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 λ, we show that (H, λ) is also uniquely determined up to isomorphism by its principally quasi-polarized truncated Barsotti–Tate group of level d (i.e., by $(H[p^d], \lambda[p^d])$).

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], [Va, 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. [Tr2, §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 $H[p^d]$.*

2000 *Mathematics Subject Classification.* 11G10, 11G18, 14L05.

Theorem 1.2 strengthens Traverso's and Vasiu's results (see [Tr1, Thm. 3] and [Va, Prop. 4.1.1]) which worked with $H[p^{d2+1}]$ and $H[p^{d2}]$ (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 σ-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.

Theorem 1.3. *Suppose H is a supersingular p-divisible group over k of height $2d$ which has a principal quasi-polarization λ. Then (H,λ) 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 [Va, 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).

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 over k. For $s\in\mathbb{N}$, let $W_s(k):=W(k)/(p^s)$. Let σ be the Frobenius automorphism of $W(k)$ induced from k. Let H be a supersingular p-divisible group over k of height $2d$, for $d\in\mathbb{N}$. Let (M,ϕ) 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 σ-linear endomorphism such that $pM\subseteq\phi(M)$. We denote also by ϕ the σ-linear automorphism of $\mathrm{End}(M[\frac{1}{p}])$ that takes $e\in\mathrm{End}(M[\frac{1}{p}])$ to $\phi(e):=\phi\circ e\circ\phi^{-1}$. Let $A:=\{e\in\mathrm{End}(M)|\phi(e)=e\}$ be the $\mathbb{Z}_p$-algebra of endomorphisms of (M,ϕ). Let $\mathcal{A}$ be the smooth, affine group scheme over $\mathrm{Spec}(\mathbb{Z}_p)$ of invertible elements of the $\mathbb{Z}_p$-algebra A. Let O be the $W(k)$-span of A. As all slopes of (M,ϕ) are $\frac{1}{2}$, all slopes of $(\mathrm{End}(M[\frac{1}{p}]),\phi)$ are 0. This implies that O is a $W(k)$-subalgebra of $\mathrm{End}(M)$ such that the quotient $W(k)$-module $\mathrm{End}(M)/O$ is torsion. Let $\vartheta: M\to M$ be the Verschiebung map of (M,ϕ); we have $\vartheta\phi=\phi\vartheta=p1_M$. Let E be the (unique) supersingular p-divisible group over k of height 2. Let (N,φ) and (N^d,φ) 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 $p^m \mathrm{End}(M) \subseteq O \subseteq \mathrm{End}(M)$. Thus m is the Fontaine–Dieudonné torsion of $(\mathrm{End}(M), \phi)$ defined in [Va, 2.2.2 (b)].

• 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 $\phi^q(M) \subseteq j(N^d)$.

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

Proof: Let $g \in \mathcal{G}(W(k))$. By induction on $s \in \mathbb{N}$, we check that there exists an element $g_s \in \mathcal{G}(W(k))$ such that the following two properties hold: (i) $g_s g \sigma(g_s)^{-1} \in \mathrm{Ker}(\mathcal{G}(W(k)) \to \mathcal{G}(W_s(k)))$, and (ii) for $s \geq 2$, the images of g_s and g_{s-1} in $\mathcal{G}(W_{s-1}(k))$ coincide. As $\mathcal{G}_{\mathbb{F}_p}$ is affine and connected, there exists $\bar{g}_1 \in \mathcal{G}(k)$ 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 $g_1 \in \mathcal{G}(W(k))$ lifts $\bar{g}_1$, then we have $g_1 g \sigma(g_1)^{-1} \in \mathrm{Ker}(\mathcal{G}(W(k)) \to \mathcal{G}(k))$. The passage from s to $s+1$ goes as follows. As $\mathcal{G}$ is smooth, the group $\mathrm{Ker}(\mathcal{G}(W_{s+1}(k)) \to \mathcal{G}(W_s(k)))$ is the group of k-valued points of the vector group $\mathcal{V}$ over $\mathbb{F}_p$ defined by $\mathrm{Lie}(\mathcal{G}_{\mathbb{F}_p})$. From Lang's theorem applied to $\mathcal{V}$, we get that there exists $\bar{g}'_{s+1} \in \mathrm{Ker}(\mathcal{G}(W_{s+1}(k)) \to \mathcal{G}(W_s(k)))$ such that $(\bar{g}'_{s+1})^{-1}\sigma(\bar{g}'_{s+1})$ is the image of $g_s g \sigma(g_s)^{-1}$ in $\mathrm{Ker}(\mathcal{G}(W_{s+1}(k)) \to \mathcal{G}(W_s(k)))$. Let $g'_{s+1} \in \mathcal{G}(W(k))$ be an element that lifts $\bar{g}'_{s+1}$. If $g_{s+1} := g'_{s+1} g_s \in \mathcal{G}(W(k))$, then we have $g_{s+1} g \sigma(g_{s+1})^{-1} \in \mathrm{Ker}(\mathcal{G}(W(k)) \to \mathcal{G}(W_{s+1}(k)))$. Moreover, as $\bar{g}'_{s+1} \in \mathrm{Ker}(\mathcal{G}(W_{s+1}(k)) \to \mathcal{G}(W_s(k)))$, the images of g_{s+1} and g_s in $\mathcal{G}(W_s(k))$ coincide. This ends the induction.

Due to (ii), the p-adic limit of the sequence $(g_s)_{s \in \mathbb{N}}$ is an element g_∞ in $\mathcal{G}(W(k))$. Due to (i), the element $g_\infty g \sigma(g_\infty)^{-1}$ is the identity. Thus $g_\infty^{-1}\sigma(g_\infty) = g$. This implies that $\mathcal{G}(W(k)) = \{g_0^{-1}\sigma(g_0) | g_0 \in \mathcal{G}(W(k))\}$. $\square$

Theorem 2.2. (a) *Let $t \in \mathbb{N}$ be the the smallest number such that for each element $g \in \boldsymbol{GL}_M(W(k))$ congruent modulo p^t to 1_M, there exists an isomorphism between $(M, g\phi)$ and (M, ϕ). Then we have $n = t$.*

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

(c) *We have $n \leq m$.*

Proof: We first prove (a). This is a special case of [Va, Lemma 3.2.2] for the group $G = \boldsymbol{GL}_M$, 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 $g \in \boldsymbol{GL}_M(W(k))$ be congruent to 1_M mod p^n. Let H_g be the p-divisible group over k whose Dieudonné module is $(M, g\phi)$. Then $H_g[p^n] = H[p^n]$ and thus H_g and H are isomorphic i.e., (M, ϕ) and $(M, g\phi)$ 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 $g \in \boldsymbol{GL}_M(W(k))$ be such that the Dieudonné module of H_t is isomorphic to $(M, g\phi)$. As $H_t[p^t]$ and $H[p^t]$ are isomorphic, we can assume that $(M, g\phi, \vartheta g^{-1})$ mod p^t is (M, ϕ, ϑ) mod p^t. This implies that g fixes $\phi(M)/p^t M$ and $M/p^{t-1}\phi(M)$. Since g fixes $pM/p^tM \subseteq \phi(M)/p^tM$, there exists $u \in \mathrm{End}(M)$ such that $g = 1_M + p^{t-1}u$. As g fixes $\phi(M)/p^tM$ and $M/p^{t-1}\phi(M)$, we get that u mod p annihilates $\phi(M)/pM$ and $M/\phi(M)$. Thus $u(\phi(M)) \subseteq pM$ and $u(M) \subseteq \phi(M)$. This implies that $u2 \in p\mathrm{End}(M)$, that $(\phi^{-1}u\phi)(M) \subseteq \phi^{-1}(pM) \subseteq \vartheta(M)$, and that $(\phi^{-1}u\phi)(\vartheta(M)) \subseteq \phi^{-1}(u(pM)) \subseteq pM$. Let $v := \phi^{-1}u\phi$; we have $u = \phi(v)$ and v mod p fixes $\vartheta(M)/pM$ and $M/\vartheta(M)$. As $\vartheta(M)/pM$ is the kernel of ϕ mod p, it is easy to see that we can write $v = pv_1 + v_2$, where $v_1, v_2 \in \mathrm{End}(M)$ and $\phi(v_2) \in p\mathrm{End}(M)$. If $g' \in \mathrm{Ker}(\boldsymbol{GL}_M(W(k)) \to \boldsymbol{GL}_M(W_t(k)))$ and if $(M, g'g\phi)$ is isomorphic to (M, ϕ), then $(M, g\phi)$ is isomorphic to $(M, g''\phi)$ for some $g'' \in \mathrm{Ker}(\boldsymbol{GL}_M(W(k)) \to \boldsymbol{GL}_M(W_t(k)))$; thus $(M, g\phi)$ is also isomorphic to (M, ϕ) (cf. the definition of t). Thus to show that $(M, g\phi)$ and (M, ϕ) (i.e., that H_t and H) are isomorphic, we can replace g by any element of $\boldsymbol{GL}_M(W(k))$ congruent modulo p^t with g. In other words, we can replace u by any element of $u + p\mathrm{End}(M)$. By replacing u with $u - \phi(v_2)$ and v with $v_1 = v - v_2$, we can assume $v = pv_1 \in p\mathrm{End}(M)$. Let $g_1 := (1_M - p^t v_1)^{-1} \in \mathrm{Ker}(\boldsymbol{GL}_M(W(k)) \to \boldsymbol{GL}_M(W_t(k)))$ and $g_2 := g_1 g\phi(g_1^{-1}) = g_1 g\phi(1_M - p^t v_1) = g_1(1_M + p^{t-1}u)(1_M - p^{t-1}u)$. As $u2 \in p\mathrm{End}(M)$ and $t \geq 1$, we have $p^{2t-2}u2 \in p^t\mathrm{End}(M)$. 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, ϕ) are isomorphic. As $g_2\phi = g_1 g\phi g_1^{-1}$, we conclude that $(M, g\phi)$ and (M, ϕ) 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 [Va, proof of Cor. 3.3.4], but we provide here a simpler argument which works for all isoclinic p-divisible groups. The inverse in $\boldsymbol{GL}_M(W(k))$ of the element $g \in O$ is a polynomial in g with coefficients in $W(k)$ and thus it belongs to O. Thus g has an inverse in O and therefore $g \in \mathcal{A}(W(k))$. Any invertible element of O is also an invertible element of $\mathrm{End}(M)$ and therefore we have $\mathcal{A}(W(k)) \leqslant \boldsymbol{GL}_M(W(k))$. The automorphism σ acts naturally on $\mathcal{A}(W(k))$. As $\mathcal{A}$ is an open subscheme of the vector group scheme over $\mathrm{Spec}(\mathbb{Z}_p)$ 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, ϕ). Thus (b) holds.

Based on (a), to prove (c) it suffices to show that for each element $g \in \boldsymbol{GL}_M(W(k))$ congruent modulo p^m to 1_M, $(M, g\phi)$ and (M, ϕ) are isomorphic. As $g - 1_M \in p^m \mathrm{End}(M) \subseteq O$, we have $g \in O$. Thus $(M, g\phi)$ and (M, ϕ) are isomorphic, cf. (b). Thus (c) holds. $\square$

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 $\phi 2(px) = \phi(py) = p^2 x$. The image of the map $\varphi 2 - p1_N : N \to N$ is pN. Let $N^* := \mathrm{Hom}(N, W(k))$. 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 $\mathrm{End}(N) = N \otimes_{W(k)} N^*$. The σ-linear automorphism φ of $\mathrm{End}(N[\frac{1}{p}])$ 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_1 of endomorphisms of (N, φ). We have inclusions $p\mathrm{End}(N) \subseteq O_1 \subsetneqq \mathrm{End}(N)$.

Let O_d be the $W(k)$-span of the $\mathbb{Z}_p$-algebra of endomorphisms of (N^d, ϕ). The inclusion $O_d \subseteq \mathrm{End}(N^d)$ can be identified with the inclusion of matrix $W(k)$-algebras $M_d(O_1) \subseteq M_d(\mathrm{End}(N))$. Thus we have $p\mathrm{End}(N^d) \subseteq O_d \subsetneqq \mathrm{End}(N^d)$. 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. *We have $q \leq d - 1$.*

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 $d \geq 2$. 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 height of M_1 is $2d - 2$, by induction there exists a monomorphism $j_1 : (N^{d-1}, \varphi) \hookrightarrow (M_1, \phi_1)$ such that $\phi_1^{d-2}(M_1) \subseteq j_1(N^{d-1})$. Let M_2 be the inverse image of $\phi_1(j_1(N^{d-1}))$ in M.

We have a short exact sequence

$$0 \to (N, \varphi) \to (M_2, \phi) \to (\phi_1(j_1(N^{d-1})), \phi_1) \to 0 \tag{1}$$

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 $W(k)$-bases $\{x, y\}$ with the properties that: (i) $\phi_1(x) = py$ and $\phi_1 2(x) = p\phi_1(y) = px$, and (ii) $x \in pj_1(N^{d-1}) \subseteq pM_1$ (see Scholium 2.3). Thus to check that (1) splits, it suffices to show that for each such $W(k)$-basis $\{x, y\}$, there exists $x_2 \in M_2$ such that it maps into x and moreover, we have $\frac{1}{p}\phi(x_2) \in M_2$

and $\phi 2(x_2) = px_2$. Let $x_1 \in pM$ be such that it maps into x, cf. (ii). Let $y_1 := \phi 2(x_1) - px_1$; it is an element of pN. Let $y_2 \in N$ be such that $\varphi 2(y_2) - py_2 = -y_1$ (see Scholium 2.3). Let $x_2 := x_1 + y_2$; it is an element of M_2 that maps into x and we have $\phi 2(x_2) - px_2 = y_1 - y_1 = 0$. As $x_1 \in pM$ and $y_2 \in pN$, we have $\frac{1}{p}\phi(x_2) = \frac{1}{p}\phi(x_1) + \frac{1}{p}\varphi(y_2) \in M$. As $\frac{1}{p}\phi(x_2)$ maps into y, we have $\frac{1}{p}\phi(x_2) \in M_2$. Thus the element x_2 exists. As $\phi_1^{d-2}(M_1) \subseteq j_1(N^{d-1})$, we have $\phi_1^{d-1}(M_1) \subseteq \phi_1(j_1(N^{d-1}))$. This implies that $\phi^{d-1}(M) \subseteq M_2$. As the short exact sequence (1) splits, there exists an isomorphism $j_2 : (N^d, \varphi) \xrightarrow{\sim} (M_2, \phi)$. Its composite with the monomorphism $(M_2, \phi) \hookrightarrow (M, \phi)$ is a monomorphism $j : (N^d, \varphi) \xrightarrow{\sim} (M, \phi)$ 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 also follows from either [Ma] (see [Ni, Thm. 1.4.8]) or [LO]. For instance, it is easy to see that [LO, proof of Lemma 1.8] implies that* $q \leq d - a$, *where* $a := \dim_k(Hom(\boldsymbol{\alpha}_p, H)) \in \mathbb{N}$ *is the a-number of* H.

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

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

$$O = \cap_{i=0}^{\infty}\phi^i(\mathrm{End}(M)) = \cap_{i=0}^{\infty}\mathrm{End}(\phi^i(M)) = \cap_{i=0}^{\infty}\mathrm{End}(p^{f(i)}\phi^i(M)).$$

Thus $m \in \mathbb{N}$ is the smallest number such that $M \subseteq \cup_{i\in\mathbb{N}} p^{f(i)}\phi^i(M) \subseteq p^{-m}M$.

3. Proof of Theorem 1.2

Theorem 3.1. *We have* $m \leq q + 1$.

Proof: We prove the Theorem by a step 2 induction on $q \in \mathbb{N}$. If $q = 0$, then H is isomorphic to E^d and thus $m = 1 = q + 1$ (cf. Scholium 2.3).

Let $q = 1$. Let $j : (N^d, \varphi) \hookrightarrow (M, \phi)$ 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 $p^{\frac{-i-2}{2}}\phi^i(M) = \frac{1}{p}X \oplus \frac{1}{p2}Y_{1i} \oplus \frac{1}{p}Y_{2i}$, where $Y_{1i} := p^{-\frac{i}{2}}\phi^i(Y_1)$ and $Y_{2i} := p^{-\frac{i}{2}}\phi^i(Y_2)$. As $Y = Y_{1i} \oplus Y_{2i}$, we have $M \subseteq p^{\frac{-i-2}{2}}\phi^i(M) \subseteq p^{-2}M$. If $i = 2l + 1$ is odd, then $p^{-l-i}\phi^i(M) = \frac{1}{p}X_{1i} \oplus X_{2i} \oplus \frac{1}{p}Y_1 \oplus \frac{1}{p}Y_2$, where $X_{1i} := p^{-l-1}\phi^i(Y_1)$ and $X_{2i} := p^{-l-1}\phi^i(Y_2)$. As $X = X_{1i} \oplus X_{i2}$, we have

$M \subseteq p^{-l-1}\phi^i(M) \subseteq p^{-1}M$. Regardless of what $i \in \mathbb{N}$ is, we have $M \subseteq \cup_{i\in\mathbb{N}} p^{f(i)}\phi^i(M) \subseteq p^{-2}M$ and thus $m \leq 2 = q+1$ (cf. Scholium 2.7).

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

$$p^{q+1}\mathrm{End}(M) \subseteq p^q\mathrm{End}(\tilde{M}) \subseteq p\tilde{O} \subseteq p\mathrm{End}(\tilde{M}) \subseteq \mathrm{End}(M).$$

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

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

Corollary 3.2. *We have $n \leq m \leq q+1 \leq d$.*

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 $\phi(e_i) = pe_{i+1}$ (here $e_{2d+1} := e_1$). We denote the corresponding p-divisible group by C_d. Let (M, ϕ_1) be the Dieudonné module with the property that $\phi_1(e_i) = \phi(e_i)$ if $i \neq d+1$ and $\phi_1(e_{d+1}) = \phi_1^{d+1}(e_1) = pe_{d+2} + p^{d-1}e_2$. Let H_1 be the p-divisible group over k whose Dieudonné module is (M, ϕ_1). We have $\phi_1^{2d}(e_1) = p^d e_1 + p^{d-1}e_{d+1} \in p^{d-1}M \setminus p^d M$. But $\phi^{2d}(M) = p^d M$. From the last two sentences, we get that (M, ϕ_1) is not isomorphic to (M, ϕ) (i.e., H_1 is not isomorphic to C_d). It is easy to see that ϕ_1 and $\vartheta_1 := p\phi_1^{-1}$ are congruent modulo p^{d-1} to ϕ and ϑ (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 $n = m = q+1 = d$.

Let θ be an invertible element of $W(k)$ such that we have $\sigma^d(\theta) = -\theta$. 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 $\psi(e_i, e_{i+d}) = -\psi(e_{i+d}, e_i) = \sigma^{i-1}(\theta)$. It is easy to see that ψ is a principal quasi-polarization of both (M, ϕ) and (M, ϕ_1). Thus, if λ is the principal quasi-polarization of C_d defined by ψ, then (C_d, λ) 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 is $a = \ell$; thus $d - q - a = \ell - 1$ 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 α (and in particular, that H' is uniquely determined up to isomorphism by $H'[p^{\ell \min\{c',d'\}}]$). 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 $\lceil \frac{q}{2} \rceil$ (see Remark 2.6) is then $\lceil \frac{b}{c'+d'} \rceil$. As $\lceil \frac{2(c'-1)(d'-1)}{c'+d'} \rceil + 1 > \min\{c', d'\}$, the mentioned description does not suffice to show that H' is uniq! uely determined up to isomorphism by $H'[p^{\min\{c',d'\}}]$.*

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 λ. Let (M, ϕ), A, and $\mathcal{A}$ be as in Section 2. Let ψ be the perfect alternating form on M induced by λ. Let ι be the involution of $\mathrm{End}(M)$ defined by ψ: for $x, y \in M$ and $e \in \mathrm{End}(M)$, we have an identity $\psi(e(x), y) = \psi(x, \iota(e)(y))$. An element $e \in \mathrm{End}(M)$ annihilates ψ (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 $G := \boldsymbol{Sp}(M, \psi)$; it is a reductive closed subgroup scheme of $\boldsymbol{GL}_M$ whose Lie algebra $\mathrm{Lie}(G)$ is $\{e \in \mathrm{End}(M) | \iota(e) = -e\}$. Moreover, for $g \in \boldsymbol{GL}_M(W(k))$, we have $g \in G(W(k))$ if and only if $\iota(g)g = 1_M$.

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

Lemma 4.1. *Suppose that $p > 2$. Then $\mathcal{I}$ is a smooth group scheme over 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 $\mathcal{I}_{\mathbb{Q}_p}$ 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 $\mathrm{Lie}(\mathcal{I}_{\mathbb{F}_p})$ is included in A^-/pA^- and thus its dimension is at most equal to the dimension of $A^- \otimes_{\mathbb{Z}_p} B(k) = \mathrm{Lie}(G)[\frac{1}{p}]$. Thus $\dim_{\mathbb{F}_p}(\mathrm{Lie}(\mathcal{I}_{\mathbb{F}_p})) \leq \dim(\mathcal{I}_{B(k)}) = \dim(\mathcal{I}_{\mathbb{Q}_p})$. As $\dim(\mathcal{I}_{\mathbb{F}_p}) = \dim(\mathcal{I}_{\mathbb{Q}_p})$, we get that $\dim_{\mathbb{F}_p}(\mathrm{Lie}(\mathcal{I}_{\mathbb{F}_p})) \leq \dim(\mathcal{I}_{\mathbb{F}_p})$. This implies that the group $\mathcal{I}_{\mathbb{F}_p}$ is smooth. Thus $\mathcal{I}$ is a smooth group scheme over $\mathrm{Spec}(\mathbb{Z}_p)$. □

4.2. The group scheme $\mathcal{I}_0$. Let $\mathcal{I}_1$ be the smoothening of $\mathcal{I}$ defined and proved to exist in [BLR, Ch. 7, pp. 174–175]. We recall that $\mathcal{I}_1$ is a smooth group scheme of finite type over $\mathrm{Spec}(\mathbb{Z}_p)$ equipped with a homomorphism $\mathcal{I}_1 \to \mathcal{I}$ which is uniquely determined by the following universal property (see [BLR, Ch. 7, Thm. 5]):

(i) if Y is a smooth scheme over $\mathrm{Spec}(\mathbb{Z}_p)$, then each morphism $Y \to \mathcal{I}$ factors uniquely through $\mathcal{I}_1$.

The scheme $\mathcal{I}_1$ is obtained from $\mathcal{I}$ through a sequence of dilatations centered on special fibres (see the paragraph before [BLR, Ch. 7, Thm. 5]) and thus it is an affine scheme over $\mathcal{I}$ (cf. the very definition of dilatations; see the first paragraph of [BLR, Ch. 3, 3.2]). Thus $\mathcal{I}_1$ is an affine group scheme over $\mathrm{Spec}(\mathbb{Z}_p)$. If $p > 2$, then from (i) and Lemma 4.1 we easily get that the homomorphism $\mathcal{I}_1 \to \mathcal{I}$ is an isomorphism; thus $\mathcal{I}_1 = \mathcal{I}$. Let $\mathcal{I}_0$ be the unique open subgroup scheme of $\mathcal{I}_1$ whose special fibre is the identity component of $\mathcal{I}_{1\mathbb{F}_p}$. Thus there exists a homomorphism $\mathcal{I}_0 \to \mathcal{I}$ whose generic fibre is an isomorphism and moreover we have:

(ii) the special fibre $\mathcal{I}_{0\mathbb{F}_p}$ is a smooth, connected, affine scheme.

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

4.4. Proof of Theorem 1.3. We will prove that $t_\lambda \leq m$. Let $g \in G(W(k))$ be congruent modulo p^m to 1_M. As $g \in \mathcal{A}(W(k))$ (see proof of Theorem 2.2 (a)) and $\iota(g)g = 1_M$, we have $g \in \mathcal{I}(W(k))$. We show that in fact we have $g \in \mathcal{I}_0(W(k))$.

We first show that $g \in \mathcal{I}_1(W(k))$. If $p > 2$, this is obvious as $\mathcal{I}_1 = \mathcal{I}$. Suppose that $p = 2$. Let R be a $\mathbb{Z}_2$-subalgebra of $W(k)$ of finite type such that the morphism $\mathrm{Spec}(W(k)) \to \mathcal{I}$ defined by g, factors through $\mathrm{Spec}(R)$. The monomorphism $\mathbb{Z}_2 \hookrightarrow W(k)$ is of index of ramification 1 and the generic point of $\mathrm{Spec}(R)$ belongs to the smooth locus of $\mathrm{Spec}(R[\frac{1}{2}])$ over $\mathrm{Spec}(\mathbb{Q}_2)$. 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 we have $R_1[\frac{1}{2}] = R[\frac{1}{2}]$ and thus we can assume that R_1 is an R-subalgebra of $W(k)$). Thus we can view g as an R_1-valued point of $\mathcal{I}$. From this and Subsection 4.2 (i) we get that we can view g as an R_1-valued point of $\mathcal{I}_1$. Thus $g \in \mathcal{I}_1(W(k))$ even if $p = 2$.

As for any prime p the number of connected components of $\mathcal{I}_{1\mathbb{F}_p}$ is finite (i.e., the group $\mathcal{I}_1(k)/\mathcal{I}_0(k)$ is finite), there exists $s \in \mathbb{N}$ such that the images of the two groups $\mathrm{Ker}(G(W(k)) \to G(W_m(k)))$ and $\mathrm{Ker}(G(W_{m+s}(k)) \to G(W_m(k)))$ in $\mathcal{I}_1(k)/\mathcal{I}_0(k)$ are equal. But $\mathrm{Ker}(G(W_{m+s}(k)) \to G(W_m(k)))$ 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 $\mathrm{Lie}(G_k)$. From the last two sentences we get that the image of $\mathrm{Ker}(G(W(k)) \to G(W_m(k)))$ 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 $\mathrm{Spec}(\mathbb{Z}_p)$ whose special fibre is a connected, affine scheme (cf. Subsection 4.2 (ii)), from Proposition 2.1 we get that there exists $g_0 \in \mathcal{I}_0(W(k)) \leqslant G(W(k))$ such that $g_0^{-1}\sigma(g_0) = g$. Thus $g_0 g \sigma(g_0)^{-1} = 1_M$. As $\sigma(g_0) = \phi(g_0)$, we have $g_0 g \phi(g_0)^{-1} = 1_M$. Thus $g_0 g \phi g_0^{-1} = \phi$ i.e., $g_0 \in G(W(k))$ is an isomorphism between $(M, g\phi)$ and (M, ϕ). 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 [Va, Example 3.3.6]. $\square$

Acknowledgments.

The first author has been supported by the Japanese Society for the Promotion of Science (JSPS PDF) while working on this paper at the University of Tokyo. The second author would like to thank University of Arizona for good conditions in which to write this note.

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.

[LO] K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Math., Vol. **1680**, Springer-Verlag, 1998.

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

[Va] A. Vasiu, *Crystalline Boundedness Principle,* accepted (in final form) for publication in Ann. Sci. École Norm. Sup. (see math.NT/0205199).

Marc-Hubert Nicole
E-mail: `nicole@ms.u-tokyo.ac.jp`
University of Tokyo, Department of Mathematical Sciences,
Komaba, 153-8914, Tokyo, Japan.

Adrian Vasiu
E-mail: `adrian@math.arizona.edu`
University of Arizona, Department of Mathematics,
617 North Santa Rita, P.O. Box 210089, Tucson, AZ-85721, U.S.A.