MINIMAL TRUNCATIONS OF SUPERSINGULAR $p$-DIVISIBLE GROUPS

MARC-HUBERT NICOLE AND ADRIAN VASIU

ABSTRACT. Let $k$ be an algebraically closed field of characteristic $p > 0$. Let $H$ be a supersingular $p$-divisible group over $k$ of height $2d$. We show that $H$ is uniquely determined up to isomorphism by its truncation of level $d$ (i.e., by $H[p^d]$). This proves Traverso’s truncation conjecture for supersingular $p$-divisible groups. If $H$ has a principal quasi-polarization $\lambda$, we show that $(H, \lambda)$ is also uniquely determined up to isomorphism by its principally quasi-polarized truncated Barsotti–Tate group of level $d$ (i.e., by $(H[p^d], \lambda[p^d])$).

MSC 2000: 11G10, 11G18, and 14L05.

1. Introduction

Let $p \in \mathbb{N}$ be a prime. Let $k$ be an algebraically closed field of characteristic $p$. Let $c, d \in \mathbb{N}$. Let $H$ be a $p$-divisible group over $k$ of codimension $c$ and dimension $d$; thus the height of $H$ is $c + d$. Let $n \in \mathbb{N}$ be the smallest number such that $H$ is uniquely determined up to isomorphism by $H[p^n]$ (i.e., if $H_1$ is a $p$-divisible group over $k$ such that $H_1[p^n]$ is isomorphic to $H[p^n]$, then $H_1$ is isomorphic to $H$). Thus $H[p^n]$ is the minimal truncation of $H$ which determines $H$. It is known that the number $n$ admits upper bounds that depend only on $c$ and $d$ (see [Ma], [Tr1, Thm. 3], [Tr2, Thm. 1], [Va1, Cor. 1.3], and [Oo, Cor. 1.7]). For instance, Traverso proved that $n \leq cd + 1$ (see [Tr1, Thm. 3]). Traverso’s work on Grothendieck’s specialization conjecture led him to speculate that much more is true (cf. [Tr3, §40, Conj. 4]):

Conjecture 1.1. We have $n \leq \min\{c, d\}$.

We suppose for the remainder of the paper that the codimension and the dimension of $H$ are equal. We recall that $H$ is called supersingular if all the slopes of its Newton polygon are $\frac{1}{2}$. We prove the Conjecture for the supersingular case:

Theorem 1.2. Suppose $H$ is a supersingular $p$-divisible group over $k$ of height $2d$. Then $n \leq d$ i.e., $H$ is uniquely determined up to isomorphism by $H[p^d]$.

Theorem 1.2 strengthens Traverso’s and Vasiu’s results (see [Tr1, Thm. 3] and [Val1, Prop. 4.1.1]) which worked with $H[p^{d+1}]$ and $H[p^{d^2}]$ (respectively). Theorem 1.2 was originally claimed in [Ni, §1.4]. It turns out that [Ni, Lem. 1.4.4, Cor. 1.4.7] are incorrect as stated. The proof in the present paper uses elementary methods of $\sigma$-linear algebra to avoid those issues completely.

For the sake of completeness, we also prove the following principally quasi-polarized variant of Theorem 1.2.

\begin{flushright}
Date: August 27, 2018.
\end{flushright}
Theorem 1.3. Suppose $H$ is a supersingular $p$-divisible group over $k$ of height $2d$ which has a principal quasi-polarization $\lambda$. Then $(H, \lambda)$ is uniquely determined up to isomorphism by $(H[p^d], \lambda[p^d])$ (i.e., by its principally quasi-polarized truncated Barsotti–Tate group of level $d$).

Theorem 1.3 refines and extends [Va1, Prop. 4.1.1]. Theorems 1.2 and 1.3 are optimal (i.e., they do not hold if $[p^d]$ gets replaced with $[p^{d-1}]$; see Example 3.3). Theorems 1.2 and 1.3 and Corollary 3.2 represent progress towards:

(i) the classification of (principally quasi-polarized) supersingular $p$-divisible groups, and

(ii) the understanding of the ultimate stratifications introduced in [Va1, Basic Thm. 5.3.1 and Subsubsection 5.3.2] and of the level $m$ stratifications introduced in [Va2, Subsections 4.2 and 4.4].

In Section 2, we introduce notations and basic invariants which pertain to supersingular $p$-divisible groups and which allow us to get a more precise form of Theorem 1.2 (see Corollary 3.2). In Sections 3 and 4, we prove Theorems 1.2 and 1.3 (respectively). Note that the proof of Theorem 1.2 is self-contained.

2. Basic invariants of supersingular Dieudonné modules

Let $W(k)$ be the ring of Witt vectors with coefficients in $k$. For $s \in \mathbb{N}$, let $W_s(k) := W(k)/(p^s)$. Let $\sigma$ be the Frobenius automorphism of $W(k)$ (or $W_s(k)$) induced from $k$.

Proposition 2.1. Let $G$ be a smooth group scheme over $\text{Spec}(\mathbb{Z}_p)$ such that its special fibre $G_{\mathbb{F}_p}$ is a connected, affine scheme. Let $\sigma$ act naturally on $G(W(k))$. Then we have $G(W(k)) = \{g_0^{-1}\sigma(g_0)|g_0 \in G(W(k))\}$.

Proof: Let $g \in G(W(k))$. By induction on $s \in \mathbb{N}$, we check that there exists an element $g_s \in G(W(k))$ such that the following two properties hold:

(i) we have $g_s g \sigma(g_s)^{-1} \in \text{Ker}(G(W(k)) \to G(W_s(k)))$, and

(ii) for $s \geq 2$, the images of $g_s$ and $g_{s-1}$ in $G(W_{s-1}(k))$ coincide.

Let $\sigma$ act naturally on $G(W_s(k))$. As $G_{\mathbb{F}_p}$ is affine and connected, there exists $\bar{g}_1 \in G(k)$ such that $\bar{g}_1^{-1}\sigma(\bar{g}_1)$ is the reduction mod $p$ of $g$ (cf. Lang’s theorem in [Bo, Ch. V, Cor. 16.4]). If $g_1 \in G(W(k))$ lifts $\bar{g}_1$, then we have $g_1 g \sigma(g_1)^{-1} \in \text{Ker}(G(W(k)) \to G(k))$. Thus the basis of the induction holds. The passage from $s$ to $s+1$ goes as follows. As $G$ is smooth, the group $\text{Ker}(G(W_{s+1}(k)) \to G(W_s(k)))$ is the group of $k$-valued points of the vector group $V$ over $\mathbb{F}_p$ defined by $\text{Lie}(G_{\mathbb{F}_p})$. From Lang’s theorem applied to $V$, we get that there exists $\bar{g}_{s+1} \in \text{Ker}(G(W_{s+1}(k)) \to G(W_s(k)))$ such that $(\bar{g}_{s+1})^{-1}\sigma(\bar{g}_{s+1})$ is the image of $g_s g \sigma(g_s)^{-1}$ in $\text{Ker}(G(W_{s+1}(k)) \to G(W_s(k)))$. Let $g_{s+1} \in G(W(k))$ be an element that lifts $\bar{g}_{s+1}$. If $g_{s+1} := g_{s+1} g_s \in G(W(k))$, then we have $g_{s+1} g \sigma(g_{s+1})^{-1} \in \text{Ker}(G(W(k)) \to G(W_{s+1}(k)))$. Moreover, as $\bar{g}_{s+1} \in \text{Ker}(G(W_{s+1}(k)) \to G(W_s(k)))$, the images of $g_{s+1}$ and $g_s$ in $G(W_s(k))$ coincide. This ends the induction.

Due to the property (ii), the $p$-adic limit of the sequence $(g_s)_{s \in \mathbb{N}}$ is an element $g_{\infty}$ in $G(W(k))$. Due to the property (i), the element $g_{\infty} g \sigma(g_{\infty})^{-1}$ is the identity. Thus $g_{\infty}^{-1} \sigma(g_{\infty}) = g$. This implies that $G(W(k)) = \{g_0^{-1} \sigma(g_0)|g_0 \in G(W(k))\}$. \(\Box\)
2.1. Let $H$ be a supersingular $p$-divisible group over $k$ of height $2d$, for $d \in \mathbb{N}$. Let $(M, \phi)$ be the (contravariant) Dieudonné module of $H$. Thus $M$ is a free $W(k)$-module of rank $2d$ and $\phi : M \to M$ is a $\sigma$-linear endomorphism such that we have $pM \subset \phi(M)$. Let $\vartheta : M \to M$ be the Verschiebung map of $(M, \phi)$; we have $\vartheta \phi = \phi \vartheta = p1_M$. We denote also by $\phi$ the $\sigma$-linear automorphism of $\text{End}(M[1/p])$ that takes $e \in \text{End}(M[1/p])$ to $\phi(e) := \phi \circ e \circ \phi^{-1} \in \text{End}(M[1/p])$. Let $A := \{e \in \text{End}(M) | \phi(e) = e\}$ be the $\mathbb{Z}_p$-algebra of endomorphisms of $(M, \phi)$. Let $A$ be the smooth, affine group scheme over $\text{Spec}(\mathbb{Z}_p)$ of invertible elements of the $\mathbb{Z}_p$-algebra $A$. Let $O$ be the $W(k)$-span of $A$. As all slopes of $(M, \phi)$ are $\frac{1}{2}$, all slopes of $(\text{End}(M[1/p]), \phi)$ are $0$. This implies that $O$ is a $W(k)$-subalgebra of $\text{End}(M)$ such that the quotient $W(k)$-module $\text{End}(M)/O$ is torsion. Let $E$ be the (unique up to isomorphism) supersingular $p$-divisible group over $k$ of height $2$. Let $(N, \varphi)$ and $(N^d, \varphi)$ be the Dieudonné modules of $E$ and $E^d$ (respectively).

Let $n \in \mathbb{N}$ be as in Section 1. We list two additional basic invariants of $H$:

- Let $m \in \mathbb{N}$ be the smallest number such that $p^m \text{End}(M) \subset O \subset \text{End}(M)$.
- Let $q \in \mathbb{N} \cup \{0\}$ be the smallest number such that there exists a monomorphism $j : (N^d, \varphi) \hookrightarrow (M, \phi)$ with the property that $\phi^q(M) \subset j(N^d)$.

Thus $m$ is the Fontaine–Dieudonné torsion of $(\text{End}(M), \phi)$ defined in [Va1, 2.2.2 (b)]. We have $q = 0$ if and only if there exists an isomorphism $(N^d, \varphi) \cong (M, \phi)$.

**Theorem 2.2.** Let $(M, \phi)$ be a supersingular Dieudonné module over $k$, and let $H$ be the corresponding $p$-divisible group. Let $n$, $m$, and $O$ be as above.

(a) Let $t \in \mathbb{N}$ be the smallest number such that for each element $g \in \text{GL}_M(W(k))$ congruent mod $p^t$ to $1_M$, there exists an isomorphism between the two Dieudonné modules $(M, \phi g)$ and $(M, \phi)$. Then $t = n$, i.e., $t$ is the smallest number such that $H$ is uniquely determined up to isomorphism by $H[p^t]$.

(b) Let $g \in \text{GL}_M(W(k)) \cap O$. Then $(M, \phi g)$ and $(M, \phi)$ are isomorphic.

(c) If $p^m \text{End}(M) \subset O \subset \text{End}(M)$ then $H$ is determined up to isomorphism by $H[p^m]$ i.e., we have an inequality $n \leq m$.

**Proof:** We first prove (a). This is a special case of [Va1, Lemma 3.2.2] for the group $G = \text{GL}_M$, but for the sake of completeness we include a self-contained proof which works for all $p$-divisible groups over $k$. Let us first show that $t \leq n$. Let $g \in \text{GL}_M(W(k))$ be congruent mod $p^n$ to $1_M$. Let $H_g$ be the $p$-divisible group over $k$ whose Dieudonné module is $(M, \phi g)$. Then $H_g[p^n] = H[p^n]$ and thus $H_g$ and $H$ are isomorphic i.e., $(M, \phi)$ and $(M, \phi g)$ are isomorphic. Thus $t \leq n$.

Second, we show that $n \leq t$. Let $H_t$ be a $p$-divisible group over $k$ such that $H_t[p^t]$ and $H[p^t]$ are isomorphic. Let $g \in \text{GL}_M(W(k))$ be such that the Dieudonné module of $H_t$ is isomorphic to $(M, \phi g)$. As $H_t[p^t]$ and $H[p^t]$ are isomorphic, we can assume that $(M, \phi g, \vartheta g^{-1}) \bmod p^t$ is $(M, \phi, \vartheta) \bmod p^t$. This implies that $g$ fixes $\phi(M)/p^t M$ and $M/p^{t-1} \phi(M)$. Since $g$ fixes $pM/p^t M \subset \phi(M)/p^t M$, there exists $u \in \text{End}(M)$ such that $g = 1_M + p^{t-1} u$. As $g$ fixes $\phi(M)/p^t M$ and $M/p^{t-1} \phi(M)$, we get that $u \bmod p$ annihilates $\phi(M)/p^t M$ and $M/\phi(M)$. Thus $u(\phi(M)) \subset pM$ and $u(M) \subset \phi(M)$. This implies that $u^2 \in \text{End}(M)$, that $(\vartheta^{-1} u \phi)(M) \subset \phi^{-1} (pM) = \vartheta(M)$, and that $(\vartheta^{-1} u \phi)(\vartheta(M)) = \vartheta^{-1} (u(pM)) \subset pM$. Let $v := \vartheta^{-1} u \phi \in \text{End}(M)$; we have $u = \phi(v)$ and $v \bmod p$ fixes $\vartheta(M)/p^t M$ and $M/\phi(M)$. As $\vartheta(M)/p^t M$ is
the kernel of $\phi$ mod $p$, it is easy to see that we can write $v = pv_1 + v_2$, where $v_1, v_2 \in \text{End}(M)$ and $\phi(v_2) \in \text{pEnd}(M)$.

If $g' \in \text{Ker}(GL_M(W(k)) \to GL_M(W_1(k)))$ and if $(M, g'g\phi)$ is isomorphic to $(M, \phi)$, then $(M, g\phi)$ is isomorphic to $(M, g'\phi)$ for some $g' \in \text{Ker}(GL_M(W(k)) \to GL_M(W_1(k)))$; thus $(M, g\phi)$ is also isomorphic to $(M, \phi)$ (cf. the definition of $t$). Thus to show that $(M, g\phi)$ and $(M, \phi)$ (i.e., that $H_t$ and $H$) are isomorphic, we can replace $g$ by any element of $GL_M(W(k))$ congruent mod $p^t$ to $g$. In other words, we can replace $u$ by any element of $u + \text{pEnd}(M)$. By replacing $u$ with $u - \phi(v_2)$ and $v$ with $v_1 = v - v_2$, we can assume that $v = pv_1 \in \text{pEnd}(M)$. We define $g_1 := (1 - p^t v_1)^{-1} \in \text{Ker}(GL_M(W(k)) \to GL_M(W_1(k)))$ and $g_2 := g_1 g\phi(g_1^{-1})$. We have $g_2 = g_1 g\phi(1 - p^t v_1) = g_1 (1 + p^t - 1 u)(1 - p^t u) = g_1 (1 - p^{2t - 2} u^2)$. As $u^2 \in \text{pEnd}(M)$ and $t \geq 1$, we have $p^{2t - 2} u^2 \in \text{pEnd}(M)$. Thus $g_2$ is congruent mod $p^t$ to $1_M$. From the definition of $t$ we get that $(M, g_2\phi)$ and $(M, \phi)$ are isomorphic. As $g_2\phi = g_1 g\phi g_1^{-1}$, we conclude that $(M, g\phi)$ and $(M, \phi)$ are isomorphic. Thus $H_t$ and $H$ are isomorphic. This implies that $n \leq t$. Thus $n = t$ and therefore (a) holds.

Part (b) is a particular case of [Va1, proof of Cor. 3.3.4], but we provide here a simpler argument which works for all isoclinic $p$-divisible groups. The inverse in $GL_M(W(k))$ of the element $g \in O$ is a polynomial in $g$ with coefficients in $W(k)$ (cf. the Cayley–Hamilton theorem) and thus it belongs to $O$. Thus $g$ has an inverse in $O$ and therefore $g \in \mathcal{A}(W(k))$. Each invertible element of $O$ is also an invertible element of $\text{End}(M)$ and therefore we have $\mathcal{A}(W(k)) \subseteq GL_M(W(k))$.

The automorphism $\sigma$ acts naturally on $\mathcal{A}(W(k))$. As $\mathcal{A}$ is an open subscheme of the vector group scheme over $\text{Spec}(\mathbb{Z}_p)$ defined by $A$, its fibres are connected. Thus there exists $g_0 \in \mathcal{A}(W(k))$ such that $g_0^{-1} \sigma(g_0) = g$, cf. Proposition 2.1. We have $g_0 g\sigma(g_0)^{-1} = 1_M$. As $\sigma(g_0) = \phi(g_0)$, we have $g_0 g\phi g_0^{-1} = \phi$. Thus $g_0$ is an isomorphism between $(M, g\phi)$ and $(M, \phi)$.

Based on (a), to prove (c) it suffices to show that for each element $g \in GL_M(W(k))$ congruent mod $p^n$ to $1_M$, the Dieudonné modules $(M, g\phi)$ and $(M, \phi)$ are isomorphic. As $g - 1_M \in p^n \text{End}(M) \subseteq O$, we have $g \in O$. Thus $(M, g\phi)$ and $(M, \phi)$ are isomorphic, cf. (b). Thus (c) holds.

Scholium 2.3. Let $\{x, y\}$ be a $W(k)$-basis for $N$ such that $\varphi(x) = y$ and $\varphi(y) = px$. Thus $\{px, y\}$ is a $W(k)$-basis for $\varphi(N)$ and we have $\phi(px) = py$ and $\phi^2(px) = \phi(py) = p^2x$. The image of the map $\varphi^2 - p1_N : N \to N$ is $pN$. Let $N^* := \text{Hom}(N, W(k))$. Let $\{x^*, y^*\}$ be the $W(k)$-basis for $N^*$ which is the dual of $\{x, y\}$. Thus $\{x \otimes x^*, y \otimes y^*, x \otimes y^*, y \otimes x^*\}$ is a $W(k)$-basis for $\text{End}(N) = N \otimes W(k)$.

The $\sigma$-linear automorphism $\varphi$ of $\text{End}(N[1/2])$ permutes $x \otimes x^*$ and $y \otimes y^*$ as well as $px \otimes y^*$ and $y \otimes x^*$. Thus $\{x \otimes x^*, y \otimes y^*, px \otimes y^*, y \otimes x^*\}$ is a $W(k)$-basis for the $W(k)$-span $O_k$ of endomorphisms of $(N, \varphi)$. We have inclusions $p\text{End}(N) \subsetneq O_k \subsetneq \text{End}(N)$.

Let $O_d$ be the $W(k)$-span of the $\mathbb{Z}_p$-algebra of endomorphisms of $(N^d, \varphi)$. The inclusion $O_d \subsetneq \text{End}(N^d)$ can be identified with the inclusion of matrix $W(k)$-algebras $M_d(O_1) \subseteq M_d(\text{End}(N))$. Thus we have $p\text{End}(N^d) \subsetneq O_d \subsetneq \text{End}(N^d)$. If $H \cong E^d$, we thus retrieve the well-known result that $H$ is determined by its $p$-kernel, since $n \leq m = 1$.

Lemma 2.4. Let $d$ be a natural number and let $(N^d, \varphi)$ be as above. Let $(M, \phi)$ be a supersingular Dieudonné module of rank $2d$. Then there exists a monomorphism $j : (N^d, \varphi) \rightarrow (M, \psi)$ for which $\psi^{d-1}(M)$ is contained in $j(N^d)$ i.e., $q \leq d - 1$. 

Proof: We prove the Lemma by induction on \( d \in \mathbb{N} \). If \( d = 1 \), then \( H \) is isomorphic to \( E \) and thus \( q = 0 \). Suppose \( d > 2 \). We consider a short exact sequence
\[
0 \to (N, \varphi) \to (M, \phi) \to (M_1, \phi_1) \to 0
\]
of supersingular Dieudonné modules over \( k \). As the rank of \( M_1 \) is \( 2d-2 \), by induction there exists a monomorphism \( j_1 : (N^{d-1}, \varphi) \to (M_1, \phi_1) \) such that \( \phi_{d-2}^{d}(M_1) \subseteq j_1(N^{d-1}) \). Let \( M_2 \) be the inverse image of \( \phi_1(j_1(N^{d-1})) \) in \( M \).

We have a short exact sequence
\[
0 \to (N, \varphi) \to (M_2, \phi) \to (\phi_1(j_1(N^{d-1})), \phi_1) \to 0
\]
of supersingular Dieudonné modules over \( k \). We check that the short exact sequence (1) splits. The Dieudonné module \( (\phi_1(j_1(N^{d-1})), \phi_1) \) is a direct sum of supersingular Dieudonné modules of rank 2 which have \( W(1) \) splits. The Dieudonné module \( k \) such \( W \) (see Scholium 2.3). Thus to check that (1) splits, it suffices to show that for each \( \phi \) and moreover, we have
\[
\phi_1(j_1(N^{d-1})), \phi_1 \to 0
\]
that it maps to \( E \) to \( y \) : \( \mu \) such that \( \phi \) and thus
\[
\phi_1(j_1(N^{d-1})), \phi_1 \to 0
\]
maps to \( x \), cf. (ii). Let \( y_1 := \phi_1(x_1) - px_1 \); it is an element of \( pN \). Let \( y_2 \in N \) be such that \( \phi_2(y_2) = py_1 \). Let \( x_2 \in pM \) and \( y_2 \in pN \), we have \( \frac{1}{p}\phi(x_2) = \frac{1}{p}\phi(x_1) + \frac{1}{p}\phi(y_2) \in M \). As \( \frac{1}{p}\phi(x_2) \) maps to \( y \), we have \( \frac{1}{p}\phi(x_2) \in M_2 \). Thus the element \( x_2 \) exists. As \( \phi_{d-2}^{d}(M_1) \subseteq j_1(N^{d-1}) \), we have \( \phi_{d-2}^{d}(M_1) \subseteq \phi_1(j_1(N^{d-1})) \). This implies that \( \phi^{d-1}(M) \subseteq M_2. \) As the short exact sequence (1) splits, there exists an isomorphism \( j_2 : (N^{d}, \varphi) \to (M_2, \phi) \). Its composite with the monomorphism \( (M_2, \phi) \to (M, \phi) \) is a monomorphism \( j : (N^{d}, \varphi) \to (M, \phi) \) such that we have \( \phi^{d-1}(M) \subseteq j(N^{d}) = M_2. \) Thus \( q \leq d - 1. \)

This ends the induction. \( \square \)

Remark 2.5. Lemma 2.4 follows also from [Ma, Thm. 3.7].

Remark 2.6. The smallest number \( k \in \mathbb{N} \cup \{0\} \) such that there exists an isogeny \( H \to E^d \) whose kernel is annihilated by \( p^k \), is \( \lceil \frac{d}{2} \rceil \) (i.e., it is the smallest number such that \( p^k \) annihilates \( N^d/\phi^k(N^d) \)).

Scholium 2.7. For \( i \in \mathbb{N} \cup \{0\} \), let \( f(i) \) be the biggest integer such that \( M \subseteq p^{f(i)}\phi^i(M) \). We have
\[
O = \bigcup_{i=0}^{\infty} \phi^i(\operatorname{End}(M)) = \bigcap_{i=0}^{\infty} \operatorname{End}((\phi^i(M)) = \bigcap_{i=0}^{\infty} \operatorname{End}(p^{f(i)}\phi^i(M)).
\]
Thus the Fontaine-Dieudonné torsion \( m \in \mathbb{N} \) is the smallest number such that
\[
M \subseteq \bigcup_{i=0}^{m} p^{f(i)}\phi^i(M) \subseteq p^{-m}M.
\]

3. Proof of Theorem 1.2

We recall that \( d \in \mathbb{N} \), that \( H \) is a supersingular \( p \)-divisible group over \( k \) of height \( 2d \), that \( (M, \phi) \) is the Dieudonné module of \( H \), and that we have introduced three invariants \( n, m, \) and \( q \) of \( H \) (see Subsection 2.1).

Theorem 3.1. We have inclusions \( p^{q+1} \operatorname{End}(M) \subseteq O \subseteq \operatorname{End}(M) \) i.e., \( m \leq q + 1. \).
Proof: We prove the Theorem by a step 2 induction on $q \in \mathbb{N} \cup \{0\}$. If $q = 0$, then $H$ is isomorphic to $E^d$ and thus $m = 1 = q + 1$ (cf. Scholium 2.3).

Let $q = 1$. Let $j : (N^d, \varphi) \rightarrow (M, \phi)$ be a monomorphism such that $\phi(M) \subseteq j(N^d)$. We have $j(N^d) \subseteq M \subseteq \phi^{-1}(j(N^d))$. This implies that we have a direct sum decomposition $j(N^d) = X \oplus Y_1 \oplus Y_2$ such that $M = X \oplus \frac{1}{p}Y_1 \oplus Y_2$, $\phi(X) = Y_1 \oplus Y_2$, and $\phi(Y_1 \oplus Y_2) = pX$. Let $i \in \mathbb{N}$. If $i$ is even, then $p^{-\frac{i}{2}} \phi^i(M) = \frac{1}{p}X \oplus \frac{1}{p}X_{1i} \oplus \frac{1}{p}Y_{21}$, where $X_{1i} := p^{-\frac{i}{2}} \phi^i(Y_1)$ and $Y_{2i} := p^{-\frac{i}{2}} \phi^i(Y_2)$. As $Y = Y_1 \oplus Y_2$, we have $M \subseteq p^{-\frac{i}{2}} \phi^i(M) \subseteq p^{-2}M$. If $i = 2l + 1$ is odd, then $p^{-l-i} \phi^i(M) = \frac{1}{p}X_{1i} \oplus \frac{1}{p}X_{2i} \oplus \frac{1}{p}Y_{1i} \oplus \frac{1}{p}Y_{2i}$, where $X_{1i} := p^{-l-1} \phi^i(Y_1)$ and $X_{2i} := p^{-l-1} \phi^i(Y_2)$. As $X = X_{1i} \oplus X_{2i}$, we have $M \subseteq p^{-l-1} \phi^i(M) \subseteq p^{-1}M$. Regardless of what $i \in \mathbb{N}$ is, we have $M \subseteq \cup_{i \in \mathbb{N}} \phi^i(M) \subseteq p^{-2}M$ and thus $m \leq 2 = q + 1$ (cf. Scholium 2.7).

Suppose $q \geq 2$. Let $j : (N^d, \varphi) \rightarrow (M, \phi)$ be a monomorphism such that $\phi^q(M) \subseteq j(N^d)$. Thus $\phi^{-2}(M) \subseteq \phi^{-2}(j(N^d)) = \frac{1}{p^2}j(N^d)$. Let $\tilde{M} := \frac{1}{p^2}j(N^d) + M$. Let $\tilde{\phi}$ be the $W(k)$-subalgebra of $\text{End}(\tilde{M})$ generated by endomorphisms of $(M, \phi)$. We have $\phi^{q-2}(M) = \phi^{q-2}(j(N^d)) + \phi^{q-2}(M) \subseteq j(N^d) + \frac{1}{p}j(N^d) \subseteq \frac{1}{p}j(N^d)$. Let $j : (N^d, \phi) \rightarrow (\tilde{M}, \tilde{\phi})$ be a monomorphism whose image is $\frac{1}{p}j(N^d)$. We have $\phi^{q-2}(M) \subseteq j(N^d) \subseteq \tilde{M}$. Thus by induction, we have $p^{q-1}\text{End}(M) \subseteq \tilde{O}$. As $M \subseteq \tilde{M} \subseteq \frac{1}{p}M$, we have $p\text{End}(M) \subseteq \text{End}(M) \subseteq \frac{1}{p}\text{End}(M)$. This implies that $p^{q+1}\text{End}(M) \subseteq p^q\text{End}(\tilde{M}) \subseteq p\tilde{O} \subseteq p\text{End}(\tilde{M}) \subseteq \text{End}(M)$.

As $p\tilde{O}$ is $W(k)$-generated by elements fixed by $\phi$ and as $p\tilde{O} \subseteq \text{End}(M)$, we have $p\tilde{O} \subseteq O$. Thus $p^{q+1}\text{End}(M) \subseteq p\tilde{O} \subseteq O$. This implies that $m \leq q + 1$. This ends the induction. \hfill \Box

From Theorem 2.2 (c), Theorem 3.1, and Lemma 2.4 we get:

Corollary 3.2. For each supersingular $p$-divisible group $H$ over $k$ of height $2d$, we have inequalities $n \leq m \leq q + 1 \leq d$.

This implies $n \leq d$ and ends the proof of Theorem 1.2.

Example 3.3. Let $d \geq 2$. Suppose there exists a $W(k)$-basis $\{e_1, \ldots, e_{2d}\}$ for $M$ such that for $i \in \{1, \ldots, d\}$, we have $\phi(e_i) = e_{i+1}$ and for $i \in \{d+1, \ldots, 2d\}$, we have $\phi(e_i) = pe_{i+1} + 1$. We denote the corresponding $p$-divisible group by $C_d$. Let $(M, \phi_1)$ be the Dieudonné module with the property that $\phi_1(e_i) = \phi(e_i)$ if $i \neq d+1$ and $\phi_1(e_{d+1}) = \phi^{d+1}_1(e_1) = pe_{d+2} + p^{d+1}e_2$. Let $H_1$ be the $p$-divisible group over $k$ whose Dieudonné module is $(M, \phi_1)$. We have $\phi^{d+1}_1(e_1) = p^d e_1 + p^{d+1}e_{d+1} \in p^{d+1}M \setminus p^d M$. But $\phi^{2d}(M) = p^d M$. From the last two sentences, we get that $(M, \phi_1)$ is not isomorphic to $(M, \phi)$ (i.e., $H_1$ is not isomorphic to $C_d$). It is easy to see that $\phi$ and $\phi_1 := p\phi^{-1}_1$ are congruent mod $p^{d-1}$ to $\phi$ and $\phi := p\phi^{-1}$ (respectively). Thus $C_d[p^{d-1}] = H_1[p^{d-1}]$. From the last two sentences, we get that $C_d$ is not determined by $C_d[p^{d-1}]$. Thus $n \geq d$. From this and Corollary 3.2, we obtain the equalities $n = m = q + 1 = d$; thus the inequalities of Corollary 3.2 are best possible.

We now discuss the polarized case. Let $\theta$ be an invertible element of $W(k)$ such that we have $\phi^d(\theta) = -\theta$. Let $\psi : M \otimes W(k) M \to W(k)$ be the perfect, alternating form on $M$ such that the following two properties hold: (i) for $i, j \in \{1, \ldots, 2d\}$ with $|j - i| \neq d$, we have $\psi(e_i, e_j) = 0$, and (ii) for $i \in \{1, \ldots, d\}$
we have $\psi(e_i, e_{i+d}) = -\psi(e_i, e_{i+d}) = \sigma^{i-1}(\theta)$. It is easy to see that $\psi$ is a principal quasi-polarization of both $(M, \phi)$ and $(M, \phi_1)$. Thus, if $\lambda$ is the principal quasi-polarization of $C_d$ defined by $\psi$, then $(C_d, \lambda)$ is not determined by $(C_d[p^d-1], \lambda[p^d-1])$.

**Remark 3.4.** If $s \in \{2, \ldots, d\}$ and $H \cong C_s \times E^{d-s}$, then $q = s - 1$ (cf. Example 3.3). Thus $q$ can be any number in the set $\{0, \ldots, d - 1\}$. If $d = 2\ell$ is even and $H \cong C_{2\ell}$, then $q = 1$ and the $a$-number $\dim_a(Hom(\alpha_p, H))$ of $H$ is $a = \ell$; thus the difference $d - q - a = \ell - 1$ can be any non-negative integer.

**Remark 3.5.** Let $c', d' \in \mathbb{N}$ be relatively prime. Let $\ell \in \mathbb{N}$. Let $H'$ be a $p$-divisible group over $k$ of height $\ell(c' + d')$ and unique Newton polygon slope $\alpha := \frac{d'}{c' + d'}$. If either $c' = 1$ or $d' = 1$, then the methods of this paper apply entirely to get an analogue of Corollary 3.2 for the slope $\alpha$ (and in particular, that $H'$ is uniquely determined up to isomorphism by $H'[p^{\min(c', d')}]$). Suppose $c', d' \geq 2$ and $\ell = 1$. The classical description of isogenies between such $p$-divisible groups $H'$ shows that the analogue of the invariant $q$ is an invariant $b$ which can be any number in the set $\{0, \ldots, (c' - 1)(d' - 1)\}$ (see [dJO, Subsections 5.8 and 5.32]). Moreover, the analogue of $\left[\frac{q}{2}\right]$ (see Remark 2.6) is then $\left[\frac{b}{c' + d'}\right]$. If $|d' - c'| \geq 3$, the inequality $\left[\frac{2(c' - 1)(d' - 1)}{c' + d'}\right] + 1 > \min\{c', d'\}$ holds and therefore the mentioned description does not suffice to show that $H'$ is uniquely determined up to isomorphism by $H'[p^{\min(c', d')}]$. The same applies if $|d' - c'| \in \{1, 2\}$ and $\ell >> 0$.

4. Proof of Theorem 1.3

4.1. Let $H$ be a supersingular $p$-divisible group over $k$ of height $2d$ which has a principal quasi-polarization $\lambda$. Let $(M, \phi), A, \text{ and } \mathcal{A}$ be as in Subsection 2.1. Let $\psi$ be the perfect alternating form on $\psi$ determined by $\lambda$. Let $\iota$ be the involution of $\text{End}(M)$ induced by $\lambda$. Let $\psi$ be the perfect alternating form on $\psi$ determined by $\lambda$. Let $\iota$ be the involution of $\text{End}(M)$ defined by $\psi$: for $x, y \in M$ and $e \in \text{End}(M)$, we have an identity $\psi(e(x), y) = \psi(x, e(y))$. An element $e \in \text{End}(M)$ annihilates $\psi$ (i.e., for all $x, y \in M$ we have $\psi(e(x), y) + \psi(x, e(y)) = 0$) if and only if $\iota(e) = -e$.

Let $G := \text{Sp}(M, \psi)$; it is a reductive, closed subgroup scheme of $GL_M$ whose Lie algebra $\text{Lie}(G)$ is $\{e \in \text{End}(M) | \iota(e) = -e\}$. Moreover, for an element $g \in GL_M(W(k))$, we have $g \in G(W(k))$ if and only if $\iota(g)g = 1_M$.

For $x, y \in M$, we have $\psi(\phi(x), \phi(y)) = \rho_\sigma(\psi(x, y))$. This implies that $\iota(A) = A$. It also implies that $\phi$ normalizes the Lie subalgebra $\text{Lie}(G)[\frac{1}{p}]$ of $\text{End}(M)[\frac{1}{p}]$. Thus the triple $(M, \phi, G)$ is a latticed $F$-isocrystal with a group over $k$ as defined in [Val, 1.1 (a)]. As $\iota(A) = A$, the involution $\iota$ acts naturally on all points of $A$ with values in $\mathbb{Z}_p$-algebras. Let $\mathcal{I}_q$ be the closed subgroup of $A_{\mathbb{Q}_p}$ with the property that for each $\mathbb{Q}_p$-algebra $R$, we have $\mathcal{I}_q(R) = \{g \in \mathcal{A}(R) | \iota(g)g = 1_{M \otimes_{\mathbb{Q}_p} R}\}$. Let $\mathcal{I}$ be the Zariski closure of $\mathcal{I}_q$ in $A$; it is a flat, closed subgroup scheme of $A$ whose generic fibre is $\mathcal{I}_{q_p}$.

**Lemma 4.1.** Suppose that $p > 2$. Then $\mathcal{I}$ is a smooth group scheme over $\text{Spec}(\mathbb{Z}_p)$.

**Proof:** Let $B(k)$ be the field of fractions of $W(k)$. As $G_{B(k)} = \mathcal{I}_{B(k)}$, the group $\mathcal{I}_{q_p}$ is connected. Let $A^- := \{e \in A | \iota(e) = -e\}$ and $A^+ := \{e \in A | \iota(e) = e\}$. As $p > 2$ and $\iota^2$ is the identity automorphism of $A$, we have a direct sum decomposition $A = A^- \oplus A^+$ of $\mathbb{Z}_p$-modules. The Lie algebra $\text{Lie}(\mathcal{I}_{q_p})$ is included in $A^-/pA^-$ and thus its dimension is at most equal to the dimension of $A^- \otimes_{\mathbb{Z}_p} B(k) = \text{Lie}(G)[\frac{1}{p}]$. Thus
\[ \dim_{F_p}(\text{Lie}(I_{F_p})) \leq \dim(I_{B(k)}) = \dim(I_{0p}). \] As \( \dim(I_{F_p}) = \dim(I_{0p}) \), we get that 
\[ \dim_{F_p}(\text{Lie}(I_{F_p})) \leq \dim(I_{F_p}). \]
This implies that \( \dim_{F_p}(\text{Lie}(I_{F_p})) = \dim(I_{F_p}) \) and that the group \( I_{F_p} \) is smooth. Thus \( I \) is a smooth group scheme over \( \text{Spec}(\mathbb{Z}_p) \). \( \square \)

4.2. **The group scheme** \( I_0 \). Let \( I_1 \) be the smoothing of \( I \) defined and proved to exist in [BLR, Ch. 7, pp. 174–175]. We recall that \( I_1 \) is a smooth group scheme of finite type over \( \text{Spec}(\mathbb{Z}_p) \) equipped with a homomorphism \( I_1 \to I \) which is uniquely determined by the following universal property (see [BLR, Ch. 7, 7.1, Thm. 5]):

(i) if \( Y \) is a smooth scheme over \( \text{Spec}(\mathbb{Z}_p) \), then each morphism \( Y \to I \) factors uniquely through \( I_1 \).

The scheme \( I_1 \) is obtained from \( I \) through a sequence of dilatations centered on special fibres (see the paragraph before [BLR, Ch. 7, 7.1, Thm. 5]) and thus it is an affine scheme over \( I \) (cf. the very definition of dilatations; see the first paragraph of [BLR, Ch. 3, 3.2]). Thus \( I_1 \) is an affine group scheme over \( \text{Spec}(\mathbb{Z}_p) \). If \( p > 2 \), then from (i) and Lemma 4.1 we easily get that the homomorphism \( I_1 \to I \) is an isomorphism; thus \( I_1 = I \). Let \( I_0 \) be the unique open subgroup scheme of \( I_1 \) whose special fibre is the identity component of \( I_{1F_p} \). Thus there exists a homomorphism \( I_0 \to I \) whose generic fibre is an isomorphism and moreover we have:

(ii) the special fibre \( I_{0p} \) of \( I_0 \) is a smooth, connected, affine scheme.

4.3. **Invariants.** Let \( n_\lambda \in \mathbb{N} \) be the smallest number such that \( (H, \lambda) \) is uniquely determined up to isomorphism by \( (H[p^{n_\lambda}], \lambda[p^{n_\lambda}]) \). Its existence is implied by [Va1, Subsection 3.2.5]. Let \( t_\lambda \in \mathbb{N} \) be the \( i \)-number of \((M, \phi, G)\) defined in [Va1, 3.1.4] (i.e., the smallest natural number such that for each element \( g \in G(W(k)) \) congruent mod \( p^{t_\lambda} \) to \( 1_M \), there exists an isomorphism between \((M, g\phi)\) and \((M, \phi)\) which is an element of \( G(W(k)) \)). From an argument entirely analogous to the proof of Theorem 2.2 (a) (cf. [Va1, Subsections 3.2.1 and 3.2.5]), we get that \( n_\lambda = t_\lambda \).

4.4. **Proof of Theorem 1.3.** We will use the notations of Subsection 2.1 to prove that \( t_\lambda \leq m \). Let \( g \in G(W(k)) \) be congruent mod \( p^m \) to \( 1_M \). As \( g \in A(W(k)) \) (see proof of Theorem 2.2 (a)) and \( i(g) = 1_M \), we have \( g \in I(W(k)) \). We show that in fact we have \( g \in I_0(W(k)) \).

We first show that \( g \in I_1(W(k)) \). If \( p > 2 \), this is obvious as \( I_1 = I \). Suppose that \( p = 2 \). Let \( R \) be a \( \mathbb{Z}_2 \)-subalgebra of \( W(k) \) of finite type such that the morphism \( \text{Spec}(W(k)) \to I \) defined by \( g \), factors through \( \text{Spec}(R) \). The monomorphism \( \mathbb{Z}_2 \to W(k) \) is of index of ramification 1 and the generic point of \( \text{Spec}(R) \) belongs to the smooth locus of \( \text{Spec}(R(1/2)) \) over \( \text{Spec}(\mathbb{Q}_2) \). Based on these and [BLR, Ch. 3, 3.6, Prop. 4], we get that there exists an \( R \)-algebra \( R_1 \) which is smooth over \( \mathbb{Z}_2 \) and for which there exists an \( R \)-homomorphism \( R_1 \to W(k) \) (in fact, the proof of loc. cit. shows that one can assume that we have \( R_1[1/2] = R[1/2] \) and thus that \( R_1 \) is an \( R \)-subalgebra of \( W(k) \)). Thus we can view \( g \) as an \( R_1 \)-valued point of \( I_1 \). From this and Subsection 4.2 (i) we get that we can view \( g \) as an \( R_1 \)-valued point of \( I_1 \). Thus \( g \in I_1(W(k)) \) even if \( p = 2 \).

As for each prime \( p \) the number of connected components of \( I_{1F_p} \) is finite (i.e., the group \( I_1(k)/I_0(k) \) is finite), there exists \( s \in \mathbb{N} \) such that the images of the two groups \( \text{Ker}(G(W(k)) \to G(W_m(k))) \) and \( \text{Ker}(G(W_{m+s}(k)) \to G(W_m(k))) \) in \( I_1(k)/I_0(k) \) are equal. But \( \text{Ker}(G(W_{m+s}(k)) \to G(W_m(k))) \) is the group of \( k \)-valued points of a connected group over \( k \) which has a composition series whose factors are isomorphic to the vector group over \( k \) defined by the Lie algebra \( \text{Lie}(G_k) \).
From the last two sentences we get that the image of \(\text{Ker}(G(W(k)) \rightarrow G(W_m(k)))\) in the finite group \(\mathcal{I}_1(k)/\mathcal{I}_0(k)\) is the identity. Thus we have \(g \in \mathcal{I}_0(W(k))\).

As \(\mathcal{I}_0\) is a smooth group scheme over \(\text{Spec}(\mathbb{Z}_p)\) whose special fibre is a connected, affine scheme (cf. Subsection 4.2 (ii)) and as \(g \in \mathcal{I}_0(W(k))\), from Proposition 2.1 we get that there exists an element \(g_0 \in \mathcal{I}_0(W(k))\) such that \(g_0^{-1}\sigma(g_0) = g\). Thus \(g_0\sigma(g_0)^{-1} = 1_M\). As \(\sigma(g_0) = \phi(g_0)\), we have \(g_0\phi(g_0)^{-1} = 1_M\). Thus \(g_0\phi(g_0)^{-1} = \phi\) i.e., \(g_0 \in G(W(k))\) is an isomorphism between \((M, g\phi)\) and \((M, \phi)\). This implies that \(t_\lambda \leq m\).

As \(n_\lambda = t_\lambda \leq m\), from Corollary 3.2 we get \(n_\lambda \leq q + 1 \leq d\). The inequality \(n_\lambda \leq d\) ends the proof of Theorem 1.3. For \(p > 2\), the inequality \(t_\lambda \leq m\) refines the inequality \(t_\lambda \leq m + 1\) which is a particular case of [Va1, Example 3.3.6]. □

Acknowledgments.

The first author has been supported by the Japanese Society for the Promotion of Science (JSPS) while working on this paper at the University of Tōkyō. The second author would like to thank University of Arizona for good conditions with which to write this note. The authors would like to thank the referee for pointing out a minor inaccuracy.

References

[BLR] S. Bosch, W. Lütkebohmert, and M. Raynaud, Néron models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol. 21, Springer-Verlag, 1990.

[Bo] A. Borel, Linear algebraic groups, Grad. Texts in Math., Vol. 126, Springer-Verlag, 1991.

[dJO] J. de Jong and F. Oort, Purity of the stratification by Newton polygons, J. of Amer. Math. Soc. 13 (2000), no. 1, pp. 209–241.

[Ma] Y. I. Manin, The theory of formal commutative groups in finite characteristic, Russian Math. Surv. 18 (1963), no. 6, pp. 1–83.

[Ni] M.-H. Nicole, Superspecial abelian varieties, theta series and the Jacquet-Langlands correspondence, Ph.D. thesis, McGill University, October 2005.

[Oo] F. Oort, Foliations in moduli spaces of abelian varieties, J. of Amer. Math. Soc. 17 (2004), no. 2, pp. 267–296.

[Tr1] C. Traverso, Sulla classificazione dei gruppi analitici di caratteristica positiva, Ann. Scuola Norm. Sup. Pisa 23 (1969), no. 3, pp. 481–507.

[Tr2] C. Traverso, \(p\)-divisible groups over fields, Symposia Mathematica XI (Convegno di Algebra Commutativa, INDAM, Rome, 1971), pp. 45–65, Academic Press, London, 1973.

[Tr3] C. Traverso, Specializations of Barsotti–Tate groups, Symposia Mathematica XXIV (Sympos., INDAM, Rome, 1979), pp. 1–21, Acad. Press, London-New York, 1981.

[Val] A. Vasiu, Crystalline Boundedness Principle, Ann. Sci. École Norm. Sup. 39 (2006), no. 2, pp. 245–300.

[Val2] A. Vasiu, Level \(m\) stratifications of versal deformations of \(p\)-divisible groups, manuscript, June 2006.

Marc-Hubert Nicole, Email: nicole@ms.u-tokyo.ac.jp
Address: University of Tōkyō, Department of Mathematical Sciences, Komaba, 153-8914, Tōkyō, Japan.

Adrian Vasiu, Email: adrian@math.binghamton.edu; fax: 1-607-777-2450.
Address: Department of Mathematical Sciences, Binghamton University, Binghamton, New York, 13902-6000, U.S.A.