Diophantine Approximation on Abelian varieties in characteristic p

José Felipe Voloch

1. Introduction

Let A be an abelian variety over a function field K in one variable over a finite field k. Let v be a place of K. In this paper we will study the topology induced on $A(K)$ by the v-adic topology on $A(K_v)$. In many cases this will lead to bounds for the v-adic distance between points in $A(K)$ in terms of their height and to abelian analogues of Leopoldt's conjecture. This paper also studies the question of integral points on affine open subsets of Abelian varieties in positive characteristics. In the classical case of number fields, Lang has conjectured and Faltings [F] proved that for A be an abelian variety over the number field K, if V is an affine open subset of A and S is a finite set of places of K, then the set of S-integral points of V is finite. Faltings has also a non-effective bound. Buium and the author [BV] obtained a similar result for function fields of characteristic zero, but in positive characteristic the problem has not been studied, except in dimension 1, i.e., for elliptic curves. In this case we have obtained, in [V], results on this problem. In this paper we will obtain a result under restrictive, but quite general, hypotheses for abelian varieties of arbitrary dimension and deduce the finiteness of integral points on affine subsets under these hypotheses. Our strategy will be similar to [BV]. The question of integral points is related to estimates for the v-adic distance from rational points to a divisor and this in turn will be estimated by the distance to a subvariety of smaller dimension. This inductive procedure, in the present situation, is provided by a general result of Hrushovski ([H], see theorem 1 below) and reduces the problem to our basic question of estimating v-adic distance between points.

We do not solve our problem in full generality. Our results are restricted to the cases when either A has "sufficiently general moduli"(in a sense that will be precised below) or is an elliptic curve defined over a finite field. The intermediate cases are still open.

Acknowledgments

This paper was planned as a collaboration with D. Abramovich. We had jointly obtained results similar to Hrushovski's theorem under the same restrictive hypotheses and using the same methods as in [AV]. We also had some ideas to deal with the open intermediate cases mentioned above, but there were some gaps in the argument that we hope to fix eventually. I thank him very much for the many conversations we had on this subject. I would like to thank also J.-P. Serre and J. Tate for pointers to the literature and the NSF (grant DMS-9301157) and the University of Texas's URI for financial support.

2. Local results

Let A/K be an abelian variety of dimension n. For any closed subscheme $X \subset A$ there is a function $\lambda_v(X,.) : A(K_v) \to [0,\infty]$ which satisfies the following property: for any affine open set $U \subset A$ and any system of generators $g_1,\dots,g_m \in \mathcal{O}(U)$ of the ideal defining $X \cap U$ in U, we may write $\lambda_v(X,P) = \min\{v(g_1(P)),\dots,v(g_m(P))\} + b(P)$ with b bounded on any bounded subset of $U(K_v)$. The function $\lambda_v(X,.)$ is uniquely determined by the above property up to the addition of a bounded function and is called the local height function associated to X. This notion is developed in detail in [Si]. In the analogous situation for number fields, Lang has conjectured [L] that $\lambda_v(X,P) \ll \log h(P) + O(1)$, for all $P \in A(K) \setminus X$, where $h(P)$ is the logarithmic height, and Faltings [F] proved that $\lambda_v(X,P) = o(h(P))$. The following result is theorem 6.3 of [H].

Theorem 1 (Hrushovski). *Let A and X be as above and assume that the K/k-trace of A is zero. Then there exists a subvariety Y of X, defined over $\bar{K}$, which is a finite union of translates of abelian subvarieties of A, such that $\lambda_v(X,P) \ll \lambda_v(Y,P) + 1$ for all $P \in A(K)$.*

Let A be an abelian variety over a local field of characteristic p with valuation v. Let A_1 be the formal group of A, that is the kernel of reduction modulo v. Then A_1 is naturally a $\mathbf{Z}_p$-module, since $p^n P \to \mathcal{O}, n \to \infty$ for P in A_1. We will be studying this $\mathbf{Z}_p$-module structure and will begin by lemma 1 below. Let us remark that it is not hard to check that A_1 has infinite $\mathbf{Z}_p$-rank. We will not, strictly speaking, need this fact but it

is helpful to put some of our results in perspective.

Lemma 1. *Let A be an ordinary Abelian variety over a local field of characteristic p with valuation v. There exists a neighbourhood U of $\mathcal{O}$ in the v-adic topology, such that $\lambda_v(\mathcal{O}, pP) = p\lambda_v(\mathcal{O}, P) + O(1)$ for all P in U.*

Proof: Let $n = \dim A$ and $t_1, \dots, t_n$ be local parameters at $\mathcal{O}$, so that $\lambda_v(\mathcal{O}, P) = \min\{v(t_1(P)), \dots, v(t_n(P))\}$ and the parameters can be chosen so that $t_i(pP) = a_i t_i(P)^p + \cdots, i = 1, \dots, n$, because A has an ordinary formal group, where the $\cdots$ represent a power series in $t_1(P), \dots, t_n(P)$ of degree greater than p and the a_i are non-zero v-adic integers. The result now follows. Note that the implied constant depends on the valuation of the a_i's, which in turn depend on the reduction type of A at v, in particular this constant is zero if A has good, ordinary reduction at v.

3. Global results

Lemma 2. *Let A be an abelian variety over a function field K over a finite field of characteristic $p > 0$ and v a place of K. Assume that $A[p^\infty] \cap A(K_s) = \Gamma$ is finite, where K_s is the separable closure of K. Then there is a neighbourhood U of $\mathcal{O}$ in the v-adic topology, such that, if $P \in A(K) \cap U$ then $P \in pA(K)$.*

Proof: Assume first that $\Gamma = \{\mathcal{O}\}$. Let $\ker[p]$ be the group subscheme of A which is the kernel of multiplication by p. For any field extension L/K, there is a coboundary map in flat cohomology of group-schemes, $\delta_L : A(L)/pA(L) \to H^1(L, \ker[p])$ which is injective. The image of δ_K is finite, by the Mordell-Weil theorem. Also δ_{K_v} is continuous in the v-adic topology. ([M2], Lemma III.6.5). It follows that there is a v-adic neighbourhood U of $\mathcal{O}$ such that if $P \in A(K) \cap U$ then $\delta_{K_v}(P) = 0$. We will show that, in fact $P \in pA(K)$, which will prove the lemma. From the above there exists $Q \in A(K_v)$, such that $pQ = P$. Let $L = K(Q)$, then L/K is a finite extension and $L \subset K_v$ so, in particular, v is unramified in L and, a fortiori, L/K is separable. Let M/K be the Galois closure of L/K. Then $P \in \ker \delta_M$. Hence $\delta_K(P)$ is in the kernel of the restriction map $H^1(K, \ker[p]) \to H^1(M, \ker[p])$. But, by the Hochschild-Serre spectral sequence ([M1], Remark II.2.21 (a)), the kernel of restriction

is the Galois cohomology group $H^1(\mathrm{Gal}(M/K), \ker[p](M))$. However, $\ker[p](M) = \mathcal{O}$ by hypothesis, since M/K is separable. Hence $\delta_K(P) = 0$, which shows that $Q \in A(K)$. Note that since $\Gamma = \{\mathcal{O}\}$, Q is uniquely determined by P. We claim that, as $P \to \mathcal{O}$ v-adically, we have $Q \to \mathcal{O}$ also. Indeed, if this were not so, there would be a sequence $P_n \to \mathcal{O}$ with $P_n = pQ_n$ and Q_n bounded away from $\mathcal{O}$. Since $A(K_v)$ is compact, after passing to a subsequence, we can assume that $Q_n \to Q \neq \mathcal{O}$ and $pQ = \mathcal{O}$, but Q is separable over K, since is defined over K_v and this contradicts $\Gamma = \{\mathcal{O}\}$.

In general, let $\phi : A \to A/\Gamma = B$ and $\psi : B \to A, \phi \circ \psi = [p^m]$. If $P \in A(K)$ is sufficiently close to $\mathcal{O}$ v-adically, then so is $\phi(P)$ and therefore, by the above there exists $Q \in B(K), \phi(P) = p^{m+1}Q = \phi(\psi(pQ))$. Therefore $P - p\psi(Q) \in \Gamma$, but if we choose P sufficiently close to $\mathcal{O}$ then Q will be close to $\mathcal{O}$ also and therefore, $P - p\psi(Q) = \mathcal{O}$ since Γ is finite. This completes the proof.

Theorem 2. *Let A be an ordinary abelian variety over a function field K of characteristic $p > 0$ and v a place of K and assume that the K/k-trace of A is zero and that $A[p^\infty] \cap A(K_s)$ is finite. Let X be a subvariety of A. Then $\lambda_v(X, P) \ll h(P)^{1/2}$ for all $P \in A(K), P \notin X$.*

Corollary 1. *Hypotheses as in Theorem 2. Assume further that X is an ample divisor. Then for any finite set S of places of K, the set of S-integral points of $A \backslash X$ is finite.*

Proof of corollary 1: In this case, $h(P)$, for an S-integral point of $A \backslash X$, is the sum of $\lambda_v(X, P)$ over the elements of S, and it follows that the height is bounded, which proves the corollary.

Proof of theorem 2: By theorem 1, we can replace X by Y which is a finite union of translates of abelian subvarieties of A and by taking a component of Y, we can assume that Y is an abelian subvariety of A. Finally passing to A/Y we are reduced to showing that $\lambda_v(\mathcal{O}, P) \ll h(P)^{1/2}$ for all $P \in A(K)$.

Now, using theorem 1 and lemmas 1 and 2 we may assume that $P \in U$, where U is a neighbourhood of $\mathcal{O}$ in the v-adic topology such that for all $P \in A(K) \cap U$ we have $P \in pA(K)$ and $\lambda_v(\mathcal{O}, pP) \leq p\lambda_v(\mathcal{O}, P) + O(1)$. Moreover, we can assume that U does

not contain any non-zero torsion point. Let r be maximal with $P = p^r Q, Q \in A(K) \cap U$, which exists since P is not torsion. Then $\lambda_v(\mathcal{O}, P) \leq p^r(\lambda_v(\mathcal{O}, Q) + O(1))$. Also $\lambda_v(\mathcal{O}, Q)$ is bounded, since if Q were sufficiently close to $\mathcal{O}$ then Lemma 2 would imply that r is not maximal. It follows that there exists $c > 0$ such that $\lambda_v(\mathcal{O}, P) \leq cp^r$. On the other hand, since Q is not a torsion point, $h(P) = p^{2r}h(Q) \geq dp^{2r}$, where d is the minimum height of a non-torsion point. Putting these inequalities together, we get $\lambda_v(\mathcal{O}, P) \leq cp^r \leq (c/d^{1/2})h(P)^{1/2}$, as desired.

4. Moduli and p-torsion points

In this section we show that the condition that $A[p^\infty] \cap A(K_s)$ is finite holds if A has sufficiently general moduli.

Suppose T is a scheme, S is a scheme over T and A is an abelian scheme over S. Let $\boldsymbol{\omega}^1_A$ denote the sheaf on S of invariant relative one-forms on A/S and ${}^tA$ the dual of A. Then one has the Kodaira-Spencer pairing $\kappa: \boldsymbol{\omega}^1_A \otimes \boldsymbol{\omega}^1_{{}^tA} \to \Omega^1_{S/T}$. Let $S = \mathrm{Spec}(R)$, where R is a complete local ring of characteristic p with residue field $\bar{k}$ and $T = \mathrm{Spec}(\bar{k})$. Let f denote the map ${}^tA \to S$ and $\Omega^1_{R/\bar{k}} = \Omega^1_{S/T}$. Then the sequence of sheaves on ${}^tA$

$$0 \to f^*\Omega^1_{R/\bar{k}} \to \Omega^1_{{}^tA/\bar{k}} \to \Omega^1_{{}^tA/R} \to 0$$

is exact. Let Kod denote the composition

$$\boldsymbol{\omega}^1_{{}^tA} \cong f_*\Omega^1_{{}^tA/R} \to R^1 f_* f^* \Omega^1_{R/\bar{k}} \cong R^1 f_* \mathcal{O}_{{}^tA} \otimes \Omega^1_{R/\bar{k}},$$

where the second map is the boundary map. Then, $\kappa(\omega, {}^t\omega) = \omega.Kod({}^t\omega)$.

For an object X over R, we let $\bar{X}$ denote its special fibre. Suppose the residue field $\bar{k}$ of R is algebraically closed. If m is the maximal ideal of R, a construction of Serre and Tate gives a pairing $q: T_p\bar{A}(\bar{k}) \times T_p^t\bar{A}(\bar{k}) \to 1 + m$ for an ordinary abelian variety A, where $T_p\bar{A}(\bar{k})$ is the "physical" Tate module of $\bar{A}$, which in turn gives local parameters on the local moduli space of ordinary abelian varieties over an Artin local ring of residue characteristic p (see [K]). In [K], Katz gives formulas for the Serre-Tate parameters in terms

of the Kodaira-Spencer pairing. We will need the following theorem which is a corollary of Katz's results.

Suppose A and ${}^tA$ are dual ordinary abelian varieties over R. If $\alpha \in T_pA$, we can view it as a homomorphism from the p-divisible group of ${}^tA$ to $\mathbf{G}_m$, the formal multiplicative group. We define then, $\omega_\alpha = \alpha^*(dt/t) \in \boldsymbol{\omega}^1_{{}^tA}$, where dt/t is the canonical invariant form on $\mathbf{G}_m$. For $a \in R^*$, let $d\log(a) = da/a \in \Omega^1_{R/\bar{k}}$.

Theorem 3 (Katz). *Suppose R is as above, $\bar{k}$ is algebraically closed and A is an ordinary abelian variety over R. If $\alpha \in T_p\bar{A}(\bar{k})$ and ${}^t\alpha \in T_p^t\bar{A}(\bar{k})$, we have:*

$$d\log q(\alpha, {}^t\alpha) = \kappa(\omega_{{}^t\alpha}, \omega_\alpha) \ .$$

To justify the assertion, made in the introduction, that abelian varieties with sufficiently general moduli satisfy the hypotheses of Theorem 2, we will prove the following result.

Proposition. *Let A be an ordinary abelian variety over a function field K of characteristic $p > 0$ such that the Kodaira-Spencer map has maximal rank, then $A[p] \cap A(K_s) = \mathcal{O}$.*

Proof: Let us briefly recall the definition of the Serre-Tate pairing (see [K]). Given an element of $T_p\bar{A}(\bar{k}) \times T_p^t\bar{A}(\bar{k})$ one constructs canonically a subgroup of the p-divisible group of A isomorphic to an extension of $\mathbf{Z}_p$ by $T_p\mu$, where the latter is the p-divisible group of p-power roots of unity. Then the value of the Serre-Tate pairing is the class of this extension in $\mathrm{Ext}^1(\mathbf{Z}_p, T_p\mu)$. If we are interested (as is the case) only in the Serre-Tate pairing modulo p-th powers, we can restrict our attention to extensions of $\mathbf{Z}/p\mathbf{Z}$ by μ_p contained in the group-scheme $\ker[p]$. If $A[p] \cap A(K_s)$ contains a non-zero element, it gives rise to a trivial such extension for each subgroup of $\ker[p]$ isomorphic to μ_p. It follows that the Serre-Tate pairing modulo p-th powers is not of maximal rank and hence, from Katz's theorem, that the Kodaira-Spencer map is also not of maximal rank, proving the proposition.

5. Abelian analogues of Leopoldt's conjecture in characteristic p

Leopoldt's conjecture asserts that the $\mathbf{Z}_p$-rank of the p-adic closure of the group of units of a number field is the same as the $\mathbf{Z}$-rank of the group of units. This is known in a few cases but is open in general. An analogue of it for function fields of characteristic p has been shown by Kisilevsky [Ki]. These questions have obvious abelian analogues replacing the multiplicative group by an abelian variety and we will study this question now. Recall that A_1, the kernel of reduction in $A(K_v)$, is naturally a $\mathbf{Z}_p$-module. Also, since we assumed that K is a function field in one variable over a finite field, $A_1 \cap A(K)$ is of finite index in $A(K)$.

Theorem 4. *Let A be an ordinary abelian variety over a function field K of characteristic $p > 0$ and v a place of K and assume that $A[p^\infty] \cap A(K_s) =$ is finite. Then the $\mathbf{Z}_p$-rank of the closure of $A_1 \cap A(K)$ in $A(K_v)$ in the v-adic topology is equal to the $\mathbf{Z}$-rank of $A(K)$.*

Proof: Let $P_1, \ldots, P_n \in A(K)$ be $\mathbf{Z}$-linearly independent generating $A_1 \cap A(K)$ over $\mathbf{Z}$ and assume that they become $\mathbf{Z}_p$ dependent, say $\sum \alpha_i P_i = 0$. We may assume that not all the α_i are divisible by p. Let a_i be integers p-adically close to α_i. Then $a_i - \alpha_i$ are divisible by a high power of p and so $\sum (a_i - \alpha_i) P_i$ is v-adically close to zero, hence $\sum a_i P_i$ is close to zero which implies, by lemma 2, that the a_i are divisible by p, but then so are the α_i, giving a contradiction that proves the theorem.

Remark: Theorem 4 is valid, with the same proof, for semi-abelian varieties satisfying the same hypotheses. In particular it is valid for the multiplicative group, giving a new proof of the characteristic p analogue of Leopoldt's conjecture already proved by Kisilevsky [Ki].

The same proof as in Lemma 2 yields the following result:

Lemma 3. *Let A be an abelian variety defined over a finite field k and F be the corresponding Frobenius automorphism of A. Let K/k be a function field of characteristic $p > 0$ and v a place of K. Then there is a neighbourhood U of $\mathcal{O}$ in the v-adic topology, such that, if $P \in A(K) \cap U$ then $P \in F(A(K))$.*

It is also clear that points v-adically close to $\mathcal{O}$ have images under F even closer to

$\mathcal{O}$. It follows that if R is the completion of the ring $\mathbf{Z}[F]$ with respect to the maximal ideal generated by F then the R-rank of the v-adic closure of $A(K)$ in $A(K_v)$ is equal to the $\mathbf{Z}[F]$-rank of $A(K)$. If R happens to be contained in $\mathbf{Z}_p$ then the $\mathbf{Z}_p$-rank of the v-adic closure of $A(K)$ in $A(K_v)$ will be smaller than the $\mathbf{Z}$-rank of $A(K)$. This happens for example if A is an ordinary elliptic curve defined over the finite field k. Indeed, let $x^2 - ax + q$ be the characteristic polynomial of Frobenius (hence $\#A(k) = q + 1 - a$). Since A is ordinary, a is prime to $q = \#k$, so the characteristic polynomial has a p-adic root $\phi \equiv 0 \bmod p$ and $\mathbf{Z}[F] = \mathbf{Z}[\phi] \subset \mathbf{Z}_p$. Hence the analogue of Leopoldt's conjecture fails in this case. This example also shows that Theorem 2 does not hold with the hypothesis on the p-power torsion removed.

Corollary 2. *Let A be an ordinary abelian variety over a function field K of characteristic $p > 0$ and v a place of K and assume that $A[p^\infty] \cap A(K_s)$ is finite. If $P \in A(K) \cap A_1$ and $\alpha \in \mathbf{Z}_p$ is irrational then αP is transcendental over K.*

Proof: Assume by contradiction that αP is algebraic and extend K, if necessary, so that it is rational. However, if α is irrational, P and αP are $\mathbf{Z}$-independent, but $\mathbf{Z}_p$-dependent, contradicting Theorem 4 and remark (b) above.

Remarks:(c) The analogue of this corollary for the multiplicative group has been proved by Mendès France and van der Poorten [MP].

(d) There is an analogue of this corollary for ordinary elliptic curves defined over a finite field. However one needs to assume that $\alpha \notin \mathbf{Z}[F]$. (See lemma 3 and the discussion following it).

References.

[AV] D. Abramovich and J. F. Voloch, *Toward a proof of the Mordell- Lang conjecture in characteristic p*, International Math. Research Notices No. 5 (1992) 103-115.

[BV] A. Buium, J. F. Voloch, *Integral points of abelian varieties over function fields of characteristic zero*, Math. Ann. **297** (1993) 303-307.

[F] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. Math. **133** (1991) 549-576.

[H] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, preprint, 1993.

[K] N. M. Katz, *Serre-Tate local moduli*, Springer LNM 868 (1981) 138-202.

[Ki] H. Kisilevsky, *Multiplicative independence in function fields*, J. Number Theory **44** (1993) 352-355.

[L] S. Lang, *Number Theory III: Diophantine Geometry*, Encyclopaedia Math. Sci. **60**, Springer, Berlin 1991.

[MP] M. Mendès France, A. J. van der Poorten, *Automata and the arithmetic of formal power series*, Acta Arithmetica, **XLVI** (1986) 211-214.

[M1] J. S. Milne, *Étale cohomology*, Princeton Univ. Press, 1990.

[M2] J. S. Milne, *Arithmetic duality theorems*, Academic Press, Orlando, 1986.

[P] A. N. Parshin, *Finiteness theorems and hyperbolic manifolds*, in *The Grothendieck festschrift*, P. Cartier et al., eds., Birkaüser, Basel, 1990, vol. 3,pp 163-178.

[Si] J. H. Silverman, *Arithmetic distance functions and height functions in Diophantine geometry*, Math. Ann. **279** (1987) 193-216.

[V] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990) 247-258.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu