element of $\mathscr{I}_a$, and thus we can find a suitable $\mathrm{gen}_2 \in \mathscr{I}_a$ that represents a generator of a submodule of $T(\mathrm{ind}_{KZ}^{G} \mathrm{quot}(\alpha))$ which has codimension at most two.

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

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

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

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

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

Consequently, either $\mathscr{I}_a$ contains a representative of a generator of a finite-codimensional submodule of $T(1 \bullet_{KZ,\overline{\mathbb{F}}_p} X^{\underline{2\alpha - r}})$, or it contains a representative of a generator of $\mathrm{ind}_{KZ}^{G} \mathrm{quot}(\alpha)$ (the latter being a stronger statement), and we can take gen_2 to be that element of $\mathscr{I}_a$. ∎

Lemma 23. *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

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

Let

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

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

$$\begin{aligned}&(\vartheta'+C_{-1})\bullet_{KZ,\overline{\mathbb{Q}}_p}\theta^\alpha x^{p-1}y^{r-\alpha(p+1)-p+1} + C_{-1}\bullet_{KZ,\overline{\mathbb{Q}}_p}\theta^n x^{\alpha-n}y^{r-np-\alpha}\\ &\quad+\textstyle\sum_{\xi=\alpha+1}^{2\nu-\alpha-1} E_\xi\bullet_{KZ,\overline{\mathbb{Q}}_p}\theta^\xi h_\xi + F\bullet_{KZ,\overline{\mathbb{Q}}_p}h' + H,\end{aligned}\tag{4.3}$$

for some h_ξ, h', E_ξ, F, H *such that*

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

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 22. 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 (4.3), 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 (4.3) without these extra conditions, and to complete the proof of lemma 23 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 21, 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 21. 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 21. Finally, condition (4) follows from the description of the error term in lemma 20, as in the proof of lemma 22. ∎

Corollary 24. *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*

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

are such that

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

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

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

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 23: 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 23 implies that the element in (4.3) is in $\mathrm{im}(T-a)$. 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 $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\alpha)$.

(3, 4, 5) The condition $v_p(a)-\alpha < v \leqslant v_p(C_{-1})$ ensures that the term with the dominant valuation in (4.3) 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 23. This element L is in $\mathrm{im}(T-a)$, 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 22, if $C_0 \in \mathbb{Z}_p^\times$ then this element always generates a finite-codimensional submodule of

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

and if additionally $A \neq 0$ (over $\mathbb{F}_p$) then in fact we have the stronger conclu-

sion that it generates

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

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 $\widehat{N}_\alpha$. ∎

Corollary 25. *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

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

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

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

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

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

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

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. $\Big(v_p(a) - \alpha < v \leqslant v_p(C_{-1})$ *&* $C_0 \in \mathbb{Z}_p^\times$, $\mathbf{r}_2\Big)$, *where*

$$\mathbf{r}_2$$

is a finite-codimensional submodule of

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

6. $\Big(v_p(a) - \alpha = v = v_p(\vartheta') \leqslant v_p(C_{-1})$ *&* $\check{C} \notin \mathbb{Z}_p^\times$ *&* $C_0 \in \mathbb{Z}_p^\times$, $\mathbf{r}_3\Big)$ *for*

$$\mathbf{r}_3 = \left(T + \hat{C}\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) - \frac{C_0^{-1}\vartheta'}{ap^{-\alpha}}\right)(\operatorname{ind}_{KZ}^G \operatorname{quot}(\alpha)),$$

where

$$\hat{C} = [r \equiv_{p-1} 2\alpha]\left((-1)^\alpha \textstyle\sum_{l=0}^{\alpha} C_0^{-1} C_l \binom{r-\alpha+l}{s-\alpha} - 1\right).$$

7. $\Big(v_p(a) - \alpha = v = v_p(C_{-1}) < v_p(\vartheta')$ *&* $C_0 \notin \mathbb{Z}_p^\times$ *&* $\underline{2\alpha - r} > 0$, $\mathbf{r}_4\Big)$ *for*

$$\mathbf{r}_4 = \left(T + \frac{\check{C}ap^{-\alpha}}{C_{-1}}\right)(\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha)).$$

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

9. $\Big(v_p(a) - \alpha = v = v_p(C_{-1}) < v_p(\vartheta')$ *&* $C_0 \in \mathbb{Z}_p^\times$, $\mathbf{r}_5\Big)$, *where*

$$\mathbf{r}_5$$

is a finite-codimensional submodule of

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

Proof. (1, 2, 3, 4, 5) The proofs of these parts are nearly identical to the proofs of the corresponding parts of corollary 24.

(6) The proof is similar to the proof of (5), the only difference being that the valuation of ϑ' is the same as the valuation of the coefficient of H. To be more specific, we divide γ by C_0, the term "T" comes from the expression for H given in lemma 23, the term "$\hat{C}\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)$" comes from

$$[r \equiv_{p-1} 2\alpha](C_0^{-1}B - 1)\left(\begin{smallmatrix}0&1\\p&0\end{smallmatrix}\right),$$

the reason there is no term "$A\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)$" is because $A = \check{C} = \mathsf{O}(p)$, and the term "$-\frac{C_0^{-1}\vartheta'}{ap^{-\alpha}}$" comes from the first line of the formula for γ given in (4.3).

(7) As in the previous parts we can deduce that $\mathscr{I}_a$ contains

$$L := \tfrac{\check{C}ap^{-\alpha}}{C_{-1}}\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right) \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\alpha(y^{r'} - x^{p-1}y^{r'-p+1}) + 1 \bullet_{KZ,\overline{\mathbb{Q}}_p} \theta^\alpha y^{r'} + L',$$

where $r' = r - \alpha(p+1)$ and L' reduces modulo $\mathfrak{m}$ to a trivial element of $\mathrm{sub}(\alpha)$. The reduction modulo $\mathfrak{m}$ of the element $\sum_{\mu\in\mathbb{F}_p}\left(\begin{smallmatrix}1&0\\[\mu]&p\end{smallmatrix}\right)L$ generates $\mathbf{r}_4$.

(8, 9) The proofs of these parts are similar to the proofs of (4, 5). ∎

5

Proof of theorem 5

The proof of theorem 5 is based on the approach outlined in [BG09], and roughly consists of finding enough elements in $\mathscr{I}_a$, consequently eliminating enough subquotients of $\mathrm{ind}_{KZ}^{G} \Sigma_r$, and using that information to find $\overline{\Theta}_{k,a}$.

5.1 Running assumptions

Throughout this chapter we assume that

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

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

5.2 Theorem 5 is equivalent to propositions 26 + 27

Let us first show the equivalence between theorem 5 and the union of the following two propositions.

Proposition 26. *If $k \in \mathscr{R}_0^{s,\nu}$ then any infinite-dimensional factor of $\overline{\Theta}_{k,a}$ is a quotient of $\widehat{N}_{\nu-1}$. If $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ then none of the infinite-dimensional factors of $\overline{\Theta}_{k,a}$ are quotients of a representation in the set*

$$\left\{\widehat{N}_0, \ldots, \widehat{N}_{\max\{\nu-t-1,\beta\}-1}\right\}.$$

Proposition 27. *If $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ then none of the infinite-dimensional factors of $\overline{\Theta}_{k,a}$ are quotients of a representation in the set*

$$\left\{\widehat{N}_{\max\{\nu-t-1,\beta\}+1}, \ldots, \widehat{N}_{\nu-1}\right\}.$$

Proof that theorem 5 is equivalent to propositions 26 + 27. First let us assume that propositions 26 and 27 are true. Together they imply that any infinite-dimensional factor of $\overline{\Theta}_{k,a}$ is a quotient of $\widehat{N}_\alpha$, where $\alpha = \nu - 1$ if $k \in \mathscr{R}_0^{s,\nu}$ and $\alpha = \max\{\nu - t - 1, \beta\}$ if $k \in \mathscr{R}_{\beta,t}^{s,\nu}$. The classifications given by theorem 4 and theorem 2.7.1 in [Bre03a] imply that if $\overline{\Theta}_{k,a}$ is reducible then it must have exactly two infinite-dimensional factors. There may be an additional one-dimensional factor, a twist of the Steinberg representation. Suppose that the infinite-dimensional factors are quotients of $\mathrm{ind}_{KZ}^G(\sigma_b(b'))$ and $\mathrm{ind}_{KZ}^G(\sigma_d(d'))$, respectively. By theorem 4 we must have

$$b' - d' \equiv_{p-1} d + 1 \text{ and } b + d \equiv_{p-1} -2.$$

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

$$2\alpha - r \equiv_{p-1} 2\alpha - r + 1.$$

Similarly, the two representations cannot be two copies of $\mathrm{ind}_{KZ}^G \mathrm{sub}(\alpha)$, as

that would imply that

$$2\alpha \equiv_{p-1} s+1,$$

a contradiction since $2\alpha \in \{2,\dots,2\nu-2\}$ and $s \in \{2\nu,\dots,p-1\}$. And, the two representations cannot be two copies of $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\alpha)$, as that would imply that

$$2\alpha \equiv_{p-1} s-1,$$

which is similarly a contradiction. Thus we can conclude that $\overline{\Theta}_{k,a}$ must be irreducible, and the classifications given by theorem 4 and theorem 2.7.1 in [Bre03a] imply that the only possible quotient of $\widehat{N}_\alpha$ that $\overline{\Theta}_{k,a}$ can be is $\Theta\mathrm{Irr}(b_\alpha)$. This implies theorem 5.

Conversely, if theorem 5 is true, then the fact that $\overline{\Theta}_{k,a} \cong \Theta\mathrm{Irr}(b_\alpha)$ implies that $\overline{\Theta}_{k,a}$ is irreducible and not a quotient of a representation in the set

$$\left\{\widehat{N}_0,\dots,\widehat{N}_{\nu-1}\right\} \setminus \{N_\alpha\}.$$

■

5.3 Proof of proposition 26

Recall from section 2.7 that $X_n = X(X-1)\cdots(X-n+1) \in \mathbb{Z}_p[X]$ is the falling factorial. Let $\alpha \in \{0,\dots,\nu-2\}$ and let us consider $\widehat{N}_\alpha$. The task is to show that if $\alpha < \max\{\nu-t-1,\beta\}$ then none of the infinite-dimensional factors of $\overline{\Theta}_{k,a}$ are quotients of $\widehat{N}_\alpha$.

Let $v \in \mathbb{Q}$, let $\{C_l\}_{l\in\mathbb{Z}}$ be any family of elements of $\mathbb{Z}_p$, and let us define the constants

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

Let us note from the definition of $\vartheta_j(D_\bullet)$ for $j \in \{0,\dots,p-1\}$ that it is a $\mathbb{Z}_p$-linear combination of the constants $C_{-1}, C_0, \dots, C_\alpha$. In the proof we make suitable choices for the constants $C_{-1}, C_0, \dots, C_\alpha$ so that the constants

$\{D_i\}_{i\in\mathbb{Z}}$ satisfy the conditions of lemma 22, i.e.

$$\begin{aligned} v &\leqslant v_p(\vartheta_\alpha(D_\bullet)),\\ v' := \min\{v_p(a)-\alpha, v\} &\leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } \alpha < w < 2\nu-\alpha,\\ v' &< v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha,\\ C_0 &\in \mathbb{Z}_p^\times,\\ v_p(C_{-1}) &\geqslant v_p(\vartheta'). \end{aligned}$$

Suppose that we find such choices for $C_{-1}, C_0, \ldots, C_\alpha$ and that moreover we have $v_p(\vartheta') \leqslant v'$. Then we can conclude from part (1) of lemma 22 that none of the infinite-dimensional factors of $\overline{\Theta}_{k,a}$ are quotients of $\widehat{N}_\alpha$.

Let U denote the $(2\nu-\alpha)\times(\alpha+1)$ matrix with entries in $\mathbb{Q}_p$ such that

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

Let U^{sub} denote the $(\alpha+1)\times(\alpha+1)$ submatrix consisting of the top $\alpha+1$ rows of U. Note that $\alpha \in \{0,\ldots,\nu-2\}$ implies that $\alpha+1 < 2\nu-\alpha$. We have

$$U_{w,j} = \textstyle\sum_v (-1)^{w-v}\binom{j+w-v-1}{w-v}\binom{r-\alpha+j}{v}\left(\binom{s-\alpha+j-v}{j-v} - \binom{r-\alpha+j-v}{j-v}\right) + \mathsf{O}(p)$$

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

Let us consider four different cases, and find constants $\{C_j\}$ that are suitable in each case.

- *Suppose that* $\alpha = 0$. Let us choose $C_0 = 1$ and $C_{-1} = 0$. Then, due to (c-b),

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

Moreover, due to (c-b) and (c-c),

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

for $0 < w < 2\nu$. So if $0 = \alpha < \max\{\nu - t - 1, \beta\}$, then either $\beta > 0$ in which case $s - r \in \mathbb{Z}_p^\times$ and $\vartheta_0(D_\bullet) \in \mathbb{Z}_p^\times$ and therefore the constants $\{C_j\}$ are suitable for $v = 0$, or $\beta = 0$ and $t \leqslant \nu - 2$ in which case $v_p(\vartheta_0(D_\bullet)) = t$ and $v_p(\vartheta_w(D_\bullet)) \geqslant t$ for $0 < w < 2\nu$ and therefore the constants $\{C_j\}$ are suitable for $v = v' = t$.

- *Suppose that* $\alpha > 0$ *and* $\beta \notin \{0, \ldots, \alpha\}$. The second condition implies that $v_p((s-r)_{\alpha+1}) = 0$. Let M and c be as in lemma 15, and let us make the substitutions $X = r - \alpha$ and $Y = s - \alpha$. Let us apply lemma 15 with $(C_{-1}, C_0) = (0, 1)$ and

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

for $0 < j \leqslant \alpha$. Then

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

We can use (c-b) and (c-g) to compute that

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

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

$$U_{w,j} = p^{[j=0]}(M_{w,j} + \mathsf{O}(p))$$

for $0 \leqslant w \leqslant \alpha$ and $0 < j \leqslant \alpha$. Therefore, due to lemma 15, the first α entries of the resulting column vector $(\vartheta_0(D_\bullet), \ldots, \vartheta_{2\nu-\alpha-1}(D_\bullet))^T$ are $\mathsf{O}(p^2)$,

and the entry indexed α is

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

Since all subsequent entries are evidently $\mathsf{O}(p)$, we can conclude that the constants $\{C_j\}$ are suitable for $v = 1$.

- *Suppose that* $\alpha > 0$ *and* $\beta = 0$. Again let $C_{-1} = 0$. We can similarly compute

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

for $0 \leqslant w < 2\nu - \alpha$ and $0 < j \leqslant \alpha$. Again, the column vector with entries $\vartheta_w(D_\bullet)$ for $0 \leqslant w < 2\nu - \alpha$ is equal to $U(1, C_1, \ldots, C_\alpha)^T$, its first α entries are in $\mathsf{O}(p^{t+2})$, and the entry indexed α is

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

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

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

and, since $r = s + \mathsf{O}(p^t)$, we can replace r with s in the expression for $U_{w,j}$ when $j > 0$ to deduce that

$$\begin{aligned} U_{w,j} &= \textstyle\sum_v (-1)^{w-v}\binom{j+w-v-1}{w-v}\binom{s-\alpha+j}{v}\binom{s-\alpha+j-v}{j-v} + \mathsf{O}(p^t) \\ &= \textstyle\sum_{i>0} \binom{s-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} + \mathsf{O}(p^t) = \mathsf{O}(p^t). \end{aligned}$$

for $0 < w < 2\nu - \alpha$ and $j > 0$. Since $v_p(C_j) \geqslant 1$ for $1 \leqslant j \leqslant \alpha$, it follows that all subsequent entries of the resulting column vector are $\mathsf{O}(p^{t+1})$. Therefore the constants $\{C_j\}$ are suitable for $v = t + 1$.

- *Suppose that* $\alpha > 0$ *and* $\beta \in \{1, \dots, \alpha\}$. Let A be the $(\alpha+1) \times (\alpha+1)$ matrix with entries

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

for $0 \leqslant w, j \leqslant \alpha$. For $C_{-1} = 0$ this would be the matrix obtained from U^{sub} by dividing the first column by p, however this time we need to choose a nonzero C_{-1}. The matrix A is precisely the matrix such that

$$A(C_0, C_1/p, \dots, C_\alpha/p)^T = ((\vartheta_0(D_\bullet) - C_{-1})/p, \vartheta_1(D_\bullet)/p, \dots, \vartheta_\alpha(D_\bullet)/p)^T.$$

We have

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

so in particular A has integer entries. However, these expressions for the entries of A are not useful as we need to compute A up to precision $\mathsf{O}(p^{t+1})$. Recall that

$$\binom{X}{n}^\partial = \tfrac{\partial}{\partial X} \binom{X}{n}.$$

Let us also consider the $(\alpha+1) \times (\alpha+1)$ matrices S and N with integer entries

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

for $0 \leqslant w, j \leqslant \alpha$. Recall that $\epsilon = u_0 p^t$. Let us prove the following claim.

Approximation claim.

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

Proof of approximation claim. First let us look at the entries with $j > 0$.

Due to (c-g),

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

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

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

This holds true since the denominator $j!$ of $\binom{r-\alpha+j}{j}$ is coprime to p (see the note about approximating polynomials in $\mathbb{Z}_p[X]$ in section 2.4). Due to (c-g),

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

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

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

The first two lines are in $\mathsf{O}(\epsilon p)$ since

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

due to (c-a). The third line is also evidently in $\mathsf{O}(\epsilon p)$, which proves that

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

Now let us look at the entries with $j = 0$. In this case

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

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

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

The second line is in $\mathsf{O}(\epsilon p^2)$ since, due to (c-b) and (c-c),

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

Due to (c-b) and (c-c),

$$\textstyle\sum_{i>0}\left(\binom{r-\alpha-w}{i(p-1)-w} - \binom{s+\beta(p-1)-\alpha-w}{i(p-1)-w}\right)$$

is

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

For the first equality we use (c-b) to compute $\mathrm{S}_\star$. The $\mathsf{O}(\epsilon p^2)$ term in the second line comes from the fact that the terms

$$\mathsf{O}\big(t_{r-\alpha-j}p^2\big),\ \mathsf{O}\big(t_{s+\beta(p-1)-\alpha-j}p^2\big)$$

are congruent modulo p^{t+2}—we can show this by noting that $t_{r-\alpha-j}$ and

$t_{s+\beta(p-1)-\alpha-j}$ are congruent modulo p^t and using the explicit description of $\mathsf{O}(t_u p^2)$ in the proof of $(c\text{-}b)$. The second equality comes from the fact that $t_{r-\alpha-j} = \beta - \epsilon + \mathsf{O}(\epsilon p)$ and $t_{s+\beta(p-1)-\alpha-j} = \beta$. Consequently,

$$\begin{aligned} &p(A_{w,0} - S_{w,0} - \epsilon N_{w,0}) \\ &\quad = \epsilon p(-1)^w \tfrac{w!}{(s-\alpha)_{w+1}} \left(\tbinom{s+\beta(p-1)-\alpha}{w} - \tbinom{r-\alpha}{w} \right) + \mathsf{O}(\epsilon p^2) = \mathsf{O}(\epsilon p^2), \end{aligned}$$

just as we wanted to prove. □

Thus we have shown that

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

Let $B = B_\alpha$ be the $(\alpha+1) \times (\alpha+1)$ matrix defined in lemma 11. 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

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

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

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

which can be simplified to

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

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

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

Thus $\overline{Q}$ is the matrix M from lemma 16, and that lemma implies that there is a solution of

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

such that $z_0 \neq 0$. Then $\overline{u} = (z_0, \ldots, z_\alpha)^T$ is in $\ker \overline{BS} = \ker \overline{S}$ and

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

for some $\overline{v}$ (because the submatrix of $\overline{BS}$ consisting of the rows indexed $1, \ldots, \beta$ has full rank). So $(z_0, \ldots, z_\alpha)^T \in \ker \overline{S}$ lifts to a $u \in \ker S$, and that implies that

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

for any lift v of $\overline{v}$. Since $A = S + \epsilon N + \mathsf{O}(\epsilon p)$, if we write

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

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

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

Since the zeroth column of B is $(1, 0, \ldots, 0)^T$, we also have

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

Let us choose $C_{-1} = -\epsilon p$. Then $\vartheta_\alpha(D_\bullet) = \mathsf{O}(p^{t+2})$, which makes

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

We moreover have

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

for all $0 \leqslant w \leqslant \alpha$, and

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

for all $\alpha < w < 2\nu - \alpha$. Indeed, 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 still $A = S + \epsilon N + \mathsf{O}(p^{t+1})$. Therefore, since $A \equiv S \bmod \epsilon$ (as the entries of N are integers), and as all rows of S are linear combinations of the rows of BS indexed $1, \ldots, \beta$, it follows that every entry of $A(C_0, C_1/p, \ldots, C_\alpha/p)^T$ is $\mathsf{O}(\epsilon)$.[1] This means that the constants $\{C_j\}$ are suitable for $v = t + 1$.

Therefore we can always find suitable constants $\{C_j\}$, and that concludes the proof of proposition 26. ∎

[1] Note that it is crucial here that the entries of N be integers. In this case they are since all equations in the proof of the approximation claim hold true for $w < s - \alpha$. If $w \geqslant s - \alpha$ then the equation for $N_{w,j}$ is different (as, for instance, a certain alternating sum is not $(-1)^w \frac{w!}{(s-\alpha)_{w+1}}$). This is one of the places where the proof breaks down if $s < 2\nu$.

5.4 Proof of proposition 27

Let $\alpha \in \{0, \dots, \nu-2\}$ and let us consider $\widehat{N}_\alpha$. The task is to show that if $\alpha > \max\{\nu - t - 1, \beta\}$ then none of the infinite-dimensional factors of $\overline{\Theta}_{k,a}$ are quotients of $\widehat{N}_\alpha$. Note that the condition on α implies both $\alpha > \beta$ and

$$t \geqslant \nu - \alpha > v_p(a) - \alpha.$$

Let us apply part (3) of corollary 24 with v chosen arbitrarily in the open interval $(v_p(a) - \alpha, t)$ and

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

for some constants $C_1^*, \dots, C_\alpha^*$ yet to be chosen. We need to show that the constants $\{C_j\}$ are suitable, i.e. that the conditions of corollary 24 are satisfied. Clearly

$$v_p(a) - \alpha < v \leqslant v_p(C_{-1})$$

and $C_0 = \mathsf{O}(p)$. Moreover,

$$\begin{aligned} \textstyle\sum_{l=1}^{\alpha} C_l\binom{r-\alpha+l}{l} &= \textstyle\sum_{l=1}^{\alpha}(-1)^{\alpha-l}\binom{s-\alpha+1}{\alpha-l}\binom{s-\alpha-\beta+l}{l} + \mathsf{O}(p) \\ &= (-1)^{\alpha}\binom{\beta}{\alpha} + (-1)^{\alpha+1}\binom{s-\alpha+1}{\alpha} + \mathsf{O}(p) \\ &= (-1)^{\alpha+1}\binom{s-\alpha+1}{\alpha} + \mathsf{O}(p). \end{aligned}$$

The third equality follows from the fact that $\alpha > \beta$. Since

$$p + \alpha - 1 > s > 2\alpha - 2$$

for $\alpha > 0$, and $\binom{s-\alpha+1}{\alpha} = 1$ for $\alpha = 0$, it follows that

$$\textstyle\sum_{l=1}^{\alpha} C_l\binom{r-\alpha+l}{l} \in \mathbb{Z}_p^\times.$$

Thus we only need to verify the most delicate condition, that

$$v \leqslant v_p(\vartheta_w(D_\bullet))$$

for $0 \leqslant w < 2\nu - \alpha$. By $(c\text{-}a)$ and $(c\text{-}g)$, if

$$L_1(r) := \sum_{i>0} \binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w}$$

then $L_1(r) = L_1(s + \beta(p-1)) + \mathsf{O}(\epsilon)$ for $0 \leqslant w < 2\nu - \alpha$. So in order to verify the last condition it is enough to show that

$$L_2(s) := \sum_{j=1}^{\alpha} \left((-1)^{\alpha-j}\binom{s-\alpha+1}{\alpha-j} + pC_j^*\right)\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j} = \mathsf{O}(p^v) \qquad (5.1)$$

for all $i \in \{1, \ldots, \beta\}$. We have

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

We also have

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

The second equality follows from Vandermonde's convolution formula. The third equality follows from the assumptions that $i > 0$ and $\alpha > \beta$. So (5.1) is true modulo p, and we can transform (5.1) into the matrix equation

$$\left(\binom{s+\beta(p-1)-\alpha+j}{i(p-1)+j}\right)_{1\leqslant i\leqslant\beta,\, 1\leqslant j\leqslant\alpha} (C_1^*, \ldots, C_\alpha^*)^T = (w_1, \ldots, w_\beta)^T$$

for some $w_1, \ldots, w_\beta \in \mathbb{Z}_p$. This matrix equation always has a solution since the left $\beta \times \beta$ submatrix of the reduction modulo p of the matrix

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

is upper triangular with units on the diagonal. Therefore we can indeed always choose the constants $C_1^*, \ldots, C_\alpha^*$ in a way that $v \leqslant v_p(\vartheta_w(D_\bullet))$ for $0 \leqslant w < 2\nu - \alpha$. Then all conditions of part (3) of corollary 24 are satisfied, which concludes the proof of proposition 27. ∎

Propositions 26 and 27 are already sufficient to compute $\overline{\Theta}_{k,a}$, since they imply that $\overline{\Theta}_{k,a}$ must be a quotient of $\widehat{N}_\alpha$, where $\alpha = \nu - 1$ if $k \in \mathscr{R}_0^{s,\nu}$ and $\alpha = \max\{\nu - t - 1, \beta\}$ if $k \in \mathscr{R}_{\beta,t}^{s,\nu}$. Let us show that in fact the surjective map

$$\widehat{N}_\alpha \twoheadrightarrow \overline{\Theta}_{k,a}$$

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

Proposition 28. *If $k \in \mathscr{R}_0^{s,\nu}$ then the surjective map*

$$\widehat{N}_{\nu-1} \twoheadrightarrow \overline{\Theta}_{k,a}$$

factors through $\operatorname{ind}_{KZ}^G \operatorname{quot}(\nu - 1)$.

Proof. Let $\alpha = \nu - 1$. Note that since $k \in \mathscr{R}_0^{s,\nu}$ we have

$$\beta \in \{\nu - 1, \dots, p - 1\}.$$

Let us apply part (2) of corollary 24 with $v = 0$ and some constants

$$C_{-1}, C_0, \dots, C_\alpha$$

such that $C_{-1} = \binom{\beta}{\alpha}$ and $C_0 = 0$. The conditions that need to be satisfied in order for the corollary to be applicable are $v_p(\vartheta_w(D_\bullet)) > 0$ for $0 \leqslant w < \alpha$, and $v_p(\vartheta') > 0$. Let us consider the matrix $A = (A_{w,j})_{0 \leqslant w,j \leqslant \alpha}$ that has integer entries

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

Then $v_p(\vartheta') > 0$ is equivalent to $\vartheta_\alpha(D_\bullet) = C_{-1} + \mathsf{O}(p) = \binom{\beta}{\alpha} + \mathsf{O}(p)$, so the two equations we want to show are equivalent to

$$A(0, C_1, \dots, C_\alpha)^T = \left(-\tbinom{\beta}{\alpha}, 0, \dots, 0, \tbinom{\beta}{\alpha}\right)^T + \mathsf{O}(p).$$

By (c-g) we have

$$\overline{A}_{w,j} = F_{w,j}(r,s),$$

where $F_{w,j}(z,\psi) \in \mathbb{F}_p[z,\psi]$ is the polynomial defined in lemma 13. Then the conclusion of that lemma is that

$$\overline{A}(0,C_1,\dots,C_\alpha)^T = \left(-\tbinom{\beta}{\alpha},0,\dots,0,\tbinom{\beta}{\alpha}\right)^T$$

with

$$C_j = (-1)^j \tbinom{s-\alpha+1}{\alpha-j}$$

for $j \in \{1,\dots,\alpha\}$. Thus these choices for $C_{-1},C_0,\dots,C_\alpha$ are suitable, and we can apply part (2) of corollary 24 with $v=0$ and conclude that $\operatorname{ind}_{KZ}^{G}\operatorname{sub}(\alpha)$ is trivial modulo $\mathscr{I}_a$. ∎

Proposition 29. *If $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ then the surjective map*

$$\widehat{N}_{\max\{\nu-t-1,\beta\}} \twoheadrightarrow \overline{\Theta}_{k,a}$$

factors through $\operatorname{ind}_{KZ}^{G}\operatorname{quot}(\max\{\nu-t-1,\beta\})$.

Proof. Let $\alpha = \max\{\nu-t-1,\beta\}$. Let us apply part (2) of corollary 24 with $v=t$ and

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

We need to show that the constants $\{C_j\}$ are suitable, i.e. that the conditions of corollary 24 are satisfied. Clearly $v_p(C_{-1}) = t < v_p(a) - \alpha$. We also need to show that $t < v_p(\vartheta_w(D_\bullet))$ for $0 \leqslant w < \alpha$ and $t < v_p(\vartheta')$ and $t \leqslant v_p(\vartheta_w(D_\bullet))$ for $\alpha \leqslant w < 2\nu - \alpha$. Let us consider the matrix $A = (A_{w,j})_{0\leqslant w,j\leqslant\alpha}$ that has integer entries

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

If we consider the approximation claim in the proof of proposition 26 and multiply the first column by p, we get

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

where

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

Exactly as in the proof of proposition 26 we can deduce the three conditions we need to show as long as

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

Let $B = B_\alpha$ be the $(\alpha+1)\times(\alpha+1)$ matrix defined in lemma 11. 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

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

when $w \in \{1,\ldots,\beta\}$. Moreover,

$$B_{i,w} = [(i,w)=(0,0)] + \textstyle\sum_{l=1}^{\alpha}(-1)^i\binom{l}{i}\binom{l-1}{l-w} + \mathsf{O}(p).$$

By using this formula we can compute that

$$B(-1,0,\ldots,0,1)^T = \left(0,-\binom{\alpha}{1},\ldots,(-1)^\alpha\binom{\alpha}{\alpha}\right)^T + \mathsf{O}(p),$$

and therefore if $\overline{R}$ 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 $\overline{BS}$ and then discarding the zeroth row and the zeroth column, the condition that needs

to be satisfied is equivalent to the claim that

$$\overline{R}(C_1,\dots,C_\alpha)^T = \left(-(1-[1\leqslant\beta])\tbinom{\alpha}{1},\dots,(-1)^\alpha(1-[\alpha\leqslant\beta])\tbinom{\alpha}{\alpha}\right)^T. \quad (5.2)$$

The matrix $\overline{R}$ is the lower right $\alpha\times\alpha$ submatrix of the matrix $\overline{Q}$ defined in the proof of proposition 26, where we compute that

$$\overline{R}_{i-1,j-1} = \tbinom{s-\alpha-\beta+j}{j-i}\cdot\begin{cases}\tbinom{\beta}{i} & \text{if } i\in\{1,\dots,\beta\},\\ -\tbinom{\beta}{i}^{\partial} & \text{otherwise,}\end{cases}$$

for $i,j\in\{1,\dots,\alpha\}$. We have

$$\begin{aligned}&\textstyle\sum_{j=1}^{\alpha}(-1)^{\alpha+\beta+j}\alpha\tbinom{\alpha-1}{\beta}\tbinom{s-\alpha+1}{\alpha-j}\tbinom{s-\alpha-\beta+j}{j-i}\\ &\quad=\textstyle\sum_j(-1)^{\alpha+\beta+i}\alpha\tbinom{\alpha-1}{\beta}\tbinom{s-\alpha+1}{\alpha-j}\tbinom{\alpha+\beta-s-i-1}{j-i}\\ &\quad=(-1)^{\alpha+\beta+i}\alpha\tbinom{\alpha-1}{\beta}\tbinom{\beta-i}{\alpha-i}.\end{aligned}$$

If $i\in\{1,\dots,\beta\}$ then the last expression is zero, and if $i\in\{\beta+1,\dots,\alpha\}$ then it is

$$(-1)^\beta\alpha\tbinom{\alpha-1}{\beta}\tbinom{\alpha-\beta-1}{i-\beta-1} = (-1)^\beta i\tbinom{i-1}{\beta}\tbinom{\alpha}{i} = (-1)^i\tbinom{\alpha}{i}\cdot\left(-\tbinom{\beta}{i}^{\partial}\right)^{-1},$$

which implies (5.2). Consequently we can apply part (2) of corollary 24 with $v=t$ and conclude that $\operatorname{ind}_{KZ}^{G}\operatorname{sub}(\alpha)$ is trivial modulo $\mathscr{I}_a$. ∎

6

Proof of theorem 6

The proof of theorem 6 is very similar to the proof of theorem 5. The major difference is that we apply corollary 25 instead of corollary 24 since $v_p(a)$ is an integer, which means that $\overline{\Theta}_{k,a}$ is reducible in some cases.

6.1 Running assumptions

We make the same assumptions as in chapter 5. We assume that

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

for some $\beta \in \{0, \ldots, p-1\}$ and $u_0 \in \mathbb{Z}_p^\times$ and $t \in \mathbb{Z}_{>0}$, that $\epsilon = u_0 p^t$, that $v_p(a) = \nu - 1$ for some $\nu \in \{1, \ldots, \frac{p-1}{2}\}$, that $s \in \{2\nu, \ldots, p-2\}$, and that $k > p^{100}$ (and consequently $r > p^{99}$).

6.2 Theorem 6 is equivalent to proposition 30

Let $\mu = \lambda$ if $k \in \mathscr{R}_0^{s,\nu}$ and $\mu = \lambda_{\beta,t}$ if $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ (in the notation of theorem 2). Let $\gamma = \nu - 1$ if $k \in \mathscr{R}_0^{s,\nu}$ and $\gamma = \max\{\nu - t - 1, \beta\}$ if $k \in \mathscr{R}_{\beta,t}^{s,\nu}$. Let us first show the equivalence between theorem 6 and the following proposition.

Proposition 30. *Let either $k \in \mathscr{R}_0^{s,\nu}$, or $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ and $t < \nu - \beta - 1$.*

1. $(T - \mu^{-1})(\mathrm{ind}_{KZ}^G \mathrm{quot}(\gamma - 1))$ *is trivial modulo $\mathscr{I}_a$.*

2. $(T - \mu)(\mathrm{ind}_{KZ}^G \mathrm{sub}(\gamma))$ *is trivial modulo $\mathscr{I}_a$.*

3. $\mathrm{ind}_{KZ}^G \mathrm{sub}(\gamma - 1)$ *is trivial modulo $\mathscr{I}_a$.*

4. $\mathrm{ind}_{KZ}^G \mathrm{quot}(\gamma)$ *is trivial modulo $\mathscr{I}_a$.*

Proof that theorem 6 is equivalent to proposition 30. First let us assume that proposition 30 is true. In the setting of theorem 5, propositions 26, 27, 28, and 29 show that if $k \in \mathscr{R}_0^{s,\nu}$ then $\overline{\Theta}_{k,a}$ is a quotient of $\mathrm{ind}_{KZ}^G \mathrm{quot}(\nu - 1)$, and if $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ then $\overline{\Theta}_{k,a}$ is a quotient of $\mathrm{ind}_{KZ}^G \mathrm{quot}(\max\{\nu - t - 1, \beta\})$. Their proofs are based on corollary 24. They amount to considering the element of $\mathrm{im}(T - a)$ coming from equation 4.3 in lemma 23, and noting that the term with dominant valuation is either H or

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

depending on how t compares to $v_p(a) - \alpha$. In the setting of theorem 6 we can apply the analogous corollary 25 to conclude that any infinite-dimensional factor of $\overline{\Theta}_{k,a}$ must be a quotient of one of

$$\mathrm{ind}_{KZ}^G \mathrm{sub}(\gamma - 1),\ \mathrm{ind}_{KZ}^G \mathrm{quot}(\gamma - 1),\ \mathrm{ind}_{KZ}^G \mathrm{sub}(\gamma),\ \mathrm{ind}_{KZ}^G \mathrm{quot}(\gamma),$$

where for convenience we define $\mathrm{sub}(-1)$ and $\mathrm{quot}(-1)$ to be the trivial representation. The key reason why the proofs of propositions 26 and 27 copy verbatim to prove this is that outside of these subquotients the valuations t and

$v_p(a) - \alpha$ never match, so again exactly one of the two aforementioned terms is dominant. The only subtlety when copying the proofs of propositions 26 and 27 is that we do not know whether $\mathscr{I}_a$ contains $1 \bullet_{KZ,\overline{\mathbb{Q}}_p} x^{\nu-1}y^{r-\nu+1}$. This ultimately does not present a problem since when working with $\widehat{N}_{\nu-1}$ we always assume that $C_0 = 0$. As the proofs of propositions 26 and 27 work here nearly without modification except for replacing corollary 24 with 25, we omit the full details of the arguments. Proposition 30 then implies that any infinite-dimensional factor of $\overline{\Theta}_{k,a}$ must be a quotient of one of

$$\operatorname{ind}_{KZ}^{G} \operatorname{quot}(\gamma - 1)/(T - \mu^{-1}),\ \operatorname{ind}_{KZ}^{G} \operatorname{sub}(\gamma)/(T - \mu),$$

and together with theorem 4 they completely determine $\overline{\Theta}_{k,a}$.

The converse, that theorem 5 implies proposition 30, is clear since theorem 5 completely determines $\overline{\Theta}_{k,a}$. ∎

6.3 Proof of proposition 30

(1) Suppose first that $k \in \mathscr{R}_0^{s,\nu}$. Let $c = (c_1, \dots, c_\alpha)$ be as in lemma 15, and let us make the substitutions $X = r - \alpha$ and $Y = s - \alpha$. We apply part (6) of corollary 25 with $v = 1$. We choose $C_{-1} = 0$ and $C_0 = 1$ and $C_j = \frac{c_j p}{(s-\alpha)_\alpha}$ for $j \in \{1, \dots, \alpha\}$. In the proof of proposition 26 we show that for these constants we have

$$\begin{aligned} \vartheta' &= \tfrac{(s-r)_{\nu-1}}{(s-\nu+2)_{\nu-1}} p + \mathsf{O}(p^2), \\ 1 &\leqslant v_p(\vartheta_w(D_\bullet)) \text{ for } \alpha \leqslant w < 2\nu - \alpha, \\ 1 &< v_p(\vartheta_w(D_\bullet)) \text{ for } 0 \leqslant w < \alpha. \end{aligned}$$

Moreover, since $C_1, \dots, C_\alpha = \mathsf{O}(p)$ we have $\check{C} = \mathsf{O}(p)$, and

$$\mu = \tfrac{(s-\nu+2)_{\nu-1} a}{(s-r)_{\nu-1} p^\nu} = \tfrac{a}{C_0^{-1} \vartheta' p^{\nu-2}}.$$

Therefore the conditions needed to apply part (6) of corollary 25 (i.e. the three conditions

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

in addition to the two extra conditions on $\check{C}$ and C_0 in part (6) of the corollary) are satisfied and we can conclude that

$$(T - \mu^{-1})(\mathrm{ind}_{KZ}^G \mathrm{quot}(\gamma - 1))$$

is trivial modulo $\mathscr{I}_a$. If $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ and $t < \nu - \beta - 1$ then the argument is similar: we choose $v = t + 1$ and the same constants $\{C_j\}$ as in the third bullet point (if $\beta = 0$) or the fourth bullet point (if $\beta \in \{1, \ldots, \gamma - 1\}$) of the proof of proposition 26. In the former case

$$\vartheta' = \tfrac{(s-r)_{\alpha+1}}{(s-\alpha)_{\alpha+1}} p + \mathsf{O}(p^{t+2}),$$

and in the latter case

$$\vartheta' = \epsilon Q_{0,0} p + \mathsf{O}(p^{t+2}).$$

In both cases

$$\mu = \tfrac{a}{C_0^{-1} \vartheta' p^{\nu - t - 2}}$$

and the conditions needed to apply part (6) of corollary 25 are satisfied, so again we can conclude that

$$(T - \mu^{-1})(\mathrm{ind}_{KZ}^G \mathrm{quot}(\gamma - 1))$$

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

(2) Suppose first that $k \in \mathscr{R}_0^{s,\nu}$. We use the constants

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

We can show just as in the proof of proposition 28 that these constants satisfy all of the conditions needed to apply part (7) of corollary 25 with $v = 0$. Moreover, we have

$$\begin{aligned} \check{C} &= \textstyle\sum_{j=1}^{\nu-1}(-1)^{\nu-j-1}\binom{s-\nu+2}{\nu-j-1}\binom{r-\nu+j+1}{j} - (-1)^{\nu-1}\binom{s-r}{\nu-1} + \mathsf{O}(p) \\ &= (-1)^{\nu-1}\textstyle\sum_{j=1}^{\nu-1}\binom{s-\nu+2}{\nu-j-1}\binom{\nu-r-2}{j} - (-1)^{\nu-1}\binom{s-r}{\nu-1} + \mathsf{O}(p) \\ &= (-1)^{\nu}\binom{s-\nu+2}{\nu-1} + \mathsf{O}(p). \end{aligned}$$

Thus

$$-\frac{\check{C}ap^{1-\nu}}{C_{-1}} = \frac{\binom{s-\nu+2}{\nu-1}a}{\binom{s-r}{\nu-1}p^{\nu-1}} = \mu,$$

so part (7) of corollary 25 implies that

$$(T - \mu)(\operatorname{ind}_{KZ}^{G} \operatorname{sub}(\gamma))$$

is trivial modulo $\mathscr{I}_a$. If $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ and $t < \nu - \beta - 1$ then the argument is similar: we choose $v = t$ and the constants

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

as in the proof of proposition 29. Again all of the conditions needed to apply

part (7) of corollary 25 with $v = t$ are satisfied and

$$\begin{aligned}\check{C} &= (-1)^{\beta+\gamma}\gamma\tbinom{\gamma-1}{\beta}\textstyle\sum_{j=1}^{\gamma}(-1)^j\tbinom{s-\gamma+1}{\gamma-j}\tbinom{r-\gamma+j}{j} + \mathsf{O}(p)\\ &= (-1)^{\beta+\gamma}\gamma\tbinom{\gamma-1}{\beta}\textstyle\sum_{j=1}^{\gamma}\tbinom{s-\gamma+1}{\gamma-j}\tbinom{\gamma-r-1}{j} + \mathsf{O}(p)\\ &= (-1)^{\beta+\gamma}\gamma\tbinom{\gamma-1}{\beta}\left(\tbinom{s-r}{\gamma} - \tbinom{s-\gamma+1}{\gamma}\right) + \mathsf{O}(p)\\ &= (-1)^{\beta+\gamma+1}\gamma\tbinom{\gamma-1}{\beta}\tbinom{s-\gamma+1}{\gamma} + \mathsf{O}(p).\end{aligned}$$

The last equality follows from the fact that $\binom{s-r}{\gamma} = \mathsf{O}(p)$. Thus

$$-\frac{\check{C}a}{C_{-1}p^{\nu-t-1}} = \frac{(-1)^{\beta+\gamma}\gamma\binom{\gamma-1}{\beta}\binom{s-\gamma+1}{\gamma}a}{\epsilon p^{\nu-t-1}} = \mu,$$

so part (7) of corollary 25 implies that

$$(T-\mu)(\operatorname{ind}_{KZ}^{G}\operatorname{sub}(\gamma))$$

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

(3) This is very similar to part (2) of this proposition: if $k \in \mathscr{R}_0^{s,\nu}$ then we use part (2) of corollary 25 just as in the proof of proposition 28, and if $k \in \mathscr{R}_{\beta,t}^{s,\nu}$ and $t < \nu - \beta - 1$ then we use part (2) of corollary 25 just as in the proof of proposition 29. We omit the full details.

(4) We apply part (8) of corollary 25 with the same constants as in the proof of part (2) of this proposition—since $\check{C} \in \mathbb{Z}_p^{\times}$ all of the necessary conditions are satisfied and we can conclude that $\operatorname{ind}_{KZ}^{G}\operatorname{quot}(\gamma)$ is trivial modulo $\mathscr{I}_a$. ∎

7

Proof of theorem 7

Theorem 7 is the most involved among the main results in this thesis. We prove it 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.

7.1 Running assumptions

We assume that

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

for some $\beta \in \{0, \dots, p-1\}$ and $u_0 \in \mathbb{Z}_p^\times$ and $t \in \mathbb{Z}_{>0}$, and we write $\epsilon = u_0 p^t$. As theorem 5 implies theorem 7 for $s \geqslant 2\nu$, we may assume that

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

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

7.2 Propositions 31–39 imply theorem 7

In this section we give a list of nine propositions, and show that their union implies theorem 7.

Proposition 31. *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 32. *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 33. *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 34. *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 35. *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 36. *If $\beta \in \{1, \ldots, \frac{s}{2} - 1\}$ and $t > \nu - \frac{s}{2} - 2$ then*

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

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

Proposition 37. *If $\beta \in \{1, \ldots, \frac{s}{2} - 1\}$ and $t = \nu - \frac{s}{2}$ then*

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

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

Proposition 38. *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 39. *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 31–39 imply theorem 7. Let us assume that $\overline{\Theta}_{k,a}$ is reducible with the goal of reaching a contradiction. The classification given by theorem 4 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 $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\alpha_1)$ and $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\alpha_2)$ then

$$\alpha_1 + \alpha_2 \equiv_{p-1} s + 1.$$

2. If the two representations are $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\alpha_1)$ and $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\alpha_2)$ then

$$\alpha_1 - \alpha_2 \equiv_{p-1} 1.$$

3. If the two representations are $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\alpha_1)$ and $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\alpha_2)$ then

$$\alpha_1 + \alpha_2 \equiv_{p-1} s - 1.$$

The facts that

$$\begin{aligned} \alpha_1 + \alpha_2 &\in \{0, \ldots, 2\nu - 2\} \subseteq \{0, \ldots, p-3\}, \\ \alpha_1 - \alpha_2 &\in \{1 - \nu, \ldots, \nu - 1\} \subseteq \{-\tfrac{p-3}{2}, \ldots, \tfrac{p-3}{2}\}, \\ s &\in \{2, \ldots, 2\nu - 2\} \subseteq \{2, \ldots, p-3\} \end{aligned}$$

imply that the following classification is true as well.

1. If the two representations are $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\alpha_1)$ and $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\alpha_2)$ then

$$\alpha_1 + \alpha_2 = s + 1.$$

2. If the two representations are $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\alpha_1)$ and $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\alpha_2)$ then

$$\alpha_1 = \alpha_2 + 1.$$

3. If the two representations are $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\alpha_1)$ and $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\alpha_2)$ then

$$\alpha_1 + \alpha_2 = s - 1.$$

This classification and propositions 31, 32, 33, 34, and 35 together imply that one of the two representations must be either $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\frac{s}{2})$ or $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(\frac{s}{2})$,

and in that case the other representation is either

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

(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

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

(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 $\mathrm{ind}_{KZ}^{G}\,\mathrm{quot}(0)$, or $\nu \leqslant 2$ in which case $\overline{V}_{k,a}$ is known to be irreducible. Propositions 34, 36, 37, 38, and 39 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. ∎

7.3 Proof of proposition 31

First suppose that $\beta \geqslant \alpha$. We apply part (2) of corollary 24 with $v = 0$ and

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

Since

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

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

$$\sum_{j=1}^{\alpha}(-1)^{\alpha-j}\binom{s-\alpha+1}{\alpha-j}\sum_{i>0}\binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = (-1)^{\alpha}([w=\alpha]-[w=0])\binom{s-r}{\alpha} + \mathsf{O}(p) \quad (7.1)$$

for $0 \leqslant w \leqslant \alpha$. Let $F_{w,j}(z,\psi) \in \mathbb{F}_p[z,\psi]$ denote the polynomial defined in lemma 13. Since

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

by (c-g), the conclusion of that lemma when evaluated at $z = r$ and $\psi = s$ implies (7.1). Thus if $\beta \geqslant \alpha$ then we can apply part (2) of corollary 24 and conclude that $\mathrm{ind}_{KZ}^{G} \mathrm{sub}(\alpha)$ is trivial modulo $\mathscr{I}_a$.

Suppose now that $\beta \in \{0, \dots, \alpha - 1\}$. If $t > v_p(a) - \alpha$ then the proof of proposition 26 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 24 with $v = t$ and

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

for some constants $C_1^{*}, \dots, C_\alpha^{*}$ 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 24 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 proposition 26 (the approximation claim on page 97) we can show that

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

where

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

We still have equation 7.1 since the constants are the same, and since

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

we have

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

Let $B = B_\alpha$ be the $(\alpha+1) \times (\alpha+1)$ matrix defined in lemma 11. 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

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

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

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

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 proposition 26 we note that S has rank β and therefore we can choose $C_1^*, \ldots, C_\alpha^*$ in a way that $(C_0, \ldots, C_\alpha)^T \in \ker BS$. 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

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

which is itself equivalent to

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

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 proposition 26 (where it is shown that $\overline{Q}$ is equal to the matrix M from lemma 16) and is therefore upper triangular with units on the diagonal. Thus we can apply part (2) of corollary 24 with $v = t$ and conclude that $\operatorname{ind}_{KZ}^G \operatorname{sub}(\alpha)$ is trivial modulo $\mathscr{I}_a$. ∎

7.4 Proof of proposition 32

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

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

We apply part (1) of corollary 24 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

$$\textstyle\sum_{j=0}^{\alpha} C_j \sum_{0<i(p-1)<r-2\alpha} \binom{r-\alpha+j}{i(p-1)+j}\binom{i(p-1)}{w} = -[w=0]\binom{s-r-1}{\alpha+1} + \mathsf{O}(p) \quad (7.2)$$

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

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

By (c-g),

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

so the conclusion of lemma 14 evaluated at $z = r$ implies (7.2). Thus we can apply part (1) of corollary 24 and conclude that $\widehat{N}_\alpha$ is trivial modulo $\mathscr{I}_a$. ∎

7.5 Proof of proposition 33

First let us assume that $\beta \in \{0, \ldots, \alpha\}$. If we attempt to copy the proof of proposition 26 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—see footnote 1). To be more specific, the equation for $N_{w,0}$ in this setting is

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

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

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

On the other hand,

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

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

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

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

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

What this means is that if we proceed with the proof of proposition 26 and apply lemma 23 with the constants $(C_{-1}, C_0, \ldots, C_\alpha)$ 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 $\mathrm{im}(T - a)$ 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 23. 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 $T(\mathrm{ind}_{KZ}^G \mathrm{quot}(\alpha))$ 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 23.

Now let us assume that $\beta > \alpha$. We use the constants constructed in the second bullet point of the proof of proposition 26, and we apply lemma 23.

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 $\mathrm{im}(T-a)$ 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 23. 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 $\beta \in \{\alpha+1, \ldots, s-\alpha\}$ 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 $\mathscr{I}_a$. ∎

7.6 Proof of proposition 34

By proposition 32 we may assume that $\beta \notin \{1, \ldots, \alpha+1\}$, and by proposition 33 we may assume that $\beta \neq \alpha+1$. If $\alpha \neq \frac{s}{2}$ and $\beta \in \{1, \ldots, s-\alpha\}$ and $s-\alpha < v_p(a)-t$ then the claim follows from proposition 33. Thus it is enough to show that if $\beta \in \{1, \ldots, \alpha\}$ then

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

is trivial modulo $\mathscr{I}_a$. If $\alpha < v_p(a)-t$ we apply part (1) of corollary 24, and if $\alpha > v_p(a)-t$) we apply part (5) of corollary 24. In both cases we choose

$v = t$ and

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

Since $v_p(C_{-1}) = t$ and $C_0 = 1$, the conditions we need to verify in order to be able to apply corollary 24 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

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

As in the proof of the approximation claim on page 97 (and as in proposition 31) we can show that

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

where

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

The first condition follows from an argument similar to the one in the fourth bullet point in the proof of proposition 26: 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 proposition 26, the second and third conditions follow if

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

Let $B = B_\alpha$ be the $(\alpha+1)\times(\alpha+1)$ matrix defined in lemma 11. 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 $i \in \{1,\ldots,\beta-1\}$. Let $\overline{R}$ denote the $(\alpha+1)\times(\alpha+1)$ matrix over $\mathbb{F}_p$ obtained from $\overline{BN}$ by replacing the rows indexed $1,\ldots,\beta-1$ with the corresponding rows of $\overline{BS}$. As in the proof of proposition 26 we can compute

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

Thus lemma 17 implies that

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

So the conditions we need to apply corollary 24 are indeed satisfied, and that completes the proof. ∎

7.7 Proof of proposition 35

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 proposition 26 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

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

which is indeed the case since $s_\alpha - \alpha = p-1+s-\alpha \geqslant 2\nu-\alpha$. So there is an analogous version of proposition 26, and we can conclude the desired result—as the proof of proposition 26 works nearly without modification, we omit the full details of the arguments. ∎

7.8 Proof of proposition 36

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 24 with v chosen in the open interval $(v_p(a)-\alpha, t)$ and

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

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

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

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

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

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

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

in a way that $\vartheta_w(D_\bullet) = 0$ for $0 \leqslant w < 2\nu - \alpha$ similarly as in the proof of proposition 26 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 24 are satisfied and we can conclude that $\widehat{N}_{s/2+1}$ is trivial modulo $\mathscr{I}_a$. ∎

7.9 Proof of proposition 37

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 33 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 36 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 $x_2 \in \mathrm{im}(T - a)$. 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 proposition 26 we can apply part (1) of corollary 24 and conclude that $\widehat{N}_\alpha$ is trivial modulo $\mathscr{I}_a$ as long as $(\epsilon, 0, \ldots, 0)^T$ is in the image of the matrix $A = (A_{w,j})_{0 \leqslant w,j \leqslant \alpha}$ that has integer entries

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

with S and N as in proposition 31. 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 $x_3 \in \mathrm{im}(T-a)$. This in turn by proposition 36 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 $x_4 \in \mathrm{im}(T-a)$. Here we use the fact that the valuation of the constant C_1 from proposition 36 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 $x_5 \in \mathrm{im}(T-a)$. 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 20. 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

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

from the proof of lemma 22, and we can translate this back to adding the extra column

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

to A. As in proposition 31 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 proposition 26 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 34 we can find that

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

with

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

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 24 are satisfied and we can conclude that $\widehat{N}_{s/2-1}$ is trivial modulo $\mathscr{I}_a$. ∎

7.10 Proof of proposition 38

Let us write $\alpha = \frac{s}{2} + 1$. The reason why the proof of proposition 36 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 23 is

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

for the constant

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

which has valuation $v_p(a) - \alpha + 1$. As in proposition 37 it is crucial here that $C_1 = \mathsf{O}(p)$. Just as in the proof of proposition 36 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 $C_1 = \mathsf{O}(p)$ and

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

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

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

This follows from lemma 19. So the conditions we need to apply corollary 24 are satisfied and we can conclude that $\widehat{N}_{s/2+1}$ is trivial modulo $\mathscr{I}_a$. ∎

7.11 Proof of proposition 39

Let us write $\alpha = \frac{s}{2} + 1$. This time the proofs of both parts (36) and (38) 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

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

Let $\overline{R}$ be the matrix constructed in proposition 34. Then just as in the proof of proposition 36 we can show that $\check{C} = \mathsf{O}(p)$, and just as in the proof of proposition 31 we can show that the dominant term coming from equation (4.3) in lemma 23 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 $\operatorname{ind}_{KZ}^G \operatorname{sub}(\frac{s}{2}+1)$ is trivial modulo $\mathscr{I}_a$) as long as

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

This follows from lemma 18. Thus the conditions we need to apply corollary 24 are satisfied and we can conclude that $\mathrm{ind}_{KZ}^{G}\,\mathrm{sub}(\frac{s}{2}+1)$ is trivial modulo $\mathscr{I}_a$. ∎

Bibliography

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

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

[Ber12] ———, *Local constancy for the reduction mod p of two-dimensional crystalline representations*, Bulletin of the London Mathematical Society **44** (2012), no. 3, 451–459.

[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.

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

[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.

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

[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.

[BG16] ———, *Slopes of modular forms*, Families of Automorphic Forms and the Trace Formula (2016), 93–109.

[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.

[Gou01] Fernando Q. Gouvêa, *Where the slopes are?*, Journal of the Ramanujan Mathematical Society **16** (2001), no. 1, 75–99.

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

[Roz] ———, *On the locus of 2-dimensional crystalline representations with a given reduction modulo p*, preprint. `https://arxiv.org/abs/1705.01060`.