Boundedness results for finite flat group schemes over discrete valuation rings of mixed characteristic

Adrian Vasiu and Thomas Zink

November 10, 2009

Abstract. Let p be a prime. Let V be a discrete valuation ring of mixed characteristic $(0, p)$ and index of ramification e. Let $f : G \to H$ be a homomorphism of finite flat commutative group schemes of p power order over V whose generic fiber is an isomorphism. We bound the kernel and the cokernel of the special fiber of f in terms of e. For $e < p - 1$ this reproves a result of Raynaud. As an application we obtain an extension theorem for homomorphisms of truncated Barsotti–Tate groups which strengthens Tate's extension theorem for homomorphisms of p-divisible groups. In particular, our method provides short new proofs of the theorems of Tate and Raynaud.

Key words: discrete valuation rings, group schemes, truncated Barsotti–Tate groups, p-divisible groups, and Breuil modules.

MSC 2000: 11G10, 11G18, 11S25, 11S31, 14F30, 14G35, 14K10, and 14L05.

1 Introduction

Let p be a rational prime. Let V be a discrete valuation ring of mixed characteristic $(0, p)$. Let K be the field of fractions of V. Let k be the residue field of V. Let e be the index of ramification of V. Let G and H be two finite flat commutative group schemes of p power order over V. For $n \in \mathbb{N}^*$, let $G\lceil p^n \rceil$ be the schematic closure of $G_K[p^n]$ in G. The goal of the paper is to prove the following theorem and to get several applications of it.

Theorem 1 *There exists a non-negative integer s that depends only on V and that has the following property.*

For each homomorphism $f : G \to H$ whose generic fiber $f_K : G_K \to H_K$ is an isomorphism, there exists a homomorphism $f' : H \to G$ such that $f' \circ f = p^s \mathrm{id}_G$ and $f \circ f' = p^s \mathrm{id}_H$ and therefore the special fiber homomorphism $f_k : G_k \to H_k$ has a kernel and a cokernel annihilated by p^s. If moreover H is a truncated Barsotti–Tate group of level $n > s$, then the natural homomorphism $f[p^{n-s}] : G[p^{n-s}] \to H[p^{n-s}]$ is an isomorphism.

The number s admits computable upper bounds in terms only of e. For instance, if p is odd then we have $s \le (\log_p e + \mathrm{ord}_p e + 2)(\mathrm{ord}_p e + 2) - 1$ (cf. Examples 2 and 4). If $e \le p - 2$, then $s = 0$ (cf. Example 1) and therefore we regain in a different way the following classical theorem of Raynaud.

Corollary 1 *We assume that $e \le p - 2$ (thus p is odd). Then each finite flat commutative group scheme of p power order over K extends in at most one way to a finite flat commutative group scheme over V.*

Corollary 1 was first proved in [R], Theorem 3.3.3 or Corollary 3.3.6 and more recently in [VZ2], Proposition 15. The first part of the next result is an equivalent form of the first part of Theorem 1.

Corollary 2 *Let $h : G_K \to H_K$ be a homomorphism over K. Then $p^s h$ extends to a homomorphism $G \to H$ (i.e., the cokernel of the natural monomorphism $\mathrm{Hom}(G, H) \hookrightarrow \mathrm{Hom}(G_K, H_K)$ is annihilated by p^s). Thus the natural homomorphism $\mathrm{Ext}^1(H, G) \to \mathrm{Ext}^1(H_K, G_K)$ has a kernel annihilated by p^s.*

The following two results are a mixed characteristic geometric analogue of the homomorphism form [V], Theorem 5.1.1 of the *crystalline boundedness principle* presented in [V], Theorem 1.2.

Corollary 3 *We assume that G and H are truncated Barsotti–Tate groups of level $n > s$. Let $h : G_K \to H_K$ be a homomorphism. Then the restriction homomorphism $h[p^{n-s}] : G_K[p^{n-s}] \to H_K[p^{n-s}]$ extends to a homomorphism $G[p^{n-s}] \to H[p^{n-s}]$.*

Corollary 4 *We assume that $n > 2s$. Let H be a truncated Barsotti–Tate group of level n over V. Let G be such that we have an isomorphism $h : G_K \to H_K$. Then the quotient group scheme $G[p^{n-s}]/G[p^s]$ is isomorphic to $H[p^{n-2s}]$ and thus it is a truncated Barsotti–Tate group of level $n - 2s$.*

Let Y be a normal noetherian integral scheme with field of functions L of characteristic zero. A classical theorem of Tate ([T], Theorem 4) says that for every two p-divisible groups D and F over Y, each homomorphism $D_L \to F_L$ extends uniquely to a homomorphism $D \to F$. From Corollary 3 we obtain the following sharper version of this theorem.

Theorem 2 *Let Y and L be as above. Then there exists a non-negative integer s_Y which has the following property.*

Let $\mathcal{G}$ and $\mathcal{H}$ be truncated Barsotti–Tate groups over Y of level $n > s_Y$ and of order a power of the prime p. Let $h : \mathcal{G}_L \to \mathcal{H}_L$ be a homomorphism. Then there exists a unique homomorphism $g : \mathcal{G}[p^{n-s_Y}] \to \mathcal{H}[p^{n-s_Y}]$ that induces $h[p^{n-s_Y}]$ over L.

Section 2 recalls for $p > 2$ (resp. for $p = 2$) the classification of finite flat (resp. connected finite flat) commutative group schemes of p power order over V in terms of *Breuil modules* that holds when k is perfect and V is complete. This classification was conjectured by Breuil (see [Br]), was first proved in [K1] (resp. [K2]), and was generalized (using a covariant language) in [VZ1] and [L]. In Section 3 we provide recursive formulas for s as well as explicit upper bounds of it. In Section 4 we prove Theorem 1. The above four Corollaries and Theorem 2 are proved in Section 5. In Section 6 we present extra applications to different heights associated to G.

2 Breuil modules

Let $V \hookrightarrow V'$ be an extension of discrete valuation rings such that the index of ramification of V' is also e. Theorem 1 holds for V if it holds for V'. There exists an extension V' which is complete and has a perfect residue field. If we find an upper bound of s only in terms of e which holds for each complete V' with perfect residue field, then this upper bound of s is also good for V.

Thus from now on we assume that V is complete and that k is a perfect field. Let $W(k)$ be the ring of Witt vectors with coefficients in k. We will view V as a $W(k)$-algebra which is a free $W(k)$-module of rank e. Let $\mathrm{ord}_p : W(k) \to \mathbb{N} \cup \{\infty\}$ be the p-adic valuation normalized by the conditions that $\mathrm{ord}_p(p) = 1$ and $\mathrm{ord}_p(0) = \infty$. Let u be a variable and let

$$\mathfrak{S} := W(k)[[u]].$$

We extend the Frobenius endomorphism σ of $W(k)$ to $\mathfrak{S}$ by the rule $\sigma(u) = u^p$. For $n \in \mathbb{N}^*$ let $\mathfrak{S}_n := \mathfrak{S}/p^n\mathfrak{S}$. If M is a $\mathfrak{S}$-module let

$$M^{(\sigma)} := \mathfrak{S} \otimes_{\sigma,\mathfrak{S}} M.$$

Let π be a uniformizer of V. Let

$$E = E(u) = u^e + a_{e-1}u^{e-1} + \cdots + a_1 u + a_0 \in W(k)[u]$$

be the unique Eisenstein polynomial in u which has coefficients in $W(k)$ and which has π as a root. For $i \in \{0, \ldots, e-1\}$ we have $a_i \in pW(k)$; moreover a_0 is p times a unit of $W(k)$. We have a $W(k)$-epimorphism

$$q_\pi : \mathfrak{S} \twoheadrightarrow V$$

that maps u to π.

Definition 1 *By a (contravariant) Breuil window relative to $q_\pi : \mathfrak{S} \twoheadrightarrow V$ we mean a pair (Q, ϕ), where Q is a free $\mathfrak{S}$-module of finite rank and where $\phi : Q^{(\sigma)} \to Q$ is a $\mathfrak{S}$-linear map (Frobenius map) whose cokernel is annihilated by E. By a (contravariant) Breuil module relative to $q_\pi : \mathfrak{S} \twoheadrightarrow V$ we mean a pair (M, φ), where M is a $\mathfrak{S}$-module annihilated by a power of p and of projective dimension at most one and where $\varphi : M^{(\sigma)} \to M$ is a $\mathfrak{S}$-linear map (Frobenius map) whose cokernel is annihilated by E. We say that (M, φ) is connected if its reduction modulo u defines a connected Dieudonné module over k (this makes sense as E modulo u is p times a unit of $W(k)$).*

Definition 2 *Let $\mathcal{B}$ (resp. $\mathcal{B}^c$) be the category of Breuil modules (resp. of connected Breuil modules) relative to $q_\pi : \mathfrak{S} \twoheadrightarrow V$. Let $\mathcal{B}_1$ (resp. $\mathcal{B}_1^c$) be the full subcategory of $\mathcal{B}$ (resp. of $\mathcal{B}^c$) whose objects are Breuil modules (M, φ) relative to $q_\pi : \mathfrak{S} \twoheadrightarrow V$ with M annihilated by p. Let $\mathcal{F}$ (resp. $\mathcal{F}^c$) be the category of finite flat commutative group schemes (resp. of connected finite flat commutative group schemes) of p power order over V. Let $\mathcal{F}_1$ (resp. $\mathcal{F}_1^c$) be the full subcategory of $\mathcal{F}$ (resp. of $\mathcal{F}^c$) whose objects are finite flat commutative group schemes over V annihilated by p.*

If M is annihilated by p, then it is easy to see that M is a free $\mathfrak{S}_1$-module (cf. [VZ2], Section 2, p. 7); its rank is also called the rank of (M, φ). In this paper we will use the shorter terminology (connected) Breuil module.

2.1 The case $p > 2$

In this Subsection we assume that $p > 2$. We recall the following classification first proved in [K1], Theorem 2.3.5 and generalized in [VZ1], Theorem 1 and [L].

Theorem 3 *There exists a contravariant functor $\mathbb{B} : \mathcal{F} \to \mathcal{B}$ which is an antiequivalence of categories, which is $\mathbb{Z}_p$-linear, and which takes short exact sequences (in the category of abelian sheaves in the faithfully flat topology of* $\operatorname{Spec} V$*) to short exact sequences (in the category of $\mathfrak{S}$-modules endowed with Frobenius maps).*

It is easy to see that $\mathbb{B}$ induces an antiequivalence of categories $\mathbb{B} : \mathcal{F}_1 \to \mathcal{B}_1$ which takes short exact sequences to short exact sequences. For an object $G = \operatorname{Spec} R$ of $\mathcal{F}$, let $o(G) \in \mathbb{N}$ be such that $p^{o(G)}$ is the order of G i.e., is the rank of R over V.

We check that if G is an object of $\mathcal{F}_1$, then the object $\mathbb{B}(G)$ of $\mathcal{B}_1$ has rank $o(G)$. We have a short exact sequences $0 \to G^{\circ} \to G \to G^{\acute{e}t} \to 0$, where G° is connected and $G^{\acute{e}t}$ is étale. As $\mathbb{B} : \mathcal{F}_1 \to \mathcal{B}_1$ takes short exact sequences to short exact sequences, we can assume that G is either étale or connected. The case when G is étale is easy and left as an exercise. Thus we can assume that G is connected. The contravariant Dieudonné module $\mathbb{D}(G_k)$ of G_k is equal to $k \otimes_{\sigma,\mathfrak{S}} \mathbb{B}(G)$, where we denote also by σ its composite with the epimorphism $\mathfrak{S} \twoheadrightarrow k = \mathfrak{S}/(p, u)$ (the covariant part of this statement follows from either [Z1], Theorem 6 or [Z2], Theorem 1.6 once we recall that G is the kernel of an isogeny of connected p-divisible groups over V). This implies that the rank of $\mathbb{B}(G)$ is $o(G)$.

Let H be an object of $\mathcal{F}$. If p^n annihilates H, then to the chain of natural epimorphisms

$$H \twoheadrightarrow H/H\lceil p\rceil \twoheadrightarrow H/\lceil p^2\rceil \twoheadrightarrow \cdots \twoheadrightarrow H/H\lceil p^n\rceil = 0$$

corresponds a normal series of the Breuil module $\mathbb{B}(H) = (M, \varphi)$

$$0 = (M_n, \varphi_n) \subseteq (M_{n-1}, \varphi_{n-1}) \subseteq \cdots \subseteq (M_0, \varphi_0) = (M, \varphi)$$

by Breuil submodules whose quotient factors are objects of $\mathcal{B}_1$. As each M_{i-1}/M_i is a free $\mathfrak{S}_1$-module of finite rank, the multiplication by u map $u : M \to M$ is injective. One computes the order $p^{o(H)}$ of H via the formulas

$$o(H) = o(M, \varphi) := \sum_{i=1}^{n} \operatorname{rank}_{\mathfrak{S}_1}(M_{i-1}/M_i) = \operatorname{length}_{\mathfrak{S}_{(p)}}(M_{(p)}).$$

Proposition 1 *Let $f : G \to H$ be a morphism of $\mathcal{F}$. We write $g := \mathbb{B}(f) : \mathbb{B}(H) = (M, \varphi) \to \mathbb{B}(G) = (N, \psi)$. Then we have:*

(a) *The homomorphism $f_K : G_K \to H_K$ is a closed embedding if and only if the cokernel of $g : M \to N$ is annihilated by some power of u.*

(b) *The homomorphism $f_K : G_K \to H_K$ is an epimorphism if and only if the $\mathfrak{S}$-linear map $g : M \to N$ is a monomorphism.*

(c) *The homomorphism $f_K : G_K \to H_K$ is an isomorphism if and only if the $\mathfrak{S}$-linear map $g : M \to N$ is injective and its cokernel is annihilated by some power of u.*

Proof. Let $\tilde{N} := \mathrm{Coker}(g)$. We prove (a). We first show that the assumption that f_K is not a closed embedding implies that $\tilde{N}$ is not annihilated by a power of u. This assumption implies that there exists a non-trivial flat, closed subgroup scheme G_0 of G which is contained in the kernel of f and which is annihilated by p. Let $(N_0, \psi_0) := \mathbb{B}(G_0)$; the $\mathfrak{S}_1$-module N_0 is free of positive rank. From the fact that G_0 is contained in the kernel of f and from Theorem 3, we get that we have an epimorphism $\tilde{N} \twoheadrightarrow N_0$. Thus $\tilde{N}$ is not annihilated by a power of u.

To end the proof of part (a) it suffices to show that the assumption that $\tilde{N}$ is not annihilated by a power of u implies that f_K is not a closed embedding. Our assumption implies that also $N_1 := \tilde{N}/p\tilde{N}$ is not annihilated by a power of u. As $\mathfrak{S}_1 = k[[u]]$ is a principal ideal domain, we have a unique short exact sequence of $\mathfrak{S}_1$-modules

$$0 \to N_2 \to N_1 \to N_0 \to 0,$$

where N_2 is the largest $\mathfrak{S}_1$-submodule of N_1 annihilated by a power of u and where N_0 is a free $\mathfrak{S}_1$-module of positive rank. The $\mathfrak{S}$-linear map $N_1^{(\sigma)} \to N_1$ induced naturally by ψ maps $N_2^{(\sigma)}$ to N_2 and thus it induces via quotients a $\mathfrak{S}$-linear map $\psi_0 : N_0^{(\sigma)} \to N_0$. As ψ_0 is a quotient map of ψ, its cokernel is annihilated by E. Therefore the pair (N_0, ψ_0) is a Breuil module. From this and Theorem 3 we get that there exists a non-trivial flat, closed subgroup scheme G_0 of G which is contained in the kernel of f and for which we have $\mathbb{B}(G_0) = (N_0, \psi_0)$. Thus f_K is not a closed embedding. Therefore (a) holds.

Part (b) is proved similarly to (a). Part (c) follows from (a) and (b). $\square$

2.2 The case $p = 2$

In this Subsection we assume that $p = 2$. Based on [K2], Theorem 1.3.9 or its generalizations in [VZ1], Introduction and [L], we have the following analogue of Theorem 3.

Theorem 4 *There exists a contravariant functor $\mathbb{B} : \mathcal{F}^c \to \mathcal{B}^c$ which is an antiequivalence of categories, which is $\mathbb{Z}_p$-linear, and which takes short exact sequences (in the category of abelian sheaves in the faithfully flat topology of* $\operatorname{Spec} V$*) to short exact sequences (in the category of $\mathfrak{S}$-modules endowed with Frobenius maps).*

Due to Theorem 4, everything in Subsection 2.1 holds for $p = 2$, provided we work in the connected context (i.e., G and H are connected).

2.3 Basic lemmas

Let $n \in \mathbb{N}^*$. Let $t \in \mathbb{N}$. Let H be a truncated Barsotti–Tate group of level n over V. If $p = 2$, then we assume that H is connected. Let $(M, \varphi) := \mathbb{B}(H)$; thus M is a free $\mathfrak{S}_n$-module of finite rank. Let d be the dimension of H and let h be the height of H. There exists a direct sum decomposition $M = T \oplus L$ into free $\mathfrak{S}_n$-modules such that the image of φ is $ET \oplus L$ and T has rank d. The existence of such a direct sum decomposition follows from the existence of normal decompositions of Breuil windows relative to $q_\pi : \mathfrak{S} \twoheadrightarrow V$ (for the covariant context with $p > 2$ see [VZ1], Section 2; the case $p = 2$ is the same). The existence of the direct sum decomposition $M = T \oplus L$ implies the existence of two $\mathfrak{S}_n$-bases $\{e_1, \ldots, e_h\}$ and $\{v_1, \ldots, v_h\}$ of M such that for $i \in \{d+1, \ldots, h\}$ we have $\varphi(1 \otimes e_i) = v_i$ and for $i \in \{1, \ldots, d\}$ the difference $\varphi(1 \otimes e_i) - Ev_i$ belongs to the $\mathfrak{S}$-submodule of M generated by the elements $v_{d+1}, \ldots, v_h$. Indeed, we consider the composite map

$$M \to M^{(\sigma)} \to \varphi(M^{(\sigma)}) \to M/T,$$

where the first map $m \mapsto 1 \otimes m$ is σ-linear, where the second map is φ, and where the third map is induced by the natural projection of M on T along L. We tensor this composite map with the residue field k of $\mathfrak{S}$

$$k \otimes_{\mathfrak{S}_n} M \to k \otimes_{\mathfrak{S}_n} M^{(\sigma)} \to k \otimes_{\mathfrak{S}_n} \varphi(M^{(\sigma)}) \to k \otimes_{\mathfrak{S}_n} M/T.$$

As k is a perfect field, all these three maps are surjective. Therefore we find by the lemma of Nakayama a $\mathfrak{S}_n$-basis $\{e_1, \ldots, e_h\}$ of M such that the images

$\varphi(1\otimes e_{d+1}),\ldots,\varphi(1\otimes e_h)$ form a $\mathfrak{S}_n$-basis of M/T. We can take L to be the $\mathfrak{S}_n$-submodule of M generated by $v_{d+1} := \varphi(1\otimes e_{d+1}),\ldots,v_h := \varphi(1\otimes e_h)$. We choose an arbitrary $\mathfrak{S}_n$-basis $\{v_1,\ldots,v_d\}$ of T. As the image of φ is $ET\oplus L$ we obtain the desired $\mathfrak{S}_n$-basis $\{v_1,\ldots,v_h\}$ by making a suitable change of the $\mathfrak{S}_n$-basis $\{v_1,\ldots,v_d\}$ of T.

Lemma 1 *We assume $t\geq 1$. Let $x\in\frac{1}{u^t}M$ be such that $\varphi(1\otimes x)\in\frac{1}{u^t}M$. We write $x=\sum_{i=1}^h\frac{\alpha_i}{u^t}e_i$, where $\alpha_i\in\mathfrak{S}_n$. Then for each $i\in\{1,\ldots,h\}$ we have $E\sigma(\alpha_i)\in u^{t(p-1)}\mathfrak{S}_n$ (equivalently, $\frac{\sigma(\alpha_i)}{u^{tp}}E\in\frac{1}{u^t}\mathfrak{S}_n$) and thus $\alpha_i\in(p^{n-1},u)\mathfrak{S}_n$.*

Proof. We compute

$$\varphi(1\otimes x)=\sum_{i=1}^d\frac{\sigma(\alpha_i)}{u^{tp}}\varphi(1\otimes e_i)+\sum_{i=d+1}^h\frac{\sigma(\alpha_i)}{u^{tp}}\varphi(1\otimes e_i)$$

$$=\sum_{i=1}^d\frac{\sigma(\alpha_i)}{u^{tp}}Ev_i+\sum_{i=d+1}^h\eta_iv_i\in\frac{1}{u^t}M,$$

for suitable elements $\eta_i\in\frac{1}{u^t}\mathfrak{S}_n$. For $i\in\{1,\ldots,d\}$ this implies directly that

$$\frac{\sigma(\alpha_i)}{u^{tp}}E\in\frac{1}{u^t}\mathfrak{S}_n. \tag{1}$$

The η_i for $i\in\{d+1,\ldots,h\}$ are of the form

$$\eta_i=\frac{\sigma(\alpha_i)}{u^{tp}}+\sum_{j=1}^d\lambda_j\frac{\sigma(\alpha_j)}{u^{tp}},$$

for some elements $\lambda_j\in\mathfrak{S}_n$. If we multiply the last equation by E we obtain from (1) that its belonging relation also holds for $i\in\{d+1,\ldots,h\}$. □

Lemma 2 *Let N be a $\mathfrak{S}_n$-submodule of $\frac{1}{u^t}M$ which contains M. We assume that φ induces a $\mathfrak{S}$-linear map $N^{(\sigma)}\to N$. Then we have $p^tN\subseteq M$.*

Proof. We will prove this by induction on $t\in\mathbb{N}$. The case $t=0$ is trivial. For the passage from $t-1$ to t we can assume that $t>0$. Let $x\in N$. From Lemma 1 applied to x we get that $px\in u\frac{1}{u^t}M=\frac{1}{u^{t-1}}M$. This implies that $pN\subseteq\frac{1}{u^{t-1}}M$. Let $\tilde{N}:=pN+M\subseteq\frac{1}{u^{t-1}}M$. It is easy to see that φ induces a

$\mathfrak{S}$-linear map $\tilde{N}^{(\sigma)} \to \tilde{N}$. By induction applied to $\tilde{N}$ we get that $p^{t-1}\tilde{N} \subseteq M$. This implies that $p^t N \subseteq M$. This ends the induction. $\square$

The technical part of the method we use in this paper can be summarized as follows. With the notations of Lemmas 1 and 2, we will vary the uniformizer π of V to obtain a sharp upper bound t_0 of t in such a way that Lemma 2 can be improved to provide a smaller number $s \in \{0, \ldots, t_0\}$ for which we have a universal inclusion $p^s N \subseteq M$.

3 Motivation, formulas, and bounds for s

In this Section we present recursive formulas for s and upper bounds of it in terms of e. The main technical result that lies behind these formulas is also presented in this Section (see Proposition 2 below).

For a real number x, let $\lfloor x \rfloor$ be the integral part (floor) of x (i.e., the greatest integer smaller or equal to x). We define

$$m := \mathrm{ord}_p(e).$$

Let $a_e := 1$ and

$$E_0 := \sum_{i \in p\mathbb{N} \cap [0,e]} a_i u^i = a_{p\lfloor \frac{e}{p} \rfloor} u^{p\lfloor \frac{e}{p} \rfloor} + \cdots + a_{2p} u^{2p} + a_p u^p + a_0 \in W(k)[u^p].$$

Let $E_1 := E - E_0 \in W(k)[u]$. We define the numbers τ and ι as follows.

If $m = 0$, then let $\tau(\pi) := 1$ and $\iota(\pi) := 0$.

If $m \geq 1$, let $\tau(\pi) \in \mathbb{N}^* \cup \{\infty\}$ be the content $\mathrm{ord}_p(E_1)$ of E_1. Thus

$$\tau(\pi) := \mathrm{ord}_p(E_1) = \min\{\mathrm{ord}_p(a_i) | i \in \{1, 2, \ldots, e-1\} \setminus p\mathbb{N}^*\}.$$

If $m \geq 1$ and $\tau(\pi) < \infty$, let $\iota(\pi) \in \{1, 2, \ldots, e-1\} \setminus p\mathbb{N}^*$ be the smallest number such that we have

$$\tau(\pi) = \mathrm{ord}_p(a_{\iota(\pi)}) > 0.$$

For all $m \geq 0$ we define

$$\tau = \tau_V := \min\{\tau(\pi) | \pi \text{ a uniformizer of } V\}.$$

If $\tau < \infty$, then we also define

$$\iota = \iota_V := \min\{\iota(\pi) | \pi \text{ a uniformizer of } V \text{ with } \tau(\pi) = \tau\}.$$

Lemma 3 *We have $\tau \leq m+1 < \infty$.*

Proof. If $m = 0$, then this holds as $\tau = 1$. Thus we can assume that $m \geq 1$. We consider a new uniformizer $\tilde{\pi} := \pi + p$ of V. The unique Eisenstein polynomial $\tilde{E}(u) = u^e + \tilde{a}_{e-1}u^{e-1} + \cdots + \tilde{a}_1 u + \tilde{a}_0$ in u with coefficients in $W(k)$ that has $\tilde{\pi}$ as a root is $\tilde{E}(u) = E(u-p)$. Thus $\tilde{a}_{e-1} = -pe + a_{e-1} = -p^{m+1}e' + a_{e-1}$. Therefore p^{m+2} does not divide either a_{e-1} or $\tilde{a}_{e-1}$. This implies that either $\tau(\pi) \leq m+1$ or $\tau(\tilde{\pi}) \leq m+1$. Thus $\tau \leq m+1 < \infty$. $\square$

Proposition 2 *Let n and t be positive integers. Let $C = C(u) \in \mathfrak{S}$ be a power series whose constant term is not divisible by p^n. We assume that*

$$E\sigma(C) \in (u^t, p^n)\mathfrak{S}. \tag{2}$$

If $\tau(\pi) = \infty$, then we have $t \leq ne$. If $\tau(\pi) \neq \infty$, then we have

$$t \leq \min\{\tau(\pi)e + \iota(\pi), ne\}.$$

Moreover, if $m = 0$, then we have $p\sigma(C) \in (u^t, p^n)\mathfrak{S}$ and if $m \geq 1$, then we have $p^{\tau(\pi)+1}\sigma(C) \in (u^t, p^n)\mathfrak{S}$.

Proof. Clearly we can remove from C all monomials of degree i such that $pi \geq t$. Therefore we can assume that C is a polynomial of degree d such that $pd < t$. As $E_0\sigma(C)$ and $E_1\sigma(C)$ do not contain monomials of the same degree, the relation $E\sigma(C) \in (u^t, p^n)\mathfrak{S}$ implies that

$$E_0\sigma(C) \in (u^t, p^n)\mathfrak{S} \quad \text{and} \quad E_1\sigma(C) \in (u^t, p^n)\mathfrak{S}.$$

We first consider the case when p does not divide e (i.e., $m = 0$). Thus E_0 divided by p is a unit of $\mathfrak{S}$. Therefore we have $p\sigma(C) \in (u^t, p^n)\mathfrak{S}$. As $p\deg(C) = pd < t$, we get that $p\sigma(C) \equiv 0 \mod p^n$. As $E_1 \equiv u^e \mod p$ we get $u^e\sigma(C) \in (u^t, p^n)\mathfrak{S}$. As the constant term of C is not divisible by p^n this implies that $t \leq e = \min\{\tau(\pi)e + \iota(\pi), ne\}$.

From now on we will assume that $p|e$. By the Weierstraß preparation theorem ([Bo], Chapter 7, Section 3, number 8) we can assume that C is a Weierstraß polynomial of degree d (i.e., a monic polynomial of degree d such that $C - u^d$ is divisible by p). Indeed, let $c \in \{0, \ldots, n-1\}$ be such that p^c is the content of C. We set $\bar{C} := (1/p^c)C$. The constant term of $\bar{C}$ is not divisible by p^{n-c}. As $E\sigma(\bar{C}) \in (u^t, p^{n-c})\mathfrak{S}$, it suffices to prove the proposition for $\bar{C}$. But $\bar{C}$ is a unit times a Weierstraß polynomial.

Before we continue, we first prove the following Lemma.

Lemma 4 *Let n and t be positive integers. We assume that p divides e. Let*

$$C = C(u) = u^d + c_{d-1}u^{d-1} + \cdots + c_1 u + c_0 \in W(k)[u]$$

be a Weierstraß polynomial such that $pd < t$ and $c_0 \notin p^n W(k)$. We also assume that

$$E_0\sigma(C) \in (u^t, p^n)\mathfrak{S}.$$

Then $d = (n-1)\frac{e}{p}$ and for each $i \in \{0, 1, \dots, n-1\}$ we have:

$$\mathrm{ord}_p(c_{i\frac{e}{p}}) = n - i - 1, \quad \textit{and} \quad \mathrm{ord}_p(c_j) \geq n - i, \quad \textit{for} \quad 0 \leq j < i\frac{e}{p}. \qquad (3)$$

Moreover we also have $t \leq ne$.

Proof: We write

$$\sigma(C) = u^{dp} + \gamma_{d-1}u^{(d-1)p} + \cdots + \gamma_1 u^p + \gamma_0.$$

We define c_d and γ_d to be 1. For $l < 0$ or $l > d$, we define $c_l = \gamma_l = 0$. We have $\mathrm{ord}_p(\gamma_l) = \mathrm{ord}_p(c_l)$ for all $l \in \mathbb{Z}$. Moreover we set

$$E_0\sigma(C) = \sum_{j=0}^{d+\frac{e}{p}} \beta_{jp} u^{jp}, \qquad \beta_{jp} \in W(k).$$

By our assumption β_{jp} is divisible by p^n if $jp < t$ and in particular if $j \leq d$. For $j \in \{0, \dots, d + \frac{e}{p}\}$ we have the identity

$$\beta_{jp} = a_0\gamma_j + a_p\gamma_{j-1} + \cdots + a_e\gamma_{j-\frac{e}{p}}. \qquad (4)$$

By induction on $j \in \{0, \dots, d\}$ we show that (3) holds. This includes the equality part of (3) if $j = i\frac{e}{p}$. Our induction does not require that $i < n$. But of course, the assumption that $i \geq n$ in the equality part of (3) (resp. the assumptions that $j \leq d$ and $i \geq n+1$ in the inequality part of (3)), leads (resp. lead) to a contradiction as the order of any c_j can not be negative.

The case $j = 0$ follows by looking at the constant term of $E_0\sigma(C)$. The passage from $j-1$ to j goes as follows. Let us first assume that $(i-1)\frac{e}{p} < j < i\frac{e}{p}$ for some integer $i \geq 1$ (we do not require $i\frac{e}{p} \leq d$).

We show that the assumption $\mathrm{ord}_p(c_j) = \mathrm{ord}_p(\gamma_j) < n - i$ leads to a contradiction. Indeed, in this case the first term of the right hand side of

(4) would have order $\leq n-i$ but all the other terms of the right hand side of (4) would have order strictly bigger than $n-i$. Note for example that $j-\frac{e}{p} < (i-1)\frac{e}{p}$ and therefore $\mathrm{ord}_p(\gamma_{j-\frac{e}{p}}) \geq n-i+1$ by induction assumption. As $\mathrm{ord}_p(\beta_{jp}) \geq n$ we obtain a contradiction to (4).

Finally we consider the passage from $j-1$ to j in the case when $j = i\frac{e}{p}$. Then we use the equation

$$\beta_{ie} = a_0\gamma_{i\frac{e}{p}} + a_p\gamma_{i\frac{e}{p}-1} + \cdots + a_e\gamma_{(i-1)\frac{e}{p}}. \tag{5}$$

By the induction assumption we have $\mathrm{ord}_p(a_e\gamma_{(i-1)\frac{e}{p}}) = n-i$. From the inequality part of (3) we get the inequalities

$$\mathrm{ord}_p(a_p\gamma_{i\frac{e}{p}-1}) \geq n-i+1, \ldots, \mathrm{ord}_p(a_{e-p}\gamma_{1+(i-1)\frac{e}{p}}) \geq n-i+1.$$

As $\beta_{ie} = \beta_{jp} \in p^nW(k)$, it follows from (5) that

$$\mathrm{ord}_p(a_0\gamma_{i\frac{e}{p}}) = \mathrm{ord}_p(a_e\gamma_{(i-1)\frac{e}{p}}) = n-i.$$

Thus $\mathrm{ord}_p(\gamma_{i\frac{e}{p}}) = n-i-\mathrm{ord}_p(a_0) = n-i-1$. This ends our induction.

We check that $d = (n-1)\frac{e}{p}$. If d is of the form $i\frac{e}{p}$, then $0 = \mathrm{ord}_p(c_d) = n-i-1$ gives $i = n-1$ and thus d is as required. We are left to show that the assumption that d is not of this form, leads to a contradiction. Let i be the smallest integer such that $d < i\frac{e}{p}$. Then the inequality $0 = \mathrm{ord}_p(c_d) \geq n-i$ gives $i \geq n$. But then $\mathrm{ord}_p(c_{(i-1)\frac{e}{p}}) = n-i$ contradicts the assumption that C is a Weierstraß polynomial and therefore that $c_{(i-1)\frac{e}{p}} \in pW(k)$. □

Corollary 5 *With the notations of Lemma 4, let* $l \in \{0,1,\ldots,e-1\}$. *Let* $E_2 = E_2(u) = u^l + b_{l-1}u^{l-1} + \cdots + b_1u + b_0 \in W(k)[u]$ *be a Weierstraß polynomial of degree* l. *If we have* $E_2\sigma(C) \in (u^t, p^n)\mathfrak{S}$, *then* $l \geq t$.

Proof: If $n = 1$, then $d = 0$ and $C = c_0$ is a unit of $W(k)$; thus $E_2 \in (u^t, p^n)\mathfrak{S}$ and therefore $l \geq t$. Thus we can assume that $n \geq 2$. We write:

$$E_2\sigma(C) = \sum_{i=0}^{l+pd} \delta_i u^i.$$

Let $q := \lfloor \frac{l}{p} \rfloor < \frac{e}{p}$. We have the equation:

$$\delta_l = \gamma_0 + b_{l-p}\gamma_1 + \cdots + b_{l-qp}\gamma_q. \tag{6}$$

For $i \in \{0, \dots, q\}$ we have $\mathrm{ord}_p(\gamma_i) \geq n-1$ (cf. Lemma 4 and $n \geq 2$); therefore $\mathrm{ord}_p(b_{l-ip}\gamma_i) \geq n$. As $\mathrm{ord}_p(\gamma_0) = n-1$, from (6) we get $\mathrm{ord}_p(\delta_l) = n-1$. From this and the assumption $E_2\sigma(C) \in (u^t, p^n)\mathfrak{S}$, we get $l \geq t$. $\square$

We are now ready to prove Proposition 2 in the case when $p|e$ (i.e., $m \geq 1$). We remark that the case $\tau(\pi) = \infty$ follows directly from Lemma 4. Hence we can assume that $\tau(\pi) < \infty$.

If $\tau(\pi) \geq n$, then $p^{\tau(\pi)+1}\sigma(C) \in (u^t, p^n)\mathfrak{S}$ and we conclude by Lemma 4 that $t \leq ne \leq \tau(\pi)e$; thus $t \leq \min\{\tau(\pi)e + \iota(\pi), ne\}$. Therefore we can assume that $\tau(\pi) < n$.

As $\tau(\pi) = \mathrm{ord}_p(E_1)$, by Weierstraß preparation theorem we can write

$$E_1 = p^{\tau(\pi)}E_2\theta,$$

where $\theta \in \mathfrak{S}$ is a unit and where $E_2 \in W(k)[u]$ is a Weierstraß polynomial of degree $\iota(\pi) < e$. As $E_1\sigma(C) \in (u^t, p^n)\mathfrak{S}$ and as $n > \tau(\pi)$, we get that

$$E_2\sigma(C) \in (u^t, p^{n-\tau(\pi)})\mathfrak{S}.$$

We consider the polynomial

$$C_1 = C_1(u) = u^d + c_{d-1}u^{d-1} + \cdots + c_{\tau(\pi)\frac{e}{p}}u^{\tau(\pi)\frac{e}{p}} \in W(k)[u].$$

It follows from Lemma 4 that $\mathrm{ord}_p(c_j) \geq n - \tau(\pi)$ for $j < \tau(\pi)\frac{e}{p}$. Thus $C_1 - C \in p^{n-\tau(\pi)}\mathfrak{S}$ and therefore we obtain

$$E_2\sigma(C_1) = E_2\sigma(C_1 - C) + E_2\sigma(C) \in (u^t, p^{n-\tau(\pi)})\mathfrak{S}. \tag{7}$$

We write $C_1 = u^{\tau(\pi)\frac{e}{p}}C_2$. Then the constant term of C_2 is $c_{\tau(\pi)\frac{e}{p}}$ and thus it is not divisible by $p^{n-\tau(\pi)}$, cf. (3). As $n > \tau(\pi)$, the relations $(n-1)e = pd < t$ imply that $t - \tau(\pi)e > 0$. Thus from (7) we get that

$$E_2\sigma(C_2) \in (u^{t-\tau(\pi)e}, p^{n-\tau(\pi)})\mathfrak{S}. \tag{8}$$

A similar argument shows that

$$E_0\sigma(C_2) \in (u^{t-\tau(\pi)e}, p^{n-\tau(\pi)})\mathfrak{S}. \tag{9}$$

From Corollary 5 applied to the quadruple $(t-\tau(\pi)e, C_2, E_0, n-\tau(\pi))$ instead of (t, C, E_0, n), we get that $\iota(\pi) = \deg(C_2) \leq t - \tau(\pi)e$. As $\iota(\pi) \leq e-1$ and as $n \geq \tau(\pi)+1$, we conclude that $t \leq \tau(\pi)e + \iota(\pi) = \min\{\tau(\pi)e + \iota(\pi), ne\}$. As $\iota(\pi) \leq e-1$, the relations $(n-1)e = pd < t \leq \min\{\tau(\pi)e + \iota(\pi), ne\}$ imply that $n = \tau(\pi)+1$; thus $p^{\tau(\pi)+1}\sigma(C) \in (u^t, p^n)\mathfrak{S}$. This ends the proof of the Proposition 2 in the second case $p|e$. $\square$

3.1 Recursive formulas for s

For a uniformizer π of V, Lemma 1 and Proposition 2 motivate the introduction of the following invariant

$$t(\pi) := \lfloor \frac{\tau(\pi)e + \iota(\pi)}{p-1} \rfloor \in \mathbb{N} \cup \{\infty\}.$$

Always there exists a π such that $t(\pi)$ is finite, cf. Lemma 3.

Based on the last sentence of Proposition 2, we define $\epsilon \in \{0,1\}$ as follows. If $m = 0$, then $\epsilon := 0$ and if $m \geq 1$, then $\epsilon := 1$. Next we will define recursively a number $z \in \mathbb{N}$ and z pairs $(t_0, s_0), \ldots, (t_z, s_z) \in \mathbb{N}^2$ as follows.

Let t_0 be the minimum of $t(\pi)$ for all possible π; thus $t_0 = \lfloor \frac{\tau e + \iota}{p-1} \rfloor$. Let $s_0 := 0$. If $t_0 - \lfloor \frac{t_0}{p} \rfloor \leq \tau + \epsilon$, then let $z := 0$. The recursive process goes as follows. For $j \in \mathbb{N}^*$ such that $(t_0, s_0), \ldots, (t_{j-1}, s_{j-1})$'s are defined, we stop the process and set $z = j-1$ if $t_{j-1} + \lfloor \frac{t_{j-1}}{p} \rfloor \leq \tau + \epsilon$, and otherwise we set

$$(t_j, s_j) := (\lfloor \frac{t_{j-1}}{p} \rfloor, s_{j-1} + \tau + \epsilon).$$

We note that

$$0 = s_0 < s_1 < \cdots < s_z \quad \text{and} \quad 0 \leq t_z < t_{z-1} < \cdots < t_0.$$

Moreover the following relations hold:

$$t_z + s_z < t_{z-1} + s_{z-1} < \cdots < t_1 + s_1 < t_0 + s_0 = t_0 = \lfloor \frac{\tau e + \iota}{p-1} \rfloor. \tag{10}$$

If $p > 2$, we define $s = s_V := t_z + s_z$.

If $p = 2$ we modify this definition as follows. Let υ be the largest number such that a primitive root of unity of order 2^{υ} is contained in V. We set:

$$s = s_V := \upsilon + 2(t_z + s_z).$$

By Lemma 3 there exists a π such that $\tau(\pi) \leq m+1$ (with $m = \mathrm{ord}_p(e)$). For $p > 2$ we have $s \leq \lfloor \frac{\tau e + \iota}{p-1} \rfloor$ and thus, as $\iota \leq e-1$, we get

$$s \leq \frac{2e - 1 + e\,\mathrm{ord}_p(e)}{p-1}. \tag{11}$$

If $p=2$, then inequalities $\iota \le e-1$, $\upsilon \le m+1$, and $s \le \upsilon + 2(\tau e + \iota)$ imply

$$s \le 4e - 1 + (2e+1)\,\mathrm{ord}_2(e). \tag{12}$$

Example 1 We assume that $e \le p-2$. Thus p is odd, $m = \iota = 0$, and $\tau = 1$. We have $s \le \frac{e}{p-1}$, cf. (10). Therefore $s = 0$.

Example 2 We can midify slightly the recursive process to define s as follows. We stop the process if $t_{j-1} + \lfloor \frac{t_{j-1}}{p} \rfloor < \tau + \epsilon$ and continue it if this equality does not hold. Then $z+1$ steps might be necessary but in this case we have $t_{z+1} + s_{z+1} = t_z + s_z$. Let us assume $m = 0$ and $p > 2$. Let

$$t_0 = \sum_{j=0}^{u} a_j p^j, \quad 0 \le a_j < p,\ a_u \ne 0 \tag{13}$$

be the p-adic expansion. As $\tau = \tau + \epsilon = 1$, the modified recursive process stops after $u+1$ steps at the pair $(0, u+1)$. Thus we find $s = u+1$. As $t_0 = \lfloor \frac{e}{p-1} \rfloor$, we have $s = 1$ if and only if $p-1 \le e \le (p-1)^2 + p - 2 = p^2 - p - 1$. In general, we have $s \le 1 + \log_p e$.

Example 3 We assume that $E = u^p - p$. Then $\tau(\pi) = \infty$. For $n \in \mathbb{N}^*$ we have $E\sigma(\sum_{i=1}^{n} p^{n-i} u^{i-1}) = u^{pn}$; the power pn goes to infinity when $n \to \infty$.

Let $\tilde{\pi} = c_0 p + c_1 \pi + \cdots + c_{p-1}\pi^{p-1}$ be another uniformizer of V. We have $c_0, c_1, c_1^{-1}, c_2, \ldots, c_{p-1} \in W(k)$. It is easy to see that $\tilde{\pi}^p$ is congruent modulo p^2 to an element of $pW(k)$. Thus, if $\tilde{E}(u) = u^p + \tilde{a}_{p-1}u^{p-1} + \cdots + \tilde{a}_0$ is the Eisenstein polynomial that has $\tilde{\pi}$ as a root, then for $i \in \{1, \ldots, p-1\}$ we have $\tilde{a}_i \in p^2 W(k)$. Therefore $\tau \ge 2$. But $\tau \le m+1 = 2$, cf. Lemma 3. Thus $\tau = 2$. From Subsection 3.1 we get that for $p > 2$ we have $s \le \frac{2p+\iota}{p-1}$. Thus for $p = 3$ we have $s \le 4$ and for $p \ge 5$ we have $s \le 3$. Similarly we argue that if $p = 2$, then we have $s \le \upsilon + 10$.

Example 4 We consider the case $p \ge 3$ and $m \ge 1$. We consider again the p-adic expansion (13). The number of steps z in the recursive process is at most $u+1$ and the pair (t_z, s_z) is such that $t_z < \tau$. Thus we have $s \le (u+1)(\tau+1) + \tau$. We have the inequalities $(\tau+1)e/(p-1) \ge t_0$ and $\log_p t_0 \ge u$. Moreover $\tau \le m+1$ by Lemma 3. We find the inequality

$$s \le (\log_p(m+2) + \log_p e - \log_p(p-1) + 1)(m+2) + m + 1.$$

As $m = \mathrm{ord}_p e$, $\log_p(m+2) \le m$, and $\log_p(p-1) \in (0,1)$, we find that

$$s < (\log_p e + \mathrm{ord}_p e + 2)(\mathrm{ord}_p e + 2) - 1.$$

4 Proof of Theorem 1

We prove that Theorem 1 holds for the number s of Subsection 3.1 if V is complete and has perfect residue field k. We already noted in Section 2 that it is enough to treat this case. We distinguish two cases as follows.

4.1 The case $p > 2$

We choose the uniformizer π of V in such a way that $\tau = \tau(\pi)$ is minimal and $\iota = \iota(\pi)$. Let $z \in \mathbb{N}$, the sequence of pairs $(t_0, s_0), \ldots, (t_z, s_z)$, and $s \in \mathbb{N}$ be as in Subsection 3.1. Thus $t_0 = \lfloor (\tau e + \iota)/(p-1) \rfloor = t_0(\pi)$ and $s = t_z + s_z$.

Let $f : G \to H$ be a homomorphism of finite flat commutative group schemes of p power order over V, which induces an isomorphism $f_K : G_K \to H_K$ in generic fibers. We first remark that if there exists a homomorphism $f' : H \to G$ such that $f \circ f' = p^s \,\mathrm{id}_H$, then we have $f'_K = p^s f_K^{-1}$ and thus the equality $f' \circ f = p^s \,\mathrm{id}_G$ also holds as it holds generically; moreover, as the equalities continue to hold in the special fibre we conclude that the kernel and cokernel of f_k are annihilated by p^s.

We choose an epimorphism $\xi_H : \tilde{H} \twoheadrightarrow H$ from a truncated Barsotti–Tate group $\tilde{H}$. We consider the following fiber product

$$\begin{array}{ccc} \tilde{G} & \xrightarrow{\tilde{f}} & \tilde{H} \\ {\scriptstyle \xi_G}\downarrow & & \downarrow{\scriptstyle \xi_H} \\ G & \xrightarrow{f} & H \end{array}$$

in the category $\mathcal{F}$. Then $\tilde{f}_K$ is an isomorphism. Assume that there exists a homomorphism $\tilde{f}' : \tilde{H} \to \tilde{G}$ such that $\tilde{f} \circ \tilde{f}' = p^s \circ \mathrm{id}_{\tilde{H}}$. Then $\xi_G \circ \tilde{f}'$ is zero on the finite flat group scheme $\mathrm{Ker}(\xi_H)$ because this is true for the generic fibers. Thus there exists $f' : H \to G$ such that $f' \circ \xi_H = \xi_G \circ \tilde{f}'$. One easily verifies that $f \circ f' = p^s \,\mathrm{id}_H$.

Thus to prove the existence of f' we can assume that $f = \tilde{f}$ and that $H = \tilde{H}$ is a truncated Barsotti–Tate group of level $n > s$.

Next we translate the existence of f' in terms of Breuil modules. Let (M, φ) and (N, ψ) be the Breuil modules of H and G (respectively). We know by Proposition 1 (c) that to f corresponds a $\mathfrak{S}$-linear monomorphism $M \hookrightarrow N$ whose cokernel is annihilated by some power u^t. We will assume that t is the smallest natural number with this property. We put aside the case $t = 0$ (i.e., the case when $f : G \to H$ is an isomorphism) which is trivial. The existence of $f' : H \to G$ is equivalent to the inclusion

$$p^s N \subseteq M. \tag{14}$$

Before we prove this inclusion we show that (for $p > 2$) Theorem 1 follows from it. It remains to prove the last sentence of the Theorem 1. Hence again let H be a truncated Barsotti–Tate group of level $n > s$.

The identity $f \circ f' = p^s \operatorname{id}_H$ means that we have a commutative diagram:

$$\begin{array}{ccc} H & \xrightarrow{f'} & G \\ & {\scriptstyle p^s}\searrow & \downarrow{\scriptstyle f} \\ & & H. \end{array}$$

We note that a homomorphism of finite flat group schemes over V is zero if it induces the zero homomorphism at the level of generic fibers. Therefore we obtain a commutative diagram:

$$\begin{array}{ccc} H/(H[p^s]) & \xrightarrow{\breve{f}'} & G \\ & \searrow & \downarrow{\scriptstyle f} \\ & & H. \end{array}$$

We see that $\breve{f}'$ is a closed immersion because the oblique arrow is. Now we apply the functor $\lceil p^{n-s} \rceil$ (see Section 1) to the last diagram:

$$\begin{array}{ccc} H/(H[p^s]) & \xrightarrow{\breve{f}'\lceil p^{n-s}\rceil} & G\lceil p^{n-s}\rceil \\ & \searrow & \downarrow{\scriptstyle f\lceil p^{n-s}\rceil} \\ & & H[p^{n-s}]. \end{array}$$

The horizontal homomorphism is again a closed immersion. As it is a homomorphism between finite flat group schemes of the same order, it has to be an isomorphism. The oblique arrow is trivially an isomorphism. Thus $f\lceil p^{n-s}\rceil : G\lceil p^{n-s}\rceil \to H[p^{n-s}]$ is an isomorphism and therefore $G\lceil p^{n-s}\rceil$ is a Barsotti–Tate group. This shows the last sentence of Theorem 1 when $p > 2$. It remains to prove the inclusion (14).

We will prove by induction on $j \in \{0, \ldots, z\}$ that we have $p^{s_j} N \subseteq \frac{1}{u^{t_j}} M$.

We remark that by Lemma 2 this implies that $p^{t_j+s_j}N \subset M$. As $s = t_z+s_z$ the induction gives the desired inclusion (14) and ends the proof of Theorem 1 (for $p > 2$). We also remark that already the base of the induction $j = 0$ implies the Theorem 1 but with the much weaker bound $s = t_0$.

For the base of the induction it suffices to show that $t \leq t_0$. Let $x \in N$ be such that $u^{t-1}x \notin M$. With $\{e_1, \ldots, e_h\}$ a $\mathfrak{S}_n$-basis of M as before Lemma 1, we write

$$x = \sum_{i=1}^{h} \frac{\alpha_i}{u^t} e_i, \quad \alpha_i \in \mathfrak{S}_n.$$

From Lemma 1 we get that for each $i \in \{1, \ldots, h\}$ we have $E\sigma(\alpha_i) \in u^{t(p-1)}\mathfrak{S}_n$. By the minimality of t, there exists $i_0 \in \{1, \ldots, h\}$ such that α_{i_0} is not divisible by u. Let $C = C(u) \in \mathfrak{S}$ be such that its reduction modulo p^n is α_{i_0}. The constant term of C is not divisible by p^n and we have $E\sigma(C) \in (u^{t(p-1)}, p^n)\mathfrak{S}$. From this and Proposition 2 we get that $t(p-1) \leq \min\{\tau e + \iota, ne\}$. Thus $t \leq t_0 = \lfloor (\tau e + \iota)/(p-1) \rfloor$.

If $0 < j < z$, then the inductive step from $j-1$ to j goes as follows. We assume that $p^{s_{j-1}}N \subseteq \frac{1}{u^{t_{j-1}}}M$. Let $l_{j-1} \in \{0, \ldots, t_{j-1}\}$ be the smallest number such that we have $p^{s_{j-1}}N \subseteq \frac{1}{u^{l_{j-1}}}M$. If $l_{j-1} = 0$, then $p^{s_{j-1}}N \subseteq M$ and thus, as $s_{j-1} < s_j$, we also have $p^{s_j}N \subseteq M \subseteq \frac{1}{u^{t_j}}M$. Therefore we can assume that $1 \leq l_{j-1} \leq t_{j-1}$. Let $y \in p^{s_{j-1}}N$. We write

$$y = \sum_{i=1}^{h} \frac{\eta_i}{u^{n_i}} e_i,$$

where $\eta_i \in \mathfrak{S}_n \setminus u\mathfrak{S}_n$ and where $n_i \in \{0, \ldots, l_{j-1}\}$. Let $C_i = C_i(u) \in \mathfrak{S}$ be such that its reduction modulo p^n is η_i. We want to show that $p^{\tau+\epsilon}y \in \frac{1}{u^{t_j}}M$. For this it suffices to show that for each $i \in \{1, \ldots, h\}$ we have $p^{\tau+\epsilon}\frac{\eta_i}{u^{n_i}} \in \frac{1}{u^{t_j}}\mathfrak{S}_n$. To check this we can assume that $n_i \geq t_j + 1$. As

$$t_j + 1 = \lfloor \frac{t_{j-1}}{p} \rfloor + 1 \geq \frac{t_{j-1}+1}{p} \geq \frac{l_{j-1}+1}{p},$$

we get that $pn_i - l_{j-1} \geq 1$. As $\frac{\eta_i}{u^{n_i}} = \frac{\eta_i u^{l_{j-1}-n_i}}{u^{l_{j-1}}}$, from Lemma 1 we get that $E\sigma(C_i u^{l_{j-1}-n_i}) \in (u^{(p-1)l_{j-1}}, p^n)\mathfrak{S}$. This implies that

$$E\sigma(C_i) \in (u^{pn_i - l_{j-1}}, p^n)\mathfrak{S} \subseteq (u, p^n)\mathfrak{S}.$$

As $\eta_i \in \mathfrak{S}_n \setminus u\mathfrak{S}_n$, the constant term of C_i is not divisible by p^n. Thus from Proposition 2 applied to $(C_i, pn_i - l_{j-1})$ instead of (C, t) and from the definition of ϵ in Subsection 3.1, we get $\sigma(p^{\tau+\epsilon}C_i) = p^{\tau+\epsilon}\sigma(C_i) \in (u^{pn_i - l_{j-1}}, p^n)\mathfrak{S}$. This implies that we can write $p^{\tau+\epsilon}C_i = A_i + B_i$, where $A_i \in p^n\mathfrak{S}$ and where $B_i \in u^{n_i - \lfloor \frac{l_{j-1}}{p} \rfloor}\mathfrak{S}$. Thus

$$p^{\tau+\epsilon}\frac{\eta_i}{u^{n_i}} \in \frac{1}{u^{\lfloor \frac{l_{j-1}}{p} \rfloor}}\mathfrak{S}_n \subseteq \frac{1}{u^{\lfloor \frac{t_{j-1}}{p} \rfloor}}\mathfrak{S}_n = \frac{1}{u^{t_j}}\mathfrak{S}_n.$$

Therefore $p^{\tau+\epsilon}y \in \frac{1}{u^{t_j}}M$. As $s_j = s_{j-1} + \tau + \epsilon$ and as $y \in p^{s_{j-1}}N$ is arbitrary, we conclude that $p^{s_j}N = p^{\tau+\epsilon}p^{s_{j-1}}N \subseteq \frac{1}{u^{t_j}}M$. This ends the induction. $\square$

4.2 The case $p = 2$

In this Subsection we assume $p = 2$. Thus $s = v + 2w$, where $w := t_z + s_z$ (cf. Subsection 3.1). Using Theorem 4 as a substitute of Theorem 3, we get:

(i) Everything in Subsection 4.1 holds, provided G and H are connected. In this case Theorem 1 holds with s replaced by w.

We will show the existence of a homomorphism $f' : H \to G$ such that $f \circ f' = p^s \,\mathrm{id}_H$ in four steps. Let us start with three general remarks on finite flat commutative group schemes G and H over a discrete valuation ring V of mixed characteristic $(0, p)$ with field of fractions K.

(a) If H is étale, the natural homomorphism $\mathrm{Hom}(H, G) \to \mathrm{Hom}(H_K, G_K)$ is an isomorphism. Indeed, by passing to an unramified Galois extension K' of K we can assume that H is constant étale. In this case the assertion follows from the fact that V is integrally closed in K.

(b) Let $G \to H$ be a homomorphism such that H is étale. If $G_K \to H_K$ is an fppf epimorphism, then $G \to H$ is also an fppf epimorphism. Indeed, the assumption implies that there exists a K' as in (a) such that we have an epimorphism $G(K') \to H(K')$. To prove that $G \to H$ is an fppf epimorphism, we can pass from K to K'. Thus we can assume that H is constant étale and that $G(K) \to H(K)$ is an epimorphism. But then we find a section of $G_K \to H_K$; by (a) it extends to a section of $G \to H$.

(c) If H is étale, then from (a) we easily get that the natural homomorphism $\mathrm{Ext}^1(H, G) \to \mathrm{Ext}^1(H_K, G_K)$ is a monomorphism.

Step 1. We reduce the existence of f' to the case where H is connected. We consider the short exact sequence $0 \to H^o \to H \to H^{\acute{e}t} \to 0$ such that $H^{\acute{e}t}$

is an étale group scheme over V and H^o is connected. Then f induces an fppf epimorphism $G \to H^{\acute{e}t}$ because this is true in the general fiber, cf. (b). Therefore f induces a morphism of extensions:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_1 & \longrightarrow & G & \longrightarrow & H^{\acute{e}t} & \longrightarrow & 0 \\ & & {\scriptstyle g}\big\downarrow & & {\scriptstyle f}\big\downarrow & & {\scriptstyle \mathrm{id}_{H^{\acute{e}t}}}\big\downarrow & & \\ 0 & \longrightarrow & H^o & \longrightarrow & H & \longrightarrow & H^{\acute{e}t} & \longrightarrow & 0. \end{array} \tag{15}$$

As H^o is connected we can assume that there exists a homomorphism $g' : H^o \to G_1$ such that $g \circ g' = p^s \,\mathrm{id}_{H^o}$. The homomorphism $p^s f_K^{-1} : H_K \to G_K$ is a morphism of extensions inducing g'_K on $H_{1,K}$ and p^s on $H_{2,K}$.

Let $0 \to G_1 \to G^s \to H^{\acute{e}t} \to 0$ be the pull back of the first row in (15) by $p^s \,\mathrm{id}_{H^{\acute{e}t}}$ and let $0 \to G_1 \to G' \to H^{\acute{e}t} \to 0$ be the push forward of the lower row in (15) by g'.

Then $p^s f_K^{-1}$ induces an isomorphism of extensions $G'_K \to G^s_K$. Therefore the extensions G' and G^s are isomorphic, cf. (c). From the choice of an isomorphism $G' \to G^s$ we obtain a commutative diagram of extensions.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_1 & \longrightarrow & G & \longrightarrow & H^{\acute{e}t} & \longrightarrow & 0 \\ & & {\scriptstyle g'}\big\uparrow & & {\scriptstyle f'}\big\uparrow & & {\scriptstyle p^s \mathrm{id}_{H^{\acute{e}t}}}\big\uparrow & & \\ 0 & \longrightarrow & H^o & \longrightarrow & H & \longrightarrow & H^{\acute{e}t} & \longrightarrow & 0. \end{array}$$

With this f' we get $f \circ f' = p^s \,\mathrm{id}_H + u$, where $u : H^{\acute{e}t} \to H^o$ is a homomorphism. But the homomorphism $f_K^{-1} \circ u_K : H_{2,K} \to H_{1,K} \to G_{1,K}$ extends by (a) to a homomorphism $u_1 : H^{\acute{e}t} \to G_1$ such that $f \circ u_1 : H^{\acute{e}t} \to G_1 \to H^o$ is the homomorphism u. Replacing f' by $f' - u_1$ we get $f \circ f' = p^s \,\mathrm{id}_H$. This ends the reduction to the case where $H = H^o$ is connected.

Step 2. We will reduce the existence of f' to the following statement:

(ii) Let $f : G \to H$ be a homomorphism such that f_K is an isomorphism. We assume that G is étale and H is connected. Then there exists a homomorphism $f' : H \to G$ such that $f \circ f' = p^{v+w} \,\mathrm{id}_H$.

Indeed, let $f : G \to H$ be an arbitrary homomorphism such that f_K is an isomorphism. To show the existence of f' we may assume by Step 1 that H is connected. Let G^o be the connected component of G. Let H_1 be the scheme theoretic closure of the homomorphism $G^o \to G \xrightarrow{f} H$. We obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G^o & \longrightarrow & G & \longrightarrow & G^{\acute{e}t} & \longrightarrow & 0 \\ & & {\scriptstyle f_1}\big\downarrow & & {\scriptstyle f}\big\downarrow & & {\scriptstyle f_2}\big\downarrow & & \\ 0 & \longrightarrow & H_1 & \longrightarrow & H & \longrightarrow & H_2 & \longrightarrow & 0 \end{array} \tag{16}$$

whose vertical arrows induce isomorphisms in generic fibers. By (i) and the assertion (ii) we can find homomorphisms $f_1' : H_1 \to G^o$ and $f_2' : H_2 \to G^{\acute{e}t}$ such that $f_1 \circ f_1' = p^w \,\mathrm{id}_{H_1}$ and $f_2 \circ f_2' = p^{v+w} \,\mathrm{id}_{H_2}$.

We denote by $0 \to G^o \to G_2 \to H_2 \to 0$ the pull back of the upper row in (16) by $f_2' : H_2 \to G^{\acute{e}t}$. The push forward of the lower row in (16) by $p^v f_1' : H_1 \to G^o$ will be denoted by $0 \to G^o \to G_1 \to H_2 \to 0$. The commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G^o_K & \longrightarrow & G_K & \longrightarrow & G^{\acute{e}t}_K & \longrightarrow & 0 \\ & & {\scriptstyle p^v f'_{1,K}}\big\uparrow & & {\scriptstyle p^{v+w} f_K^{-1}}\big\uparrow & & {\scriptstyle f'_{2,K}}\big\uparrow & & \\ 0 & \longrightarrow & H_{1,K} & \longrightarrow & H_K & \longrightarrow & H_{2,K} & \longrightarrow & 0, \end{array}$$

induces an isomorphism of extensions $\gamma : G_{1,K} \to G_{2,K}$. The groups G_1 and G_2 are connected and therefore the schematic closure G_{12} of the graph of γ in $G_1 \times_V G_2$ is as well connected. Therefore we find by (i) applied to the first projection $g_1 : G_{12} \to G_1$ a homomorphism $g_1' : G_1 \to G_{12}$ such that $g_1 \circ g_1' = p^w \,\mathrm{id}_{G_1}$. The composite $g := g_2 \circ g_1' : G_1 \to G_2$ extends $p^w \gamma$; here $g_2 : G_{12} \to G_2$ is the second projection. Then the natural composite homomorphism $f' : H \to G_1 \xrightarrow{g} G_2 \to G$ extends the homomorphism $p^{v+2w} f_K^{-1}$ and thus we have $f \circ f' = p^{v+2w} \,\mathrm{id}_H$. This ends the reduction step 2.

Step 3. It remains to prove (ii). Using Cartier duality it suffices to show that there exists a homomorphism $(f^{\mathrm{t}})' : G^{\mathrm{t}} \to H^{\mathrm{t}}$ such that $f^{\mathrm{t}} \circ (f^{\mathrm{t}})' = p^{v+w} \,\mathrm{id}_{G^{\mathrm{t}}}$, where $f^{\mathrm{t}} : H^{\mathrm{t}} \to G^{\mathrm{t}}$ is the Cartier dual of f. We consider a short exact sequence $0 \to H_3 \to H^{\mathrm{t}} \to H_4 \to 0$ such that H_4 is an étale group scheme over V and H_3 is connected. Let G_3 be the schematic closure of $f^{\mathrm{t}}_K(H_{3,K})$ in G^{t}. Let $G_4 := G^{\mathrm{t}}/G_3$. To check the existence of $(f^{\mathrm{t}})'$, it suffices to show that the following two statements hold:

(iii) there exists a homomorphism $f_3' : G_3 \to H_3$ such that $f_3 \circ f_3' = p^w \,\mathrm{id}_{G_3}$;

(iv) both H_4 and G_4 (and thus also $f_4 : H_4 \to G_4$) are annihilated by p^v.

Indeed, as $(f^{\mathrm{t}})'$ we can take $i_3 \circ f_3' \circ f_5$, where $f_5 : G^{\mathrm{t}} \to G_3$ is the natural factorization (cf. (iv)) of the endomorphism $2^v : G^{\mathrm{t}} \to G^{\mathrm{t}}$ and where $i_3 : H_3 \hookrightarrow H^{\mathrm{t}}$ is the natural inclusion.

Both H_3 and G_3 are connected. Thus (iii) holds, cf. (i). Thus to end the argument that f' exists, we are left to prove that (iv) holds.

Step 4. The invariant υ of V does not change when V is replaced by an unramified discrete valuation ring extension of it. Thus to prove (iv), we can assume that k is algebraically closed. Therefore H_4 is a constant étale group scheme and G_4 is isomorphic to a direct sum $\oplus_{i=1}^{l}\boldsymbol{\mu}_{2^{l_i}}$, where l_i's are non-negative integers whose sum is $o(G_4) = o(H_4)$. As $f_{4,K} : H_{4,K} \to G_{4,K}$ is an isomorphism, the étale groups $(\boldsymbol{\mu}_{2^{l_i}})_K$ are constant. Thus, for each i the field K contains a primitive root of 1 of order 2^{l_i}. From this and the definition of υ in Subsection 3.1, we get that we have $l_i \leq \upsilon$ for all $i \in \{1, \ldots, l\}$. Thus 2^{υ} annihilates both H_4 and G_4 i.e., (iv) holds.

This ends the argument that f' exists. Thus Theorem 1 holds even when $p = 2$, cf. (i). This ends the proof of Theorem 1. □

5 Proofs of Corollaries 1 to 4 and Theorem 2

5.1 Proofs of the Corollaries

Corollary 1 follows from Theorem 1 and Example 1.

In connection with the other Corollaries, let $\tilde{G}$ be the schematic closure in $G \times_V H$ of the graph of the homomorphism $h : G_K \to H_K$. Via the two projections $q_1 : G \times_V H \to G$ and $q_2 : G \times_V H \to H$ we get homomorphisms $\rho_1 : \tilde{G} \to G$ and $\rho_2 : \tilde{G} \to H$. The generic fiber $\rho_{1,K}$ of ρ_1 is an isomorphism.

We prove the first part of Corollary 2. Consider the commutative diagram:

$$\begin{array}{ccccc} \tilde{G} & \xrightarrow{\ i\ } & G \times_V H & \xrightarrow{\ q_2\ } & H \\ & \searrow^{\rho_1} & \downarrow{\scriptstyle q_1} & & \\ & & G. & & \end{array}$$

By Theorem 1 there exists a homomorphism $\rho_1' : G \to \tilde{G}$ such that $\rho_1' \circ \rho_1 = p^s \,\mathrm{id}_{\tilde{G}}$. Then $q_2 \circ i \circ \rho_1'$ is the desired extension of $p^s h$.

To check the last part of Corollary 2, let $0 \to G \to J \to H \to 0$ be a short exact sequence whose generic fibre splits. It defines an arbitrary element $\nu \in \mathrm{Ker}(\mathrm{Ext}^1(H, G) \to \mathrm{Ext}^1(H_K, G_K))$. Let $h : H_K \to J_K$ be a homomorphism that is a splitting of $0 \to G_K \to J_K \to H_K \to 0$. Let $g : H \to J$ be such that its generic fibre is $p^s h$, cf. first part of Corollary 2. Let

$0 \to G \to J_s \to H \to 0$ be the pull back of $0 \to G \to J \to H \to 0$ via $p^s \operatorname{id}_H$. Then there exists a unique section $g_s : H \to J_s$ of $0 \to G \to J_s \to H \to 0$ whose composite with $J_s \to J$ is g. Thus $p^s \nu = 0$. This proofs Corollary 2.

We prove Corollary 3. From Theorem 1 we get that $\rho_1\lceil p^{n-s}\rceil : \tilde{G}\lceil p^{n-s}\rceil \to G[p^{n-s}]$ is an isomorphism. This implies that $G[p^{n-s}]$ is a closed subgroup scheme of $G \times_V H$ and thus via the second projection $G \times_V H \to H$ we get a homomorphism $G[p^{n-s}] \to H[p^{n-s}]$ which extends the homomorphism $h[p^{n-s}] : G_K[p^{n-s}] \to H_K[p^{n-s}]$.

We prove Corollary 4 for $n > 2s$. As $h : G_K \to H_K$ is an isomorphism, $\rho_{2,K}$ is also an isomorphism. Thus $\rho_2\lceil p^{n-s}\rceil : \tilde{G}\lceil p^{n-s}\rceil \to H[p^{n-s}]$ is an isomorphism, cf. Theorem 1. By applying Theorem 1 to the Cartier dual $(\rho_1\lceil p^{n-s}\rceil)^{\mathrm{t}} : (G\lceil p^{n-s}\rceil)^{\mathrm{t}} \to (\tilde{G}\lceil p^{n-s}\rceil)^{\mathrm{t}}$ of $\rho_1\lceil p^{n-s}\rceil : \tilde{G}\lceil p^{n-s}\rceil \to G\lceil p^{n-s}\rceil$, we get that $(G\lceil p^{n-s}\rceil)^{\mathrm{t}}\lceil p^{n-2s}\rceil$ is isomorphic to $(\tilde{G}\lceil p^{n-s}\rceil)^{\mathrm{t}}[p^{n-2s}]$ and thus with $H^{\mathrm{t}}[p^{n-2s}]$. Therefore $\{(G\lceil p^{n-s}\rceil)^{\mathrm{t}}\lceil p^{n-2s}\rceil\}^{\mathrm{t}}$ is isomorphic to $H[p^{n-2s}]$. From this and the fact that we have a short exact sequence $0 \to G\lceil p^s\rceil \to G\lceil p^{n-s}\rceil \to \{(G\lceil p^{n-s}\rceil)^{\mathrm{t}}\lceil p^{n-2s}\rceil\}^{\mathrm{t}} \to 0$, we get that the Corollary 4 holds. □

5.2 Proof of Theorem 2

Clearly the homomorphism $g : \mathcal{G}[p^{n-s_Y}] \to \mathcal{H}[p^{n-s_Y}]$ is unique if it exists. We proved the case $Y = \operatorname{Spec} V$ in Corollary 3. Let $y \in Y$ be a point; let $\kappa(y)$ be its residue field and let $\operatorname{Spec} \mathcal{R}_y$ be its local ring. If $h[p^{n-s_Y}]$ extends to a homomorphism $g_y : \mathcal{G}_{\mathcal{R}_y}[p^{n-s_Y}] \to \mathcal{H}_{\mathcal{R}_y}[p^{n-s_Y}]$, then $h[p^{n-s_Y}]$ extends also to a homomorphism $g_{U_y} : \mathcal{G}_{U_y}[p^{n-s_Y}] \to \mathcal{H}_{U_y}[p^{n-s_Y}]$ over an open neighborhood U_y of y in Y. It follows from our assumptions that the extension g_y of $h[p^{n-s_Y}]$ exists for each point $y \in Y$ of codimension 1. Indeed, if $\operatorname{char} \kappa(y) \neq p$ the group schemes $\mathcal{G}_{\mathcal{R}_y}$ and $\mathcal{H}_{\mathcal{R}_y}$ are étale and therefore an extension g_y trivially exists. If $\operatorname{char} \kappa(y) = p$, then Corollary 3 implies that g_y exists provided we have $n > s_y$ for a suitable non-negative integer s_y that depends only on the ramification index of the discrete valuation ring $\mathcal{R}_y$. As the set $\Omega_p(Y)$ of points of Y of codimension 1 and of characteristic p is finite, we can define

$$s_Y := \max\{s_y | y \in \Omega_p(Y)\} \in \mathbb{N}.$$

With this s_Y, there exists an extension $g_U : \mathcal{G}_U[p^{n-s_Y}] \to \mathcal{H}_U[p^{n-s_Y}]$ of $h[p^{n-s_Y}]$ over an open subscheme $U \subseteq Y$ such that $\operatorname{codim}_Y(Y \setminus U) \geq 2$. As Y is a normal noetherian integral scheme, the existence of an extension $g : \mathcal{G}[p^{n-s_Y}] \to \mathcal{H}[p^{n-s_Y}]$ of g_U is a general fact which holds for every locally free coherent $\mathcal{O}_Y$-modules $\mathcal{M}$ and $\mathcal{N}$ and for each homomorphism $\alpha_U : \mathcal{M}_U \to \mathcal{N}_U$ of $\mathcal{O}_U$-modules. □

6 Upper bounds on heights

In this Section we assume that V is complete and k is perfect. Let $\pi \in V$ and $q_\pi : \mathfrak{S} \twoheadrightarrow V$ be as in Section 2. We will study three different heights of a finite flat commutative group scheme G of p power order over V. If $p = 2$, then we will assume that both G and its Cartier dual G^{t} are connected.

Definition 3 **(a)** *By the Barsotti–Tate height of G we mean the smallest non-negative integer $h_1(G)$ such that G is a closed subgroup scheme of a truncated Barsotti–Tate group over V of height $h_1(G)$.*

(b) *By the Barsotti–Tate co-height of G we mean the smallest non-negative integer $h_2(G)$ such that G is the quotient of a truncated Barsotti–Tate group over V of height $h_2(G)$.*

(c) *By the generator height of G we mean the smallest number $h_3(G)$ of generators of the $\mathfrak{S}$-module N, where $(N, \psi) := \mathbb{B}(G)$.*

6.1 Simple inequalities

We have $h_2(G) = h_1(G^{\mathrm{t}})$. If G is a truncated Barsotti–Tate group, then $h_1(G) = h_2(G) = h_3(G)$ are equal to the height of G. Based on these two properties, it is easy to check that in general we have

$$h_3(G) = h_3(G^{\mathrm{t}}) \leq \min\{h_1(G), h_2(G)\}.$$

Lemma 5 *We have $h_1(G) \leq 2h_3(G)$.*

Proof. The proof of this is similar to the proof of [VZ1], Proposition 2 (ii) but worked out in a contravariant way. If $h_4(G) \in \{0, \ldots, h_3(G)\}$ is the smallest number of generators of $\mathrm{Im}(\psi)/EN$, then as in loc. cit. we argue that there exists a Breuil window (Q, ϕ) relative to $q_\pi : \mathfrak{S} \twoheadrightarrow V$ which has rank $h_3(G) + h_4(G)$ and which is equipped naturally with a surjection $(Q, \phi) \twoheadrightarrow (N, \psi)$. More precisely, starting with $\mathfrak{S}$-linear maps $\chi_T : T := \mathfrak{S}^{h_3(G)} \to N$ and $\chi_L : L := \mathfrak{S}^{h_4(G)} \to \mathrm{Im}(\psi)$ such that χ_T is onto and $\mathrm{Im}(\psi) = \mathrm{Im}(\chi_L) + EN$, one can take $Q := T \oplus L$ and the surjection $\chi_T \oplus \chi_L : Q \twoheadrightarrow N$.

The existence of the surjection $(Q, \phi) \twoheadrightarrow (N, \psi)$ implies that G is a closed subgroup scheme of the p-divisible group of height $h_3(G) + h_4(G)$ over V associated to (Q, ϕ). Thus $h_1(G) \leq h_3(G) + h_4(G) \leq 2h_3(G)$. □

If $o(G)$ is as in Section 2, then we obviously have

$$h_3(G) \leq o(G). \tag{17}$$

If we have a short exact sequence

$$0 \to G_1 \to G \to G_2 \to 0$$

of finite flat group schemes over V, then as the functor $\mathbb{B}$ takes short exact sequences to short exact sequences (in the category of $\mathfrak{S}$-modules endowed with Frobenius maps), we have the subadditive inequality

$$h_3(G) \leq h_3(G_1) + h_3(G_2). \tag{18}$$

Proposition 3 *For every truncated Barsotti–Tate group H over V of height r and for each G whose generic fiber is isomorphic to H_K, we have*

$$h_3(G) \leq (2s + 1)h.$$

Therefore we have $\max\{h_1(G), h_2(G), h_3(G)\} \leq (4s + 2)r$.

Proof. Let n be the level of H. If $n \leq 2s$, then from (17) we get that $h_3(G) \leq o(G) \leq 2sr$. We now assume that $n > 2s$. Then from Corollary 4 we get that $G\lceil p^{n-s}\rceil / G\lceil p^s\rceil$ is isomorphic to $H[p^{n-2s}]$ (if $p = 2$, then this forces both H and H^{t} to be connected). Therefore we have $h_3(G\lceil p^{n-s}\rceil / G\lceil p^s\rceil) = r$.

As the orders of $G\lceil p^s\rceil$ and $G/G\lceil p^{n-s}\rceil$ are equal to sr, from inequalities (17) and (18) we get first that $h_3(G\lceil p^{n-s}\rceil) \leq h_3(G\lceil p^{n-s}\rceil / G\lceil p^s\rceil) + h_3(G\lceil p^s\rceil) \leq r + sr = (s + 1)r$ and second that $h_3(G) \leq h_3(G\lceil p^{n-s}\rceil) + h_3(G/G\lceil p^{n-s}\rceil) \leq (s + 1)r + sr = (2s + 1)r$.

The group scheme G^{t} satisfies the same property as G i.e., G^{t}_K is isomorphic to H^{t}_K and, in the case when $p = 2$, it is connected and has a connected Cartier dual. Thus we also have $h_3(G^{\mathrm{t}}) \leq (2s + 1)r$. From this and Lemma 5 we get that $h_2(G) = h_1(G^{\mathrm{t}}) \leq 2h_3(G) \leq (4s + 2)r$. Similarly, $h_1(G) \leq 2h_3(G) \leq (4s + 2)r$. Thus $\max\{h_1(G), h_2(G), h_3(G)\} \leq (4s + 2)r$.□

Acknowledgments. Both authors would like to thank Bielefeld and Binghamton Universities for good work conditions.

References

[Br] Breuil, Ch.: *Schémas en groupes et corps de normes,* 13 pages, unpublished manuscript (1998).

[Bo] Bourbaki, N.: *Éléments de mathématique. Algèbre commutative. Chapitres 5 à 7.* Reprint. Masson, Paris, 1985.

[R] Raynaud, M.: *Schémas en groupes de type (p,...,p),* Bull. Soc. Math. France, Vol. **102** (1974), pp. 241–280.

[K1] Kisin, M.: *Crystalline representations and F-crystals,* Algebraic geometry and number theory, pp. 459–496, Progr. Math., Vol. **253**, Birkhäuser Boston, Boston, MA, 2006.

[K2] Kisin, M.: *Modularity of 2-adic Barsotti–Tate representations,* Invent. Math.. Vol. **178** (2009), no. 3, pp. 587–634.

[L] Lau, E.: *Frames and finite group schemes over complete regular local rings,* 22 pages, http://arxiv.org/abs/0908.4588.

[T] Tate, J.: *p-divisible groups,* 1967 Proc. Conf. Local Fields (Driebergen, 1966), pp. 158–183, Springer, Berlin.

[V] Vasiu, A.: *Crystalline boundedness principle,* Ann. Sci. École Norm. Sup. **39** (2006), no. 2, pp. 245–300.

[VZ1] Vasiu, A. and Zink, Th.: *Breuil's classification of p-divisible groups over regular local rings of arbitrary dimension,* to appear in Advanced Studies in Pure Mathematics, Proceeding of Algebraic and Arithmetic Structures of Moduli Spaces, Hokkaido University, Sapporo, Japan, 2007.

[VZ2] Vasiu, A. and Zink, Th.: *Purity results for p-divisible groups and abelian schemes over regular bases of mixed characteristic,* 28 pages, http://arxiv.org/abs/0909.0969.

[Z1] Zink, Th.: *The display of a formal p-divisible group,* Cohomologies p-adiques et applications arithmétiques. I, J. Astérisque, No. **278** (2002), pp. 127–248.

[Z2] Zink, Th.: *Windows for displays of p-divisible groups.* Moduli of abelian varieties (Texel Island, 1999), pp. 491–518, Progr. Math., Vol. **195**, Birkhäuser, Basel, 2001.

Adrian Vasiu, Email: adrian@math.binghamton.edu
Address: Department of Mathematical Sciences, Binghamton University, Binghamton, New York 13902-6000, U.S.A.

Thomas Zink, Email: zink@math.uni-bielefeld.de
Address: Fakultät für Mathematik, Universität Bielefeld,
P.O. Box 100 131, D-33 501 Bielefeld, Germany.