On the Manin-Mumford and Mordell-Lang conjectures in positive characteristic

Damian RÖSSLER*

October 26, 2012

Abstract

We prove that in positive characteristic, the Manin-Mumford conjecture implies the Mordell-Lang conjecture, in the situation where the ambient variety is an abelian variety defined over the function field of a smooth curve over a finite field and the relevant group is a finitely generated group. In particular, in the setting of the last sentence, we provide a proof of the Mordell-Lang conjecture, which does not depend on tools coming from model theory.

1 Introduction

Let B be a semiabelian variety over an algebraically closed field F of characteristic $p > 0$. Let Y be an irreducible reduced closed subscheme of B. Let $\Lambda \subseteq B(F)$ be a subgroup. Suppose that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is a finitely generated $\mathbb{Z}_{(p)}$-module (here, as is customary, we write $\mathbb{Z}_{(p)}$ for the localization of $\mathbb{Z}$ at the prime p).

Let $C := \mathrm{Stab}(Y)^{\mathrm{red}}$, where $\mathrm{Stab}(Y) = \mathrm{Stab}_B(Y)$ is the translation stabilizer of Y. This is the closed subgroup scheme of B, which is characterized uniquely by the fact that for any scheme S and any morphism $b : S \to B$, translation by b on the product $B \times_F S$ maps the subscheme $Y \times S$ to itself if and only if b factors through $\mathrm{Stab}_B(Y)$. Its existence is proven in [10, exp. VIII, Ex. 6.5 (e)].

*Institut de Mathématiques, Equipe Emile Picard, Université Paul Sabatier, 118 Route de Narbonne, 31062 Toulouse cedex 9, FRANCE, E-mail: rossler@math.univ-toulouse.fr

The Mordell-Lang conjecture for Y and B is now the following statement.

Theorem 1.1 (Mordell-Lang conjecture; Hrushovski [11]). *If $Y \cap \Lambda$ is Zariski dense in Y then there is*

- *a semiabelian variety B' over F;*
- *a homomorphism with finite kernel $h : B' \to B/C$;*
- *a model $\mathbf{B}'$ of B' over a finite subfield $\mathbb{F}_{p^r} \subset F$;*
- *an irreducible reduced closed subscheme $\mathbf{Y}' \hookrightarrow \mathbf{B}'$;*
- *a point $b \in (B/C)(F)$, such that $Y/C = b + h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$.*

Here $h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$ refers to the scheme-theoretic image of $\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F$ by h. Since h is finite and $\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F$ is reduced, this implies that $h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$ is simply the set-theoretic image of $\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F$ by h, endowed with its reduced-induced scheme structure.

Theorem 1.1 in particular implies the following result, which will perhaps seem more striking on first reading. Suppose that there are no non-trivial homomorphisms from B to a semiabelian variety, which has a model over a finite field. Then : if $Y \cap \Lambda$ is Zariski dense in Y then Y is the translate of an abelian subvariety of B.

Theorem 1.1 was first proven in 1996 by E. Hrushovski using deep results from model theory, in particular the Hrushovski-Zilber theory of Zariski geometries (see [12]). An algebraic proof of Theorem 1.1 in the situation where B is an ordinary abelian variety was given by D. Abramovich and J.-.F Voloch in [1]. In the situation where Y is a smooth curve embedded into B as its Jacobian, the theorem was known to be true much earlier. See for instance [20] and [23]. The earlier proofs for curves relied on the use of heights, which do not appear in the later approach of Voloch and Hrushovski, which is parallel and inspired by A. Buium's approach in characteristic 0 via differential equations (see below).

The *Manin-Mumford conjecture* has exactly the same form as the Mordell-Lang conjecture, but Λ is replaced by the group $\mathrm{Tor}(B(F))$ of points of finite order of $B(F)$. For the record, we state it in full:

Theorem 1.2 (Manin-Mumford conjecture; Pink-Rössler [17]). *If $Y \cap \mathrm{Tor}(B(F))$ is Zariski dense in Y then there is*

- *a semiabelian variety B' over F;*

- *a homomorphism with finite kernel* $h : B' \to B/C$*;*
- *a model* $\mathbf{B}'$ *of* B' *over a finite subfield* $\mathbb{F}_{p^r} \subset F$*;*
- *an irreducible reduced closed subscheme* $\mathbf{Y}' \hookrightarrow \mathbf{B}'$*;*
- *a point* $b \in (B/C)(F)$*, such that* $Y/C = b + h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$.

See also [21] for a model-theoretic proof of the Manin-Mumford conjecture.

Remark (important). Notice that the Manin-Mumford conjecture is not a special case of the Mordell-Lang conjecture, because $\mathrm{Tor}(A(F))$ is not in general a finitely generated $\mathbb{Z}_{(p)}$-module (because $\mathrm{Tor}(A(F))[p^\infty]$ is not finite in general). Nevertheless, it seems reasonable to conjecture that Theorem 1.1 should still be true when the the hypothesis that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is finitely generated is replaced by the weaker hypothesis that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ is finitely generated. This last statement, which is still not proven in general, is often called the *full Mordell-Lang conjecture* and it would have Theorems 1.1 and 1.2 as special cases. See [6] for more about this.

Now suppose that the group Λ is actually finitely generated and that B arises by base-change to F from an abelian variety B_0, which is defined over a function field of transcendence degree 1 over a finite field. The main result of this text is then the proof of the fact that the Manin-Mumford conjecture in general implies the Mordell-Lang conjecture in this situation. We follow here the lead of A. Pillay, who suggested in a talk he gave in Paris on Dec. 17th 2010 that it should be possible to establish this logical link without proving the Mordell-Lang conjecture first. See Theorem 1.3 and its corollary below for a precise statement.

The interest of an algebraic-geometric (in contrast with model-theoretic) proof of the implication Manin-Mumford $\Longrightarrow$ Mordell-Lang is that it provides in particular an algebraic-geometric proof of the Mordell-Lang conjecture.

Let K_0 be the function field of a smooth curve over $\bar{\mathbb{F}}_p$. Let A be an abelian variety over K_0 and let $X \hookrightarrow A$ be a closed integral subscheme. We shall write $+$ for the group law on A.

Let $\Gamma \subseteq A(K_0)$ be a finitely generated subgroup.

Theorem 1.3. *Suppose that for any field extension* $L_0|K_0$ *and any* $Q \in A(L_0)$*, the set* $X_{L_0}^{+Q} \cap \mathrm{Tor}(A(L_0))$ *is not Zariski dense in* $X_{L_0}^{+Q}$*. Then* $X \cap \Gamma$ *is not Zariski dense in* X*.*

Here $X_{L_0}^{+Q}$ stands for the scheme-theoretic image of X_{L_0} under the morphism $+Q : A_{L_0} \to A_{L_0}$.

Corollary 1.4. *Suppose that $X \cap \Gamma$ is Zariski dense in X. Then the conclusion of the Mordell-Lang conjecture 1.1 holds for $F = \bar{K}_0$, $B = A_{\bar{K}_0}$ and $Y = X_{\bar{K}_0}$.*

In an upcoming article, which builds on the present one, C. Corpet (see [5]) shows that Theorem 1.3 (and thus its corollary) can be generalized; more specifically, he shows that the hypothesis that K_0 is of transcendence degree 1 can be dropped, that the hypothesis that Γ is finitely generated can be weakened to the hypothesis that $\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is a finitely generated $\mathbb{Z}_{(p)}$-module and finally that is can be assumed that A is only semiabelian. In particular, he gives a new proof of Theorem 1.1.

In the present article, we deliberately focus on the situation of an abelian variety and a finitely generated group (which is probably the most important situation) in order to avoid some technical issues, which we feel would obscure the structure of the proof.

The structure of the article is the following. The second section contains some general results on the geometry of relative jet schemes (or spaces), which are probably known to many specialists but for which there doesn't seem to be a coherent set of references in the literature. The jet spaces considered in [16] do not seem to suffice for our purposes, because they are defined in an absolute situation and the jet spaces considered in [4] are only defined in characteristic 0 (although this is probably not an essential restriction); furthermore, the latter are defined in Buium's language of differential schemes, whereas our definition has the philological advantage of being based on the older notion of Weil restriction. The subsection 2.1 contains the definition of jet schemes and a description of the various torsor structures on the latter. The subsection 2.2 contains a short discussion on the structure of the jet schemes of smooth commutative group schemes and various natural maps that are associated with them. In the third section, we use jet schemes to construct some natural schemes in the geometrical context of the Mordell-Lang conjecture. These "critical schemes" are devised to "catch rational points"; we then proceed to show that these schemes must be of small dimension. This is deduced from a general result on the sparsity of points over finite fields, which are liftable to highly p-divisible unramified points. This last result is proved in the fourth section. Once we know that the critical schemes are small, it is but a small step to the proof of Theorem 1.3 and Corollary 1.4. The terminology of the introduction is used in the first three sections but the fourth section has its own terminology and is also technically independent of the rest of the text. A reader who would only be interested in its main result (i.e. Theorem 4.1) can skip to the fourth section directly.

The use that we make of jet schemes in this note is in many ways similar to the use that A. Buium makes of them in his article on the geometric Mordell-Lang conjecture in characteristic 0 (cf. [4]). In the article [3], where some of Buium's techniques are adapted to the context of positive characteristic, the authors give a proof of the Mordell conjecture for curves over function fields in positive characteristic, which has exactly the same structure as ours, if one leaves out the proof of the result on the the sparsity of liftable points mentioned above.

For more detailed explanations on this connection, see Remarks 4.8 and 4.9 at the end of the text.

Acknowledgments. As many people, I am very much indebted to O. Gabber, who pointed out a flaw in an earlier version of this article and who also suggested a way around it. Many thanks to R. Pink for many interesting exchanges on the matter of this article. I also want to thank M. Raynaud for his reaction to an earlier version of the text and A. Pillay for interesting discussions and for suggesting that the method used in this article should work. Finally, I would also like to thank E. Bouscaren and F. Benoist for their interest and A. Buium for his very interesting observations.

2 Preliminaries.

We first recall the definition and existence theorem for the Weil restriction functor. Let T be a scheme and let $T' \to T$ be a morphism. Let Z be a scheme over T'. The Weil restriction $\mathfrak{R}_{T'/T}(Z)$ (if it exists) is a T-scheme, which represents the functor $W/T \mapsto \mathrm{Hom}_{T'}(W \times_T T', Z)$. It is shown in [2, Par. 7.6] that $\mathfrak{R}_{T'/T}(Z)$ exists if T' is finite, flat and locally of finite presentation over T. The Weil restriction is naturally functorial in Z and sends closed immersions to closed immersions. The same permanence property is satisfied for smooth and étale morphisms. Finally notice that the definition of the Weil restriction implies that there is a natural isomorphism $\mathfrak{R}_{T'/T}(Z)_{T_1} \simeq \mathfrak{R}_{T'_{T_1}/T_1}(Z_{T'_{T_1}})$ for any scheme T_1 over T (in words: Weil restriction is invariant under base-change on T). See [2, Par. 7.6] for all this.

2.1 Jet schemes

Let k_0 be field. Let U be a smooth scheme over k_0. Let $\Delta : U \to U \times_{k_0} U$ be the diagonal immersion. Let $I_\Delta \subseteq \mathcal{O}_{U\times_{k_0}U}$ be the ideal sheaf of $\Delta_* U$. For all $n \in \mathbb{N}$, we let $U_n := \mathcal{O}_{U\times_{k_0}U}/I_\Delta^{n+1}$ be the n-th infinitesimal neighborhood of the diagonal in $U \times_{k_0} U$.

Write $\pi_1, \pi_2 : U \times_{k_0} U \to U$ for the first and second projection morphism, respectively. Write $\pi_1^{U_n}, \pi_2^{U_n} : U_n \to U$ for the induced morphisms. We view U_n as a U-scheme via the *first* projection $\pi_1^{U_n}$.

We write $i_{m,n} : U_m \hookrightarrow U_n$ for the natural inclusion morphism.

Lemma 2.1. *The U-scheme U_n is flat and finite.*

Proof. As a U-scheme, U_n is finite because it is quasi-finite and proper over U, since $U_n^{\mathrm{red}} = \Delta_*(U)$. So we only have to prove that it is flat over U. For this purpose, we may view U_n as a coherent sheaf of $\mathcal{O}_U$-algebras (via the second projection).

Let $I := I_\Delta$. For any $n \geqslant 0$, there are exact sequences of $\mathcal{O}_{U_{n+1}}$-modules (and hence $\mathcal{O}_U$-modules)

$$0 \to I^{n+1}/I^{n+2} \to \mathcal{O}_{U_{n+1}} \to \mathcal{O}_{U_n} \to 0$$

Furthermore I^{n+1}/I^{n+2} is naturally a $\mathcal{O}_{U_0}$-module and is isomorphic to $\mathrm{Sym}^{n+1}_{\mathcal{O}_{U_1}}(I/I^2)$ as a $\mathcal{O}_{U_0}$-module, because I is locally generated by a regular sequence in $U \times_{k_0} U$ (U being smooth over k_0). See [15, chap. 6, 16.] for this. Hence I^{n+1}/I^{n+2} is locally free as a $\mathcal{O}_U$-module. Since $U_0 = \Delta_*(U)$ is locally free as a $\mathcal{O}_U$-module, we may apply induction on n to prove that $\mathcal{O}_{U_n}$ is locally free, which is the claim. $\square$

Let W/U be a scheme over U.

Definition 2.2. *The n-th jet scheme $J^n(W/U)$ of W over U is the U-scheme $\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*}W)$.*

By $\pi_2^{U_n,*}W$ we mean the base-change of W to U_n via the morphism $\pi_2^{U_n} : U_n \to U$ described above.

If W_1 is another scheme over U and $W \to W_1$ is a morphism of U-schemes, then the induced morphism $\pi_2^{U_n,*}W \to \pi_2^{U_n,*}W_1$ over U_n leads to a morphism of jet schemes $J^n(W/U) \to J^n(W_1/U)$ over U, so that the construction of jet schemes is covariantly functorial in W.

Notice that the permanence properties of Weil restrictions show that if the morphism $W \to W_1$ is a closed immersion, then so is the morphism $J^n(W/U) \to J^n(W_1/U)$. Same for smooth and étale morphisms.

To understand the nature of jet schemes better, let $u \in U$ be a closed point. Suppose until the end of the sentence following the string of equations (1) that k_0 is algebraically closed. View u as closed reduced subscheme of U. Let u_n be the n-th infinitesimal neighborhood of u in U. From the definitions, we infer that there are canonical bijections

$$\begin{aligned} J^n(W/U)(u) &= J^n(W/U)_u(k_0) = \mathrm{Hom}_{U_n}(u \times_U U_n, \pi_2^{U_n,*}W) \\ &= \mathrm{Hom}_{U_n}(u_n, W_{u_n}) = \mathrm{Hom}_{u_n}(u_n, W_{u_n}) = W(u_n) \end{aligned} \quad (1)$$

In words, (1) says the set of geometric points of the fibre of $J^n(W/U)$ over u corresponds to the set of sections of W over the n-th infinitesimal neighborhood of u; the scheme $J^n(W/U)_u$ is often called the scheme of arcs of order n at u in the literature (see [16, Ex. 2.5]).

The family of U-morphisms $i_{m,n} : U_m \to U_n$ induce U-morphisms $\Lambda^W_{n,m} : J^n(W/U) \to J^m(W/U)$ for any $m \leqslant n$. These morphisms will be studied in detail in the proof of the next lemma.

Lemma 2.3. *Suppose that W is a smooth U-scheme. For all $n \geqslant 1$, the morphism*

$$\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*}W) \to \mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*}W)$$

makes $\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*}W)$ into a $\mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*}W)$-torsor under the vector bundle $\Lambda^{W,*}_{n,0}(\Omega^\vee_{W/U}) \otimes \mathrm{Sym}^n(\Omega_{U/k_0})$.

Proof. Let $T \to U$ be an affine U-scheme. By definition

$$\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*}W)(T) \simeq \mathrm{Hom}_{U_n}(T \times_U U_n, \pi_2^{U_n,*}W)$$

and

$$\mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*}W)(T) \simeq \mathrm{Hom}_{U_{n-1}}(T \times_U U_{n-1}, \pi_2^{U_{n-1},*}W).$$

Now the immersion $U_{n-1} \hookrightarrow U_n$ gives rise to a natural restriction map

$$\mathrm{Hom}_{U_n}(T \times_U U_n, \pi_2^{U_n,*}W) \to \mathrm{Hom}_{U_{n-1}}(T \times_U U_{n-1}, \pi_2^{U_{n-1},*}W). \quad (2)$$

This is the functorial description of the morphism $\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*}W) \to \mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*}W)$.

Now notice that the ideal of U_{n-1} in U_n is a square 0 ideal.

Let $f \in \mathrm{Hom}_{U_{n-1}}(T \times_U U_{n-1}, \pi_2^{U_{n-1},*}W)$. View f as a U_n-morphism $T \times_U U_{n-1} \to \pi_2^{U_n,*}W$ via the canonical closed immersions $\pi_2^{U_{n-1},*}W \hookrightarrow \pi_2^{U_n,*}W$ and $U_{n-1} \hookrightarrow U_n$. The fibre over

f of the map (2) then consists of the extensions of f to U_n-morphisms $T\times_U U_n\to\pi_2^{U_n,*}W$. The theory of infinitesimal extensions of morphisms to smooth schemes (see [8, Exp. III, Prop. 5.1]) implies that this fibre is an affine space under the group

$$H^0(T\times_U U_{n-1}, f^*\Omega^\vee_{\pi_2^{U_n,*}W/U_n}\otimes N)$$

where N is the conormal bundle of the closed immersion $T\times_U U_{n-1}\hookrightarrow T\times_U U_n$. Since U_n and U_{n-1} are flat over U, the coherent sheaf N is the pull-back to $T\times_U U_{n-1}$ of the conormal bundle of the immersion $U_{n-1}\hookrightarrow U_n$. Now since the diagonal is regularly immersed in $U\times_{k_0}U$ (because U is smooth over k_0), the conormal bundle of the immersion $U_{n-1}\hookrightarrow U_n$ is $\mathrm{Sym}^n(\Omega_{U/k_0})$ (viewed as a sheaf in $\mathcal{O}_{U_{n-1}}$-modules via the closed immersion $U_0\to U_{n-1}$). See [15, chap. 6, 16.] for this. Hence

$$\begin{aligned}&H^0(T\times_U U_{n-1}, f^*\Omega^\vee_{\pi_2^{U_n,*}W/U_n}\otimes N)\\ \simeq\ &H^0(T\times_U U_{n-1}, f^*\Omega^\vee_{\pi_2^{U_n,*}W/U_n}\otimes\mathrm{Sym}^n(\Omega_{U/k_0}))\simeq H^0(T, f_0^*\Omega^\vee_{W/U}\otimes\mathrm{Sym}^n(\Omega_{U/k_0}))\end{aligned}$$

where f_0 is the U-morphism $T\to W$ arising from f by base-change to U. This proves the lemma. □

2.2 The jet schemes of smooth commutative group schemes

We keep the terminology of the last subsection. Let $\mathcal{C}/U$ be a commutative group scheme over U, with zero-section $\epsilon: U\to\mathcal{C}$. If $n\in\mathbb{N}$, we shall write $[n]_\mathcal{C}:\mathcal{C}\to\mathcal{C}$ for the multiplication-by-n morphism. The schemes $J^n(\mathcal{C}/U)$ are then naturally group schemes over U. Furthermore, for each $n\geqslant m\geqslant 0$, the morphism $\Lambda^\mathcal{C}_{n,m}: J^n(\mathcal{C}/U)\to J^m(\mathcal{C}/U)$ is a morphism of group schemes. If $m=n-1$, the kernel of $\Lambda^\mathcal{C}_{n,m}$ is the vector bundle $\epsilon^*(\Omega^\vee_{\mathcal{C}/U})\otimes\mathrm{Sym}^n(\Omega_{U/k_0})$. The torsor structure is realized by the natural action of $\epsilon^*(\Omega^\vee_{\mathcal{C}/U})\otimes\mathrm{Sym}^n(\Omega_{U/k_0})$ on $J^n(\mathcal{C}/U)$. The details of the verification of these facts are left to the reader.

Lemma 2.4. *Let $n\geqslant 1$. Suppose that $\mathrm{char}(k_0)=p$. There is an U-morphism $[p^n]^\circ:\mathcal{C}\to J^n(\mathcal{C}/U)$ such that $\Lambda^\mathcal{C}_{n,0}\circ[p^n]^\circ=[p^n]_\mathcal{C}$ and $[p^n]_{J^n(\mathcal{C}/U)}=[p^n]^\circ\circ\Lambda^\mathcal{C}_{n,0}$.*

Proof. Let $T\to U$ be an affine U-scheme. Define a map

$$\phi_{T,n}:\mathrm{Hom}_U(T,\mathcal{C})\to\mathrm{Hom}_{U_n}(T\times_U U_n,\pi_2^*\mathcal{C})$$

by the following recipe. Let $f \in \mathrm{Hom}_U(T, \mathcal{C})$ and take any extension $\widetilde{f}$ of f to a morphism $T \times_U U_n \to (\pi_2^*\mathcal{C})_{U_n}$; then define $\phi_{T,n}(f) = p^n \cdot \widetilde{f}$. To see that this does not depend on the choice of the extension $\widetilde{f}$, notice that the kernel K_n of the restriction map

$$\mathrm{Hom}_{U_n}(T \times_U U_n, \pi_2^*\mathcal{C}) \to \mathrm{Hom}_U(T, \mathcal{C})$$

is obtained by successive extensions by the groups $H^0(T, f^*\Omega^\vee_{\mathcal{C}/U} \otimes \mathrm{Sym}^i(\Omega_{U/k_0})$ for $i = 1, \ldots, n$ (see [8, Chap. III, 5., Cor. 5.3] for all this). Hence K_n is annihilated by multiplication by p^n because T is a scheme of characteristic p.

The definition of $\phi_{T,n}$ is functorial in T and thus by patching the morphisms $\phi_{T,n}$ as T runs over the elements of an affine cover of $\mathcal{C}$ we obtain the required morphism $[p^n]^\circ$. □

Now notice that for any scheme W over U, there is a canonical map $\lambda_n^W : W(U) \to J^n(W/U)(U)$, which sends the U-morphism $f : U \to W$ to $J^n(f) : J^n(U/U) = U \to J^n(W/U)$.

Lemma 2.5. *The maps λ_n^W have the following properties :*

(a) *for $n \geqslant m \geqslant 0$ the identity $\Lambda_{n,m}^W \circ \lambda_n^W = \lambda_m^W$;*

(b) *if W/U is commutative group scheme over U, then λ_n^W is a homomorphism; furthermore on $W(U)$ we then have the identity $[p^n]_{J^n(W/U)} \circ \lambda_n^W = [p^n]^\circ$;*

(c) *if $f : W \to W_1$ is a U-scheme morphism then $J^n(f) \circ \lambda_n^W = \lambda_n^{W_1} \circ f$.*

Proof. (of Lemma 2.5). Exercise for the reader. □

Remark 2.6. An interesting feature of the map λ_n^W is that it does not arise from a morphism of schemes $W \to J^n(W/U)$.

3 Proof of Theorem 1.3 & Corollary 1.4

We now turn to the proof of our main result. We shall use the terminology of the preliminaries. Let $k_0 := \bar{\mathbb{F}}_p$ and suppose now that U is a smooth curve over k_0, whose function field is K_0. We take U sufficiently small so that X extends to a flat scheme $\mathcal{X}$ over U and so that A extends to an abelian scheme $\mathcal{A}$ over U. We also suppose that the closed immersion $X \hookrightarrow A$ extends to a closed immersion $\mathcal{X} \to \mathcal{A}$.

Recall that the following hypothesis is supposed to hold : for any field extension $L_0|K_0$ and any $Q \in A(L_0)$, the set $X_{L_0}^{+Q} \cap \mathrm{Tor}(A(L_0))$ is not Zariski dense in $X_{L_0}^{+Q}$.

3.1 The critical schemes

For all $n \geqslant 0$, we define

$$\mathrm{Crit}^n(\mathcal{X}, \mathcal{A}) := [p^n]_*(J^n(\mathcal{A}/U)) \cap J^n(\mathcal{X}/U).$$

Here $[p^n]_*(J^n(\mathcal{A}/U))$ is the scheme-theoretic image of $J^n(\mathcal{A}/U)$ by $[p^n]_{J^n(\mathcal{A}/U)}$. Notice that by Lemma 2.4, we have $[p^n](J^n(\mathcal{A}/U)) = [p^n]^\circ(\mathcal{A})$ and since $[p^n]$ is proper (because $\mathcal{A}$ is proper over U), we see that $[p^n](J^n(\mathcal{A}/U))$ is closed and that the natural morphism $[p^n]_*(J^n(\mathcal{A}/U)) \to \mathcal{A}$ is finite.

The morphisms $\Lambda^{\mathcal{A}}_{n,n-1} : J^n(\mathcal{A}/U) \to J^{n-1}(\mathcal{A}/U)$ lead to a projective system of U-schemes

$$\cdots \to \mathrm{Crit}^2(\mathcal{X}, \mathcal{A}) \to \mathrm{Crit}^1(\mathcal{X}, \mathcal{A}) \to \mathcal{X}.$$

whose connecting morphisms are finite. We let $\mathrm{Exc}^n(\mathcal{A}, \mathcal{X}) \hookrightarrow \mathcal{X}$ be the scheme-theoretic image of $\mathrm{Crit}^n(\mathcal{A}, \mathcal{X})$ in $\mathcal{X}$.

For any $Q \in \mathcal{A}(U) = A(K_0)$, we shall write $\mathcal{X}^{+Q} = \mathcal{X} + Q$ for the translation of $\mathcal{X}$ by Q in $\mathcal{A}$.

Proposition 3.1. *There exists $\alpha = \alpha(\mathcal{A}, \mathcal{X}) \in \mathbb{N}$ such that for all $Q \in \Gamma$ the set $\mathrm{Exc}^\alpha(\mathcal{A}, \mathcal{X}^{+Q})$ is not dense in $\mathcal{X}^{+Q}$.*

Remark 3.2. Proposition 3.1 should be compared to Theorem 1 in [4].

The following theorem, proved by galois-theoretic methods in section 4, will play a crucial role in the proof of Proposition 3.1.

Let $S := \mathrm{Spec}\, k_0[[t]]$. Let $L := k_0((t))$ be the function field of S. For any $n \in \mathbb{N}$, let $S_n := \mathrm{Spec}\, k_0[t]/t^{n+1}$ be the n-th infinitesimal neighborhood of the closed point of S in S. Fix $\lambda_0 \in \mathbb{N}^*$ and let $R^{\mathrm{alg}} = R^{\mathrm{alg},\lambda_0} := \mathbb{F}_{p^{\lambda_0}}[[t]] \subseteq k_0[[t]]$. Let $S^{\mathrm{alg}} = S^{\mathrm{alg},\lambda_0} := \mathrm{Spec}\, R^{\mathrm{alg}}$. There is an obvious morphism $S \to S^{\mathrm{alg}}$.

Let $\mathcal{D}$ be an abelian scheme over S and let $\mathcal{Z} \hookrightarrow \mathcal{D}$ be a closed integral subscheme. Suppose that the abelian scheme has a model $\mathcal{D}^{\mathrm{alg}}$ over S^{alg} as an abelian scheme and that the immersion $\mathcal{Z} \hookrightarrow \mathcal{D}$ has a model $\mathcal{Z}^{\mathrm{alg}} \hookrightarrow \mathcal{D}^{\mathrm{alg}}$ over S^{alg}. If $c \in \mathcal{D}(S)$, write as usual $\mathcal{Z}^{+c} :=$

$\mathcal{Z}+c$ for the translation of $\mathcal{Z}$ by c in $\mathcal{D}$. Let D_0 (resp. D) be the fibre of $\mathcal{D}$ over the closed point of S (resp. over the generic point of S). If $c\in\mathcal{D}(S)$, let Z_0^{+c} (resp. Z^{+c}) be the fibre of $\mathcal{Z}^{+c}$ over the closed point of S (resp. over the generic point of S).

Notice that there is a natural inclusion $\mathcal{D}^{\rm alg}(S^{\rm alg})\subseteq\mathcal{D}(S)$.

Theorem 3.3. *Suppose that* $\mathrm{Tor}(D(\bar{L}))\cap X_{\bar{L}}^{+c}$ *is not dense in* $X_{\bar{L}}^{+c}$ *for all* $c\in\mathcal{D}^{\rm alg}(S^{\rm alg})\subseteq\mathcal{D}(S)$. *Then there exists a constant* $n_0=n_0(\mathcal{D},\mathcal{Z})\in\mathbb{N}^*$*, such that for all* $c\in\mathcal{D}^{\rm alg}(S^{\rm alg})\subseteq\mathcal{D}(S)$*, the set*

$$\{P\in Z_0^{+c}(k_0))\mid P\text{ lifts to an element of }\mathcal{Z}^{+c}(S_{n_0})\cap p^{n_0}\cdot\mathcal{D}(S_{n_0})\}$$

is not Zariski dense in Z_0^{+c}*.*

Proof. (of Theorem 3.3). This is a special case of Corollary 4.5. □

Proof. (of Proposition 3.1). Since $\mathcal{X}$ is flat over U and X is integral, we see that $\mathcal{X}$ is also integral (see for instance [14, 4.3.1, Prop. 3.8] for this). Hence it is sufficient to show that $\mathrm{Exc}^n(\mathcal{A},\mathcal{X}^{+Q})_u$ is not Zariski dense in $\mathcal{X}_u^{+Q}$ for some (any) closed point $u\in U$. Now using (1) in the previous section, we see that

$$\begin{aligned}\mathrm{Crit}^n(\mathcal{A},\mathcal{X}^{+Q})_u(k_0) &= ([p^n]_*(J^n(\mathcal{A}/U)))_u(k_0)\cap J^n(\mathcal{X}^{+Q}/U)_u(k_0)\\ &= \{P\in J^n(\mathcal{X}^{+Q}/U)_u(k_0)\,|\,\exists\widetilde{P}\in J^n(\mathcal{A}/U)_u(k_0)\;:\;p^n\cdot\widetilde{P}=P\}\\ &= \{P\in\mathcal{X}^{+Q}(u_n)\,|\,\exists\widetilde{P}\in\mathcal{A}(u_n)\;:\;p^n\cdot\widetilde{P}=P\}\end{aligned}$$

and thus

$$\mathrm{Exc}^n(\mathcal{A},\mathcal{X}^{+Q})_u(k_0) = \{P\in\mathcal{X}_u^{+Q}(k_0)\,|\,P\text{ lifts to an element of }\mathcal{X}^{+Q}(u_n)\cap p^n\cdot\mathcal{A}(u_n)\}$$

Now notice that $\mathcal{A}$ has a model $\widetilde{\mathcal{A}}$ as an abelian scheme over a curve $\widetilde{U}$, which is smooth over a finite field; also since the group Γ is finitely generated, we might assume that Γ is the image of a group $\widetilde{\Gamma}\subseteq\widetilde{\mathcal{A}}(\widetilde{U})$. Finally, we might assume that the immersion $\mathcal{X}\hookrightarrow\mathcal{A}$ has a model $\widetilde{\mathcal{X}}\hookrightarrow\widetilde{\mathcal{A}}$ over $\widetilde{U}$. We may thus apply Theorem 3.3 to the base-change of $\mathcal{X}\hookrightarrow\mathcal{A}$ to the completion of U at u. We obtain that there is an n_0 such that the set

$$\{P\in\mathcal{X}_u^{+Q}(k_0)\,|\,P\text{ lifts to an element of }\mathcal{X}^{+Q}(u_{n_0})\cap p^{n_0}\cdot\mathcal{A}(u_{n_0})\}$$

is not Zariski dense in $\mathcal{X}_u$ for all $Q\in\Gamma$. So we may set $\alpha=n_0$. □

3.2 End of proof

The proof of Theorem 1.3 is by contradiction. So suppose that $X \cap \Gamma$ is dense in X.

Let $P_1 \in \Gamma$ be such that $(X + P_1) \cap p \cdot \Gamma$ is dense, let $P_2 \in p \cdot \Gamma$ such that $(X + P_1 + P_2) \cap p^2 \cdot \Gamma$ is dense in $X + P_1 + P_2$ and so forth. The existence of the sequence of point $(P_i)_{i \in \mathbb{N}^*}$ is guaranteed by the assumption on Γ, which implies that $p^i\Gamma/p^{i+1}\Gamma$ is finite for all $i \geqslant 0$.

Now let $\alpha = \alpha(\mathcal{A}, \mathcal{X})$ be the natural number provided by Proposition 3.1. Let $Q = \sum_{i=1}^{\alpha} P_i$. By construction, the set $\mathcal{X}^{+Q} \cap p^\alpha \cdot \Gamma$ is dense in $\mathcal{X}^{+Q}$. On the other hand, by Lemma 2.5,

$$\begin{aligned}
\mathcal{X}^{+Q}(U) \cap p^\alpha \cdot \Gamma &= \Lambda^{\mathcal{A}}_{\alpha,0}(\lambda^{\mathcal{A}}_{\alpha}(\mathcal{X}^{+Q}(U) \cap p^\alpha \cdot \Gamma)) \subseteq \Lambda^{\mathcal{A}}_{\alpha,0}[\,\lambda^{\mathcal{X}}_{\alpha}(\mathcal{X}^{+Q}(U)) \cap \lambda^{\mathcal{A}}_{\alpha}(p^\alpha \cdot \Gamma)\,] \\
&\subseteq \Lambda^{\mathcal{A}}_{\alpha,0}[\,J^\alpha(\mathcal{X}^{+Q}/U) \cap p^\alpha \cdot J^\alpha(\mathcal{A}/U)(U)\,] \subseteq \Lambda^{\mathcal{X}}_{\alpha,0}[\,\mathrm{Crit}^\alpha(\mathcal{A}, \mathcal{X}^{+Q})\,] \\
&= \mathrm{Exc}^\alpha(\mathcal{A}, \mathcal{X}^{+Q})
\end{aligned}$$

and thus we deduce that $\mathrm{Exc}^\alpha(\mathcal{A}, \mathcal{X}^{+Q})$ is dense in $\mathcal{X}^{+Q}$. This contradicts Proposition 3.1 and concludes the proof of Theorem 1.3.

The proof of Corollary 1.4 now follows directly from Theorem 1.3 and from the following invariance lemma.

Lemma 3.4. *Suppose that the hypotheses of Theorem 1.1 hold. Let F' be an algebraically closed field and let $F'|F$ be a field extension. Then Theorem 1.1 holds if and only if Theorem 1.1 holds, with F' in place of F, $Y_{F'} \hookrightarrow B_{F'}$ in place of $Y \hookrightarrow B$, and the image $\Lambda_{F'} \subseteq B_{F'}(F')$ of Λ in place of Λ.*

Proof. The implication $\Longrightarrow$ follows from the fact that $Y_{F'} \cap \Lambda_{F'}$ is dense in $Y_{F'}$ if and only if $Y \cap \Lambda$ is dense in Y; indeed the morphism $\mathrm{Spec}\, F' \to \mathrm{Spec}\, F$ is universally open (see [7, IV, 2.4.10] for this).

Now we prove the implication $\Longleftarrow$. Let $C_1 := \mathrm{Stab}(Y_{F'})^{\mathrm{red}}$ and suppose that there exists

- a semiabelian variety B'_1 over F';
- a homomorphism with finite kernel $h_1 : B'_1 \to B_{F'}/C_1$;
- a model $\mathbf{B}'_1$ of B'_1 over a finite subfield $\mathbb{F}_{p^r} \subset F'$;
- an irreducible reduced closed subscheme $\mathbf{Y}'_1 \hookrightarrow \mathbf{B}'{}_1$;
- a point $b_1 \in (B_{F'}/C_1)(F')$, such that $Y_{F'}/C_1 = b_1 + h_{1,*}(\mathbf{Y}'_1 \times_{\mathbb{F}_{p^r}} F')$.

Now first notice that since $\mathrm{Stab}(\bullet)$ represents a functor, there is a natural isomorphism $\mathrm{Stab}(Y_{F'}) \simeq \mathrm{Stab}(Y)_{F'}$ and since F is algebraically closed also a natural isomorphism $\mathrm{Stab}(Y_{F'})^{\mathrm{red}} \simeq (\mathrm{Stab}(Y)^{\mathrm{red}})_{F'}$. Secondly, we have $\mathbb{F}_{p^r} \subset F$, since F is algebraically closed. Thirdly, if B_2 and B_3 are semiabelian varieties over F and $\phi : B_{2,F'} \to B_{3,F'}$ is a homomorphism of group schemes over F', then ϕ arises by base-change from an F-morphism $B_2 \to B_3$. This is a consequence of the fact that the graph of ϕ has a dense set of torsion points in $B_{2,F'} \times_{F'} B_{3,F'}$, and torsion points are defined in $B_2 \times_F B_3$. Putting these facts together, we deduce that there exists

- a semiabelian variety B' over F;
- a homomorphism with finite kernel $h : B' \to B/C$;
- a model $\mathbf{B}'$ of B' over a finite subfield $\mathbb{F}_{p^r} \subset F$;
- an irreducible reduced closed subscheme $\mathbf{Y}' \hookrightarrow \mathbf{B}'$;
- a point $b_1 \in (B_{F'}/C_{F'})(F')$, such that $Y_{F'}/C_{F'} = b_1 + h_{F',*}(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F')$.

where $C = \mathrm{Stab}(Y)^{\mathrm{red}}$. Now last point in the list above shows that $\mathrm{Transp}(Y_{F'}/C_{F'}, h_{F',*}(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F'))(F') \neq \emptyset$. Here $\mathrm{Transp}(\bullet)$ is the transporter, which is a generalization of the stabilizer (see [10, Exp. VIII, 6.] for the definition). Thus $\mathrm{Transp}(Y/C, h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F))(F) \neq \emptyset$, which is to say that there also exists

- a point $b_1 \in (B/C)(F)$, such that $Y/C = b_1 + h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$.

This concludes the proof. $\square$

4 Sparsity of highly p-divisible unramified liftings

This section can be read independently of the rest of the text and its results do not rely on the previous ones. Also, unlike the previous sections, *the terminology of this section is independent of the terminology of the introduction.*

Let S be the spectrum of complete discrete local ring. Let k be the residue field of its closed point. We suppose that k is a *finite field* of characteristic p. Let K be the fraction field of S. Let S^{sh} be the spectrum of the strict henselisation of S and let L be the fraction field of S^{sh}. We identify $\bar{k}$ with the residue field of the closed point of S^{sh}. For any $n \in \mathbb{N}$, we shall write

S_n (resp. S_n^{sh}) for the n-th infinitesimal neighborhood of the closed point of S (resp. S^{sh}) in S (resp. S^{sh}).

Let $\mathcal{A}$ be an abelian scheme over S and let $A := \mathcal{A}_K$. Write A_0 for the fibre of $\mathcal{A}$ over the closed point of S.

Theorem 4.1. *Let $\mathcal{X} \hookrightarrow \mathcal{A}$ be a closed integral subscheme. Let X_0 be the fibre of $\mathcal{X}$ over the closed point of S and let $X := \mathcal{X}_K$.*

Suppose that $\mathrm{Tor}(A(\bar{K})) \cap X_{\bar{K}}$ is not dense in $X_{\bar{K}}$.

Then there exists a constant $m \in \mathbb{N}$, such that the set

$$\{P \in X_0(\bar{k})) \mid P \text{ lifts to an element of } \mathcal{X}(S_m^{\mathrm{sh}}) \cap p^m \cdot \mathcal{A}(S_m^{\mathrm{sh}})\}$$

is not Zariski dense in X_0.

Suppose for the time of the next sentence that S is the spectrum of a complete discrete valuation ring, which is absolutely unramified and is the completion of a number field along a non-archimedean place. In this situation, M. Raynaud proves Theorem 4.1 and Corollary 4.5 below, under the stronger hypothesis that $X_{\bar{K}}$ does not contain any translates of positive-dimensional abelian subvarieties of $A_{\bar{K}}$ (see [18, Prop. II.1.1]). See also [19, Th. II, p. 207] for a more precise result in the situation where X is a smooth curve.

In the case where S is the spectrum of the ring of integers of a finite extension of $\mathbb{Q}_p$, Theorem 4.1 implies versions of the Tate-Voloch conjecture (see [24] and [22]). We leave it to the reader to work out the details.

Preliminary to the proof of 4.1, we quote the following result. Let B be an abelian variety over an algebraically closed field F and let $\psi : B \to B$ be an endomorphism. Let $R \in \mathbb{Z}[T]$ be a polynomial, which has no roots of unity among its complex roots. Suppose that $R(\psi) = 0$ in the ring of endomorphisms of B.

Proposition 4.2 (Pink-Rössler)**.** *Let $Z \subseteq B$ be a closed irreducible subset such that $\psi(Z) = Z$. Then $\mathrm{Tor}(B(F)) \cap Z$ is dense in Z.*

The proof of Proposition 4.2 is based on a spreading out argument, which is used to reduce the problem to the case where F is the algebraic closure of a finite field. In this last case, the statement becomes obvious. See [17, Prop. 6.1] for the details.

We shall use the map $[p^\ell]^\circ : A_0(\bar{k}) \to \mathcal{A}(S_\ell^{\rm sh})$, which is defined by the formula $[p^\ell]^\circ(x) = p^\ell{\cdot}\widetilde{x}$, where $\widetilde{x}$ is any lifting of x (this does not depend on the lifting; see [13, after Th. 2.1]).

Proof. (of Theorem 4.1). Let ϕ be a topological generator of $\mathrm{Gal}(\bar{k}|k)$. By the Weil conjectures for abelian varieties, there is a a polynomial

$$Q(T) := T^{2g} - (a_{2g-1}T^{2g-1} + \cdots + a_0)$$

with $a_i \in \mathbb{Z}$, such that $Q(\phi)(x) = 0$ for all $x \in A_0(\bar{k})$ and such that $Q(T)$ has no roots of unity among its complex roots. Let M be the matrix

$$\begin{bmatrix} 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ a_0 & a_1 & \dots & a_{n-2} & a_{2g-1} \end{bmatrix}$$

We view M as an endomorphism of abelian S-schemes $\mathcal{A}^{2g} \to \mathcal{A}^{2g}$. Let $\tau \in \mathrm{Aut}_S(S^{\rm sh})$ be the canonical lifting of ϕ. By construction, τ induces an element of $\mathrm{Aut}_{S_n}(S_n^{\rm sh})$ for any $n \geqslant 0$, which we also call τ. The reduction map $\mathcal{A}(S^{\rm sh}) \to \mathcal{A}(S_n^{\rm sh})$ is compatible with the action of τ on both sides. Write

$$u(x) := (x, \tau(x), \tau^2(x), \dots, \tau^{2g-1}(x)) \in (\prod_{s=0}^{2g-1} \mathcal{A})(S^{\rm sh})$$

for any element $x \in \mathcal{A}(S^{\rm sh})$. Abusing notation, we shall also write

$$u(x) := (x, \tau(x), \tau^2(x), \dots, \tau^{2g-1}(x)) \in (\prod_{s=0}^{2g-1} \mathcal{A})(S_n^{\rm sh})$$

for any element $x \in \mathcal{A}(S_n^{\rm sh})$. By construction, for any $x \in \mathcal{A}(S^{\rm sh})$ (resp. any $x \in \mathcal{A}(S_n^{\rm sh})$), the equation $Q(\tau)(x) = 0$ implies the vector identity $M(u(x)) = u(\tau(x))$.

Now consider the closed S-subscheme of $\mathcal{A}^{2g}$

$$\mathcal{Z} := \cap_{t \geqslant 0} M_*^t\big(\cap_{r \geqslant 0} M^{r,*}(\prod_{s=0}^{2g-1} \mathcal{X})\big)$$

where for any $r \geqslant 0$, M^r is the r-th power of M. The symbol $M_*^t(\cdot)$ refers to the scheme-theoretic image and the intersections are the scheme-theoretic intersections. The intersections are finite by noetherianity.

Let $\lambda : J \to \mathcal{A}^{2g}$ be a morphism of schemes. The construction of $\mathcal{Z}$ implies that if the following conditions are verified

(i) $M^r \circ \lambda$ factors through $\prod_{s=0}^{2g-1} \mathcal{X}$ for all $r \geqslant 0$ and

(ii) for all $r \geqslant 0$, there is a morphism $\phi_r : J \to \cap_{r\geqslant 0} M^{r,*}(\prod_{s=0}^{2g-1} \mathcal{X})$ such that $\lambda = M^r \circ \phi_r$

then λ factors through $\mathcal{Z}$.

In particular, if (i) is verified and $M^{r_\lambda} \circ \lambda = \lambda$ for some $r_\lambda \geqslant 1$, then λ factors through $\mathcal{Z}$.

Remark 4.3. In particular, this implies the following: if $x \in \mathcal{X}(S^{\rm sh})$ (resp. $x \in \mathcal{X}(S_n^{\rm sh})$) has the property that $Q(\tau)(x) = 0$, then $u(x) \in \mathcal{Z}(S^{\rm sh})$ (resp. $u(x) \in \mathcal{Z}(S_n^{\rm sh})$).

Lemma 4.4. *There is a set-theoretic identity* $M(\mathcal{Z}) = \mathcal{Z}$*.*

Proof. (of the lemma) Since M is proper, we have a set-theoretic identity

$$\mathcal{Z} = \cap_{t\geqslant 0} M^t \big(\cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X})\big)$$

Now directly from the construction, we have

$$M\big(\cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X})\big) \subseteq \cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X})$$

and hence we have inclusions

$$\cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X}) \supseteq M\big(\cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X})\big) \supseteq M^2\big(\cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X})\big) \supseteq \dots$$

and thus by noetherianity

$$M^\ell\big(\cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X})\big) = M^{\ell+1}\big(\cap_{r\geqslant 0} M^{r,-1}(\prod_{s=0}^{2g-1} \mathcal{X})\big)$$

for some $\ell \geqslant 0$. This implies the result. $\square$

Now we apply Proposition 4.2 and we obtain that $\mathcal{Z}_{\bar{K},\rm red} \cap \mathrm{Tor}(\prod_{s=0}^{2g-1} A(\bar{K}))$ is dense in $\mathcal{Z}_{\bar{K},\rm red}$. Hence the projection onto the first factor $\mathcal{Z}_K \to X$ is not surjective by hypothesis.

Let T be the scheme-theoretic image of the morphism $\mathcal{Z} \to \mathcal{X}$ given by the first projection. Notice that X_0 is a closed subscheme of T, because every element P of $X_0(\bar{k})$ satisfies the equation $Q(\phi)(P) = 0$. Let H be the closed subset of T, which is the union of the irreducible components of T, which surject onto S. A reduced irreducible component I of T, which surjects onto S, is flat over S; since $H \neq \mathcal{X}$, we have in particular $I \neq \mathcal{X}$ and so we see that the dimension of the fibre of I over the closed point of S is strictly smaller than the dimension of X_0. Hence the intersection of H and X_0 is a proper closed subset of X_0. Let T_1 be the open subscheme $T \backslash H$ of T. From the previous discussion, we see that the underlying set of T_1 is a *non-empty open subset of* X_0.

We are now in a position to complete the proof of Theorem 4.1. The proof will be by contradiction. So suppose that for all $\ell \in \mathbb{N}$, the set

$$\{P \in X_0(\bar{k}) \mid P \text{ lifts to an element of } \mathcal{X}(S_\ell^{\mathrm{sh}}) \cap p^\ell \cdot \mathcal{A}(S_\ell^{\mathrm{sh}})\}$$

is Zariski dense in X_0.

Choose an arbitrary $\ell \in \mathbb{N}$ and let $P \in T_1(\bar{k})$ be a point, which lifts to an element of $\mathcal{X}(S_\ell^{\mathrm{sh}}) \cap p^\ell \cdot \mathcal{A}(S_\ell^{\mathrm{sh}})$. This exists because the set of points in $X_0(\bar{k})$ with this property is assumed to be dense in X_0. Let $\widetilde{P} \in \mathcal{A}(S_\ell^{\mathrm{sh}})$ be such that $p^\ell \cdot \widetilde{P} \in \mathcal{X}(S_\ell^{\mathrm{sh}})$ and such that $p^\ell \cdot \widetilde{P}_0 = P$. Here $\widetilde{P}_0 \in A_0(\bar{k})$ is the $\bar{k}$-point induced by $\widetilde{P}$. Since the map $[p^\ell]^\circ : \mathcal{A}_0(\bar{k}) \to \mathcal{A}(S_\ell^{\mathrm{sh}})$ intertwines ϕ and τ, we see that

$$Q(\tau)([p^\ell]^\circ(\widetilde{P}_0)) = 0.$$

By the remark 4.3, we thus have

$$u([p^\ell]^\circ(\widetilde{P}_0)) \in \mathcal{Z}(S_\ell^{\mathrm{sh}}).$$

Hence

$$[p^\ell]^\circ(\widetilde{P}_0) \in T_1(S_\ell^{\mathrm{sh}}) \subseteq T(S_\ell^{\mathrm{sh}}).$$

This shows that $T_1(S_\ell^{\mathrm{sh}}) \neq \emptyset$. Since ℓ was arbitrary, this shows that the generic fibre $T_{1,K}$ of T_1 is not empty, which is a contradiction. $\square$

Corollary 4.5. *We keep the hypotheses of the Theorem 4.1. We suppose furthermore that* $\mathrm{Tor}(A(\bar{K})) \cap X_{\bar{K}}^{+c}$ *is not dense in* $X_{\bar{K}}^{+c}$ *for all* $c \in \mathcal{A}(S)$*. Then there exists a constant* $m \in \mathbb{N}$*, such that for all* $c \in \mathcal{A}(S)$ *the set*

$$\{P \in X_0^{+c}(\bar{k}) \mid P \text{ lifts to an element of } \mathcal{X}^{+c}(S_m^{\mathrm{sh}}) \cap p^m \cdot \mathcal{A}(S_m^{\mathrm{sh}})\}$$

is not Zariski dense in X_0^{+c}*.*

Here as usual $\mathcal{X}^{+c} = \mathcal{X} + c$ is the translate inside $\mathcal{A}$ of $\mathcal{X}$ by $c \in \mathcal{A}(S)$. Slightly abusing notation, we write X^{+c} for $(\mathcal{X}^{+c})_K$ and X_0^{+c} for $(\mathcal{X}^{+c})_k$.

Proof. By contradiction. Write $m(\mathcal{X}^{+c})$ for the smallest integer m such that

$$\{P \in X_0^{+c}(\bar{k}) \mid P \text{ lifts to an element of } \mathcal{X}^{+c}(S_m^{\mathrm{sh}}) \cap p^m \cdot \mathcal{A}(S_m^{\mathrm{sh}})\}$$

is not Zariski dense in X_0. Suppose that there exists a sequence $(a_n \in \mathcal{A}(S))_{n\in\mathbb{N}}$, such that $m(\mathcal{X}^{+a_n})$ strictly increases. Replace $(a_n \in \mathcal{A}(S))_{n\in\mathbb{N}}$ by one of its subsequences, so that $\lim_n a_n = a \in \mathcal{A}(S)$, where the convergence is for the topology given by the discrete valuation on the ring underlying S (notice that $\mathcal{A}(S)$ is compact for this topology, because S is complete and has a finite residue field at its closed point). Replace $(a_n \in \mathcal{A}(S))_{n\in\mathbb{N}}$ by one of its subsequences again, so that the image of a_n in $\mathcal{A}(S_n)$ equals the image of a in $\mathcal{A}(S_n)$. By construction, we have $m(\mathcal{X}^{+a_n}) \geqslant n$ and hence by definition $m(\mathcal{X}^a) \geqslant n$. Since this is true for all $n \geqslant 0$, this contradicts Theorem 4.1. □

The following corollary should be viewed as a curiosity only, since it is a special case of Theorem 1.3. The interest lies in its proof, which avoids the use of jet schemes, unlike the proof of Theorem 1.3.

Corollary 4.6. *We keep the notations and assumptions of Corollary 4.5. Suppose furthermore that S is a ring of characteristic p and that the fibres of $\mathcal{A}$ over S are ordinary abelian varieties. We also suppose that $\mathcal{X}$ is smooth over S. Let $\Gamma \subseteq A(K)$ be a finitely generated subgroup. Then the set $X \cap \Gamma$ is not Zariski dense in X.*

We shall call the topology on $A(K)$ induced by the discrete valuation *the v-adic topology*.

Before the proof of the corollary, recall a simple but crucial lemma of Voloch (see [1, Lemma1]):

Lemma 4.7 (Voloch)**.** *Let L_0 be a field and let T be a reduced scheme of finite type over L_0. Then $T(L_0^{\mathrm{sep}})$ is dense in T if and only if T is geometrically reduced.*

Proof. (of Corollary 4.6). The proof is by contradiction. We shall exhibit a translate of X by an element of $A(K)$, which violates the conclusion of Theorem 4.1. Suppose that $X \cap \Gamma$ is Zariski dense in X. Let $P_1 \in \Gamma$ be such that $(X + P_1) \cap p \cdot \Gamma$ is dense, let $P_2 \in p \cdot \Gamma$ such that $(X + P_1 + P_2) \cap p^2 \cdot \Gamma$ is dense in X and so forth. The existence of the sequence of point (P_i) is guaranteed by the assumption on Γ, which implies that the group $p^\ell\Gamma/p^{\ell+1}\Gamma$ is finite for all $\ell \geqslant 0$. Since the v-adic topology on the set $A(K)$ is compact (because S is a discrete valuation ring with a finite residue field), the sequence $Q_i = \sum_{\ell \geqslant 1}^{i} P_\ell$ has a subsequence, which converges in $A(K)$. Let Q be the limit point of such a subsequence. By construction, $(X+Q) \cap p^\ell \cdot A(K)$ is dense for all $\ell \geqslant 0$. Let $\mathcal{X}^{+Q} := \mathcal{X} + Q$.

Consider the morphism $([p^\ell]^*\mathcal{X}^{+Q})_{\mathrm{red}} \to \mathcal{X}^{+Q}$. There is a diagram

$$\begin{array}{ccccc} ([p^\ell]^*\mathcal{X}^{+Q})_{\mathrm{red}} \hookrightarrow & ([p^\ell]^*\mathcal{X}^{+Q}) & \xrightarrow{\qquad [p^\ell] \qquad} & & \mathcal{X}^{+Q} \\ & \big\downarrow & & & \big\downarrow \\ & \mathcal{A} & \xrightarrow{\mathrm{Frob}^\ell_{\mathcal{A}/S}} & \mathcal{A}^{(p^\ell)} \xrightarrow{\mathrm{Ver}^\ell} & \mathcal{A} \end{array}$$

where F_S is the absolute Frobenius morphism on S, $\mathcal{A}^{(p^\ell)} = F_S^{\ell,*}\mathcal{A}$ is the base-change of $\mathcal{A}$ by $F_S^{\ell,*}$, $\mathrm{Frob}_{\mathcal{A}/S}$ is the Frobenius morphism relatively to S and Ver is the Verschiebung (see [9, $\mathrm{VII}_{\mathrm{A}}$, 4.3] for the latter). The square is cartesian (by definition). By assumption, the morphism Ver is étale. Hence $\mathrm{Ver}^{\ell,*}(\mathcal{X}^{+Q})$ is a disjoint union of schemes, which are integral and smooth over S. Let $\mathcal{X}_1 \hookrightarrow \mathrm{Ver}^{\ell,*}(\mathcal{X}^{+Q})$ be an irreducible component such that $\mathcal{X}_{1,K} \cap \mathrm{Frob}^\ell_{A/K}(A(K))$ is dense. Let $\mathcal{X}_2 := (\mathrm{Frob}^{\ell,*}_{\mathcal{A}/S}(\mathcal{X}_1))_{\mathrm{red}}$ be the corresponding reduced irreducible component.

Now notice that $\mathcal{X}_{2,K}$ is geometrically reduced, since $\mathcal{X}_2(K)$ is dense in $\mathcal{X}_{2,K}$ (Voloch's lemma). Furthermore $\mathcal{X}_2$ is flat over S, because it is reduced and dominates S. Hence $(\mathcal{X}_2)^{(p^\ell)}$ is also flat over S. Furthermore, by its very construction $(\mathcal{X}_{2,K})^{(p^\ell)}$ is reduced, since $\mathcal{X}_{2,K}$ is geometrically reduced. Hence $(\mathcal{X}_2)^{(p^\ell)}$ is reduced (for this last step, see for instance [14, 4.3.8, p. 137]). Recall that $(\mathcal{X}_2)^{(p^\ell)}$ stands for the base-change of $\mathcal{X}_2$ by $F_S^{\ell,*}$. Notice that we have a commutative diagram

$$\begin{array}{ccc} \mathcal{X}_2 & \xrightarrow{\mathrm{Frob}^\ell_{\mathcal{X}_2/S}} & (\mathcal{X}_2)^{(p^\ell)} \\ \big\downarrow & & \big\downarrow \\ \mathcal{A} & \xrightarrow{\mathrm{Frob}^\ell_{\mathcal{A}/S}} & \mathcal{A}^{(p^\ell)} \end{array}$$

and that $\mathrm{Frob}^\ell_{\mathcal{X}_2/S}$ is bijective. Hence $(\mathcal{X}_2)^{(p^\ell)}$ is isomorphic to $\mathcal{X}_1$. Now since F_S is faithfully flat and $\mathcal{X}_2$ is flat over S, we see that $\mathcal{X}_2$ is actually smooth over S, because $\mathcal{X}_1$ is smooth over S. Hence every point of $\mathcal{X}_2(\bar{k})$ can be lifted to a point in $\mathcal{X}_2(S^{\mathrm{sh}})$ (see for instance [14, Cor. 6.2.13, p. 224]). Since the morphism $[p^\ell]$ is finite and flat and the scheme $\mathcal{X}^{+Q}$ is integral, we see that the map $\mathcal{X}_2 \to \mathcal{X}^{+Q}$ is surjective. This implies that the map $\mathcal{X}_2(\bar{k}) \to \mathcal{X}^{+Q}(\bar{k})$ is surjective. We conclude that *every element of $\mathcal{X}^{+Q}(\bar{k})$ is liftable to an element in $\mathcal{X}^{+Q}(S^{\mathrm{sh}}) \cap p^{\ell} \cdot \mathcal{A}(S^{\mathrm{sh}})$.*

Since ℓ was arbitrary, this contradicts Theorem 4.1. $\square$

Now we want to to conclude by

Remark 4.8. In [4], A. Buium also introduces an "exceptional set", which is very similar to the set Exc considered here and he makes a similar use of it (catching rational points). There is nevertheless one important difference between Buium's and our methods: the proof of Theorem 3.3, which is crucial in our study of the structure of Exc uses "Galois equations" and not differential equations as in [4]. In this sense, our techniques also differ from the techniques employed in [11], which is close in spirit to [4] and where the galois-theoretic language is not used either.

Remark 4.9. Although Corollary 1.4 shows that the Mordell-Lang conjecture may be reduced to the Manin-Mumford conjecture under the assumptions of Theorem 1.3, the difficulty of circumventing the fact that the underlying abelian variety might not be ordinary (which was a hurdle for some some time) is not thus removed. Indeed, the most difficult part of the algebraic-geometric proof of the Manin-Mumford conjecture given in [17] concerns the analysis of endomorphisms of abelian varieties, which are not globally the composition of a separable isogeny with a a power of a relative Frobenius morphism.

References

[1] Dan Abramovich and José Felipe Voloch, *Toward a proof of the Mordell-Lang conjecture in characteristic p*, Internat. Math. Res. Notices **5** (1992), 103–115.

[2] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[3] Alexandru Buium and José Felipe Voloch, *Lang's conjecture in characteristic p: an explicit bound*, Compositio Math. **103** (1996), no. 1, 1–6.

[4] A. Buium, *Intersections in jet spaces and a conjecture of S. Lang*, Ann. of Math. (2) **136** (1992), no. 3, 557–567.

[5] C. Corpet, *Around the Mordell-Lang and Manin-Mumford conjectures in positive characteristic*, in preparation.

[6] Dragos Ghioca and Rahim Moosa, *Division points on subvarieties of isotrivial semi-abelian varieties*, Int. Math. Res. Not., posted on 2006, Art. ID 65437, 23, DOI 10.1155/IMRN/2006/65437, (to appear in print).

[7] A. Grothendieck, *Éléments de géométrie algébrique.* Inst. Hautes Études Sci. Publ. Math. **4, 8, 11, 17, 20, 24, 28, 32** (1960-1967).

[8] Alexander Grothendieck, *Revêtements étales et groupe fondamental. Fasc. I: Exposés 1 à 5*, Séminaire de Géométrie Algébrique, vol. 1960/61, Institut des Hautes Études Scientifiques, Paris, 1963.

[9] *Schémas en groupes. I: Propriétés générales des schémas en groupes*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151, Springer-Verlag, Berlin, 1970.

[10] *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 152, Springer-Verlag, Berlin, 1962/1964.

[11] Ehud Hrushovski, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), no. 3, 667–690.

[12] Ehud Hrushovski and Boris Zilber, *Zariski geometries*, J. Amer. Math. Soc. **9** (1996), no. 1, 1–56, DOI 10.1090/S0894-0347-96-00180-4.

[13] N. Katz, *Serre-Tate local moduli*, Algebraic surfaces (Orsay, 1976), Lecture Notes in Math., vol. 868, Springer, Berlin, 1981, pp. 138–202.

[14] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné; Oxford Science Publications.

[15] Hideyuki Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989. Translated from the Japanese by M. Reid.

[16] Rahim Moosa and Thomas Scanlon, *Jet and prolongation spaces*, J. Inst. Math. Jussieu **9** (2010), no. 2, 391–430.

[17] Richard Pink and Damian Roessler, *On ψ-invariant subvarieties of semiabelian varieties and the Manin-Mumford conjecture*, J. Algebraic Geom. **13** (2004), no. 4, 771–798.

[18] M. Raynaud, *Around the Mordell conjecture for function fields and a conjecture of Serge Lang*, Algebraic geometry (Tokyo/Kyoto, 1982), Lecture Notes in Math., vol. 1016, Springer, Berlin, 1983, pp. 1–19.

[19] ______, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), no. 1, 207–233.

[20] Pierre Samuel, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*, Inst. Hautes Études Sci. Publ. Math. **29** (1966), 55–62.

[21] Thomas Scanlon, *A positive characteristic Manin-Mumford theorem*, Compos. Math. **141** (2005), no. 6, 1351–1364, DOI 10.1112/S0010437X05001879.

[22] ______, *The conjecture of Tate and Voloch on p-adic proximity to torsion*, Internat. Math. Res. Notices **17** (1999), 909–914.

[23] *Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux*, Astérisque, vol. 86, Société Mathématique de France, Paris, 1981.

[24] John Tate and José Felipe Voloch, *Linear forms in p-adic roots of unity*, Internat. Math. Res. Notices **12** (1996), 589–601.