THE abc THEOREM FOR COMMUTATIVE ALGEBRAIC GROUPS IN CHARACTERISTIC p

THOMAS SCANLON

Abstract. Buium proved what he called the *abc* theorem for abelian varieties over function fields in characteristic zero [3]. Using methods of algebraic model theory we prove an analog of his theorem for commutative algebraic groups in characteristic p.

In what follows, k is an algebraically closed field of characteristic p, C is a smooth projective curve over k, and $K = k(C)$ is the function field of C. Identify each point $x \in C(k)$ with its corresponding valuation $v_x := \mathrm{ord}_x$ on K.

The purpose of this paper is to demonstrate:

Theorem 0.1. *Let A be an abelian variety over K. Let $f : A \to \mathbb{P}^1$ be a rational function. Let r be a positive integer, then there is a bound $B_r \in \mathbb{Z}$ such that for any $P \in A(K)$ either there are some $a \in A(K^{sep})$ and $Q \in A(K)$ such that $f(Q) \in \{0, \infty\}$ and $P = Q + [p^r]a$ or $v_x(f(P)) \leq B_r$ for any $x \in C(k)$.*

Theorem 0.1 is the characteristic p analog of Buium's *abc* theorem [3]. Our proof works for more general commutative algebraic groups and for distances computed to subvarieties of codimension greater than one. More general statements are in Section 1.

Our proof follows the general form of Buium's proof. We construct uniformly continuous homomorphisms from $A(K^{sep})$ to some unipotent group with kernel $[p^r]A(K^{sep})$ using differential algebra. The maps allow us to bound the distance from points in $A(K) \setminus [p^r]A(K^{sep})$ to 0. We then use a general lemma on approximations to reduce the theorem to the case of bounding the distance to a point. These estimates dovetail to give a proof of the theorem. Using Hrushovski's Mordell-Lang theorem [8] we can give qualitative estimates on the growth of B_r with r in many cases.

The results of this paper formed a chapter of my Ph. D. thesis [14] written under the direction of E. Hrushovski whom I now thank for his advice. I thank B. Mazur for his advice and for insisting that a more geometric presentation of these arguments be given (though I admit that the argument is still not geometric). I thank D. Abramovich and J. F. Voloch for their comments on an earlier version.

1. A More General Formulation

We give now a definition of the distance to a subvariety.

Definition 1.1. Let $Y \subseteq \mathbb{A}^n_K$ be a subvariety of affine space over K. Let $P \in \mathbb{A}^n(K)$. Let $x \in C(k)$. Then the distance from P to Y is

$$d_{v_x}(P, Y) \quad := \quad \min\{v_x(f(P)) : f \in I_Y \cap \mathcal{O}_{K,v_x}[X_1, \ldots, X_n]\}$$

Date: 9 July 1997.

Let X be a quasi-compact variety over K. Let $\mathcal{V} := \{V_i\}$ be a finite affine cover of X. Let $\varphi_i : V_i \hookrightarrow \mathbb{A}^M$ express the affine co-ordinates on V_i. Let $Y \subseteq X$ be a subvariety. If $P \in X(K)$ and $x \in C(k)$ then

$$d_{v_x}(P, Y) \quad := \quad \min\{d_{v_x}(\varphi_i(P), \varphi_i(V_i \cap Y)) : P \in V_i(K)\}$$

Remark 1.2. As presented, the distance to a subvariety depends on the choice of an affine cover. We suppress this dependence in the notation, but it is still there.

Finally, we need the notion of an *almost integral* set of points.

Definition 1.3. Let $\Upsilon \subseteq C(k)$. A subset $\Sigma \subseteq \mathbb{A}^N(K)$ of affine space over K is said to be *almost* Υ*-integral* if $\{v_x(\sigma) : \sigma \in \Sigma, x \in \Upsilon\}$ is bounded below.

If X is an abstract variety over K, then $\Sigma \subseteq X(K)$ is said to be *almost* Υ*-integral* if for some (equivalently, any) affine cover $\mathcal{V} = \{V_i\}$ of X relative to the affine co-ordinates on V_i, $V_i(K) \cap \Sigma$ is almost Υ-integral for each i.

Now for the more general version of Theorem 0.1.

Theorem 1.4. *Let $T \subseteq C(k)$ be a finite set of closed points. Let $U = C \setminus T$. Let G be a commutative algebraic group over K. Let $\Gamma \subseteq G(K)$ be a finitely generated subgroup. Assume that Γ is almost $U(k)$-integral. Let $X \subseteq G$ be a subvariety. Let $r \in \mathbb{Z}_+$. Then there is an integer B_r such that for any $P \in \Gamma$ either there is some $Q \in \Gamma \cap X$ and $a \in G(K^{sep})$ such that $P = Q + [p^r]a$ or $d_{v_x}(P, X) \leq B_r$ for any $x \in U(k)$.*

The statement of Theorem 1.4 implicitly involves a choice of a finite affine cover of G.

Remark 1.5. We included the more general statement involving the proximity functions not only to formally strengthen the theorem but because our proof – even for the case of X a hypersurface – passes through the case of X of higher codimension.

We can give a more geometric statement of Theorem 1.4.

Theorem 1.6. *Let $U = C \setminus T$ where T is a finite set of closed points. Let G be a smooth commutative quasi-projective group scheme over U. Let $\Gamma \subseteq G(U)$ be a finitely generated subgroup. Let $\eta := \mathrm{Spec} K \hookrightarrow U$ denote the inclusion of the generic point into U. Consider the sections of G over U as K-rational points of G_η via $\iota : G(U) \hookrightarrow G_\eta(K)$. Let $X \subseteq G$ be a closed subscheme over U. Let r be a positive integer. There is an integer B_r such that for any $P \in \Gamma$ either there is some $Q \in \Gamma$ with $\iota(Q) \in X_\eta(K)$ and $a \in G_\eta(K^{sep})$ such that $\iota(P) = \iota(Q) + [p^r]a$ or $P \notin X_x(\mathcal{O}_{C,x}/\mathfrak{m}_x^{B_r+1})$ for all points $x \in U(k)$.*

We abused notation slightly in the above statement by denoting the image of P in $X_x(\mathcal{O}_{C,x}/\mathfrak{m}_x^{B_r+1})$ by P as well. In this geometric context, B_r may be regarded as a bound on the order of contact of the curve P with X at x. Theorem 1.6 may be regarded as an instance of Theorem 1.4 by taking an affine cover for G over U and then lifting this cover to G_η to calculate the distances.

Remark 1.7. It is necessary to allow B_r to grow with r. Consider for example the case of $G = \mathbb{G}_m$ and $X = 1$. Then one has $d_{v_x}([p]P, X) = p \cdot d_{v_x}(P, X)$. For general, if X is the origin of G, then B_r is $O(p^{rh})$ where h is the height of the formal group of G.

If it should happen that the Zariski closure of $X \cap \Gamma$ is a finite union of cosets, then the growth of B_r is bounded in the same way as it is when X is just the origin. Hrushovski's Mordell-Lang theorem [8] ensures that this hypothesis is true for a wide class of G and X. If X falls into this class, we will say that X is *general* *with respect to* k. We give a precise description of this class below, but the reader is advised to regard the phrase X *is general with respect to* k as a synonym for *the Mordell-Lang conjecture is true in the case* X. Roughly, a general variety has the property that the only subvarieties which descend to k are cosets of groups.

Definition 1.8. Let k be an algebraically closed field of characteristic p. Let K/k be an extension of fields. Let G be a commutative algebraic group over K and let $X \subseteq G$ be a subvariety. X is said to be *general with respect to* k if the following condition holds.

Whenever $H \subseteq G$ is a semi-abelian variety defined over K^{alg}, H_0 is a semi-abelian variety defined over k, $X_0 \subseteq H_0$ is an irreducible subvariety defined over k, $\phi : H \to H_0$ is a homomorphism, and $a \in G$, then $(a + \phi^* X_0) \cap X \subseteq Y \subseteq Y \subseteq X$ for some Y a coset of a group variety.

Example 1.9. If G is a simple abelian variety of sufficiently general moduli, then G can have no positive dimensional image defined over k. In the case, every subvariety of G will be general with respect to k.

Example 1.10. If X is itself a coset of a group, then X is general for in the definition of general we may take $Y = X$.

With the definition of *general* in place, we can state a version of Theorem 1.4 with estimates on B_r.

Theorem 1.11. *Let G be a commutative algebraic group over K. Let $X \subseteq G$ be a general subvariety. Let $T \subseteq C(k)$ be a finite set of points and let $U = C \setminus T$. Let $\Gamma \subseteq G(K)$ be a finitely generated almost $U(k)$-integral subgroup. Let h be the height of the maximal semi-abelian quotient of G. There are constants $C_1, C_2 \in \mathbb{Z}_+$ such that for any integer r if $P \in \Gamma$ either there are $Q \in \Gamma \cap X$ and $a \in [p^r]G(K^{sep})$ with $P = Q + [p^r]a$ or $d_{v_x}(P, X) < C_1 p^{rh} + C_2$ for any $x \in U(k)$.*

2. Valuation Estimates for Hasse-Schmidt Derivations

Our goal in this section is to construct differential operators on K which behave well with respect to all the K/k-places.

Let R be a commutative ring. A stack of HS derivations on R is given by a sequence of functions $\{\partial_n : R \to R\}_{n=0}^{\infty}$ satisfying

- $\partial_0(x) = x$
- $\partial_n(x + y) = \partial_n(x) + \partial_n(y)$
- $\partial_n(x \cdot y) = \sum_{i+j=n} \partial_i(x) \cdot \partial_j(y)$
- $\partial_i \circ \partial_j(x) = \binom{i+j}{i} \partial_{i+j}(x)$

Call a ring with a specified stack of HS derivations an *HS-differential ring*. The functional equations for a stack of HS derivations ensure that the map $R \to R[[\epsilon]]$ defined by $x \mapsto \sum_{i=0}^{\infty} \partial_i(x)\epsilon^i$ is a ring homomorphism.

Remark 2.1. Iterativity is not included in the definition of HS derivations in [10]. Since we will have no use for non-iterative stacks of HS derivations, we have built it into the definition so as to avoid repeating the word "iterative."

On the field $k(t)$ there is a natural choice a stack of HS derivations given by the ring homomorphism $\sigma : k(t) \to k(t)[[\epsilon]]$ determined by $\sigma|_k = \mathrm{id}_k$ and $\sigma(t) = t + \epsilon$.

Iterativity corresponds to the commutativity of

$$\begin{array}{ccc} k(t)[[\epsilon]] & \xrightarrow{\sigma} & k(t)[[\epsilon,\eta]] \\ \sigma\uparrow & & \uparrow \\ k(t) & \xrightarrow{\sigma} & k(t)[[\epsilon+\eta]] \end{array}$$

which in our case comes down to $t + (\epsilon + \eta) = (t + \eta) + \epsilon$.

Let $a \in k$. Then $\sigma(t-a)^m = ((t-a)+\epsilon)^m = \sum_{j=0}^{\infty} \binom{m}{j}(t-a)^{m-j}\epsilon^j$ so that $\partial_j(t-a)^m = \binom{m}{j}(t-a)^{m-j}$.

Observe that $Fix(\sigma) = k$.

Lemma 2.2. *Let k be an algebraically closed field. Let $\{\partial_n\}_{n=0}^{\infty}$ be the stack of HS derivations on $k(t)$ given by $t \mapsto t + \epsilon$. For any $f \in k(t)$ and $x \in \mathbb{P}^1(k)$ one has $v_x(\partial_n f) \geq v_x(f) - n$.*

■ We reduce the question to consider only $f \in k[t]$.

Claim 2.3. *If this lemma is valid for f and g, then it is also valid for fg.*

✠

$$\begin{aligned} v(\partial_n(fg)) &= v(\sum_{i+j=n} \partial_i(f)\partial_j(g)) \\ &\geq \min_{i+j=n} \{v(\partial_i(f)) + v(\partial_j(g))\} \\ &\geq \min_{i+j=n} \{(v(f)-i) + (v(g)-j)\} \\ &= v(fg) - n \end{aligned}$$

✠

Claim 2.4. *If the lemma is valid for $f \neq 0$, then it is also valid for $\frac{1}{f}$.*

✠ We calculate

$$\begin{aligned} 0 &= \partial_n(1) \\ &= \partial_n(f \cdot \frac{1}{f}) \\ &= f\partial_n(\frac{1}{f}) + \sum_{i=1}^{n} \partial_i(f)\partial_{n-i}(\frac{1}{f}) \end{aligned}$$

We proceed with the proof of the claim by induction on n. When $n = 0$ the claim is trivial. In general,

$$\begin{aligned} v(\partial_n(\frac{1}{f})) &= v(\sum_{i=1}^{n} \frac{\partial_i f}{f} \partial_{n-i}(\frac{1}{f})) \\ &\geq \min_{1\leq i\leq n} \{v(\frac{\partial_i f}{f}) + v(\partial_{n-i}(\frac{1}{f}))\} \\ &\geq \min_{1\leq i\leq n} \{-i + [v(\frac{1}{f}) - (n-i)]\} \\ &= v(\frac{1}{f}) - n \end{aligned}$$

✠

By the two claims it suffices to consider $f \in k[t]$. When $f = 0$, the lemma is obvious so we take $f \neq 0$.

If $x \in \mathbb{A}^1(k)$, then we may expand f as $f = \sum_{i \geq N} f_i(t-x)^i$ where $f_N \neq 0$ and each $f_i \in k$. Then by the k-linearity of ∂_n, we compute $\partial_n(f) = \sum_{i \geq N} \binom{i}{n} f_i(t-x)^{i-n}$ which visibly has v_x valuation at least $N - n = v_x(f) - n$. When considering the place at ∞ given by $v_\infty(f) = -\text{ord}(f)$ observe that each ∂_n actually decreases the order so that $v_\infty(\partial_n f) \geq v(f) \geq v(f) - n$. ■

Lemma 2.5. *Let (K, v) be a discretely valued field. Let $\{\partial_n\}_{n=0}^\infty$ be a stack of HS derivations on K satisfying $\inf\{v(\partial_n x) - v(x) : x \in K^\times\} = B_n > -\infty$. Then there is a unique extension of the stack of HS derivations to completion K_v also satisfying $\inf\{v(\partial_n x) - v(x) : x \in K_v^\times\} = B_n$.*

■ The hypothesis on ∂_n implies that it is a continuous function on K. Thus, there is a unique extension of ∂_n to a continuous function on the completion K_v. Since K_v is a topological ring, each of the following functions is continuous.

$$\begin{aligned} Z(x) &:= \partial_0(x) - x \\ A_n(x,y) &:= \partial_n(x) + \partial_n(y) - \partial_n(x+y) \\ M_n(x,y) &:= \partial_n(xy) - \sum_{i+j=n} \partial_i(x)\partial_j(y) \\ I_{i,j}(x) &:= \partial_i \circ \partial_j(x) - \binom{i+j}{i} \partial_{i+j}(x) \end{aligned}$$

As $\{\partial_n\}_{n=0}^\infty$ is a stack of HS derivations on K, each of these functions is identically zero on K (or $K \times K$ depending on the number of arguments). Since K is dense in K_v, these functions must be identically zero on K_v as well. That is, $\{\partial_n\}_{n=0}^\infty$ is a stack of HS derivations on K_v.

The valuation $v : K_v \to \mathbb{Z} \cup \{\infty\}$ is continuous and takes the value ∞ only at zero so that the functions $E_n(x) := v(\partial_n x) - v(x)$ are continuous as maps $K^\times \to \mathbb{Z}$. By the hypotheses, $E_n^{-1}\{N : N \geq B_n\} \supseteq K^\times$. Again since K is dense in K_v, we must have $E_n^{-1}\{N : N \geq B_n\} = K_v^\times$. ■

Lemma 2.6. *If (K, v) is a discretely valued field with an algebraically closed residue field and $\{\partial_n\}_{n=0}^\infty$ is a stack of HS derivations on K satisfying $\inf\{v(\partial_n x) - v(x) : x \in K^\times\} = B_n > -\infty$, then for any finite unramified extension L/K, there is a unique extension of the stack of HS derivations still satisfying $\inf\{v(\partial_n x) - v(x) : x \in K^\times\} = B_n$.*

■ Since the residue field of K is algebraically closed, L embeds over K into K_v as a valued field. Since L is a finite separable extension of K, there is a unique extension of the stack of HS derivations to L ([10] Theorem 9.23). Thus the stack on L must agree with the restriction of the stack on K_v. By Lemma 2.5 the stated inequalities are true on K_v and hence on L. ■

Lemma 2.7. *Let (K, v) be a complete discretely valued field with a stack of HS derivations satisfying* $\inf\{v(\partial_n x) - v(x) : x \in K^\times\} = B_n > -\infty$. *Let L/K be a finite separable totally ramified extension of K. Then there is a unique extension of the stack of HS derivations to L. This stack satisfies* $\inf\{v(\partial_n x) - v(x) : x \in L^\times\} = \tilde{B}_n > -\infty$

Remark 2.8. In general, $\tilde{B}_n \neq B_n$. We will not need a precise calculation of $\tilde{B}_n$, but we note that it depends on B_n, $[L : K]$, the valuation of the the different, and linearly on n.

■ That there is unique extension of the stack is Theorem 9.23 of [10]. Let $e := [L : K]$. Let $\pi \in \mathcal{O}_L$ be a uniformizer. For each pair of integers (a, i) with $0 \leq i < e$ and $a \in \mathbb{N}$ define $E_{a,i} := v(\partial_a \pi^i) - v(\pi^i)$. Let n be given. Define $B^{(n)} := \max\{B_j : 0 \leq j \leq n\}$ and $E^{(n)} := \max\{E_{a,i} : 0 \leq a \leq n, 0 \leq i < e\}$.

Claim 2.9. *We may take* $\tilde{E}_n := B^{(n)} + E^{(n)}$.

✠ In the following calculation each $x_i \in K$ and at least one x_i is not zero.

$$\begin{aligned} v(\partial_n(\sum_{i=0}^{n-1} x_i\pi^i)) &= v(\sum_{i=0}^{n-1} \partial_n(x_i\pi^i)) \\ &\geq \min_{0\leq i<n}\{v(\partial_n(x_i\pi^i))\} \\ &= \min_{0\leq i<n}\{v(\sum_{a+b=n} \partial_b(x_i)\partial_a(\pi^i))\} \\ &\geq \min_{0\leq i<n, a+b=n}\{v(x_i) - B_b + v(\pi^i) - E_{a,i}\} \\ &\geq \min_{0\leq i<n}\{v(x_i) + v(\pi^i)\} - \tilde{B}_n \\ &= v(\sum_{i=0}^{n-1} x_i\pi^i) - \tilde{B}_n \end{aligned}$$

✠

■

Lemma 2.10. *Let k be an algebraically closed field. Let L be a finitely generated extension of transcendence degree one. There is a stack of HS derivations $\{\partial_n\}_{n=0}^\infty$ satisfying*

- $L^{(p)} = \ker \partial_1$ *and*
- *there are constants $B_n \in \mathbb{Z}$ such that for any L/k-place v and $x \in L^\times$ one has $v(\partial_n x) \geq v(x) - B_n$.*

■ Express L as a finite separable extension of $k(t)$. Let $\{\partial_n\}_{n=0}^\infty$ be the stack of HS derivations on $k(t)$ corresponding to $t \mapsto t + \epsilon$. By our calculation above, $\ker \partial_1 = k(t^p)$. Let $\{\partial_n\}_{n=0}^\infty$ also denote the unique extension of this stack to L (which exists because the extension is separable). Since $L/k(t)$ is separably algebraic, the extension on the constant fields is also separably algebraic. Thus, $\ker \partial_1 = L^{(p)}$.

As L is a separable extension of $k(t)$, only finitely many places ramify. For any unramified place v, Lemmas 2.2 and 2.6 show that $v(\partial_n x) \geq v(x) - n$ for $x \in L^\times$.

Use Lemmas 2.2 and 2.7 to bound the difference $v(\partial_n x) - v(x)$ for each of the finitely many ramified valuations. ■

From now on we will assume that K of Theorem 1.4 is equipped with such a stack of HS derivations.

Lemma 2.11. *Let K be a field with a stack of HS derivations $\{\partial_n\}_{n=0}^{\infty}$. Let Λ be an ordered abelian group. Let Σ be a set of Λ-valuations on K. Let $\{B_n\}_{n=0}^{\infty}$ be a sequence of elements of Λ with the property that for each $x \in K^{\times}$ and valuation $v \in \Sigma$ one has $v(\partial_n x) \geq v(x) - B_n$.*

Let $F(X_1, \ldots, X_n)$ be a polynomial over K in $\{\partial_j X_i\}_{j=0,i=1}^{M,n}$ with $F(0, \ldots, 0) = 0$. Then there is some $B_F \in \Lambda$ such that for any tuple $\mathbf{a} := (a_1, \ldots, a_n) \in K^n$ and valuation $v \in \Sigma$ if $v(\mathbf{a}) := \min_i\{v(a_i)\} \geq 0$, then $v(F(\mathbf{a})) \geq v(\mathbf{a}) - B_F$.

■ We proceed by induction on the construction of F. If $F = \partial_j X_i$, then the result is already true by hypothesis with $B_F = B_j$.

Suppose $F = GH$ and the result is true for G and H. Let $\mathbf{a}$ and v be given with $v(\mathbf{a}) \geq 0$.

$$\begin{aligned} v(F(\mathbf{a})) &= v(G(\mathbf{a})) + v(H(\mathbf{a})) \\ &\geq v(\mathbf{a}) - B_G + v(\mathbf{a}) - B_H \\ &\geq v(\mathbf{a}) - (B_G + B_H) \end{aligned}$$

So we may take $B_F = B_G + B_H$. (N.B.: We used $v(\mathbf{a}) \geq 0$ to obtain the last inequality.)

Suppose now $F = G + H$ and the result is true for G and H. Again take $\mathbf{a} \in K^n$ and $v \in \Sigma$ with $v(\mathbf{a}) \geq 0$.

$$\begin{aligned} v(F(\mathbf{a})) &= v(G(\mathbf{a}) + H(\mathbf{a})) \\ &\geq \min\{v(G(\mathbf{a}), v(H(\mathbf{a})\} \\ &\geq \min\{v(\mathbf{a}) - B_G, v(\mathbf{a}) - B_H\} \\ &= v(\mathbf{a}) - \max\{B_G, B_H\} \end{aligned}$$

So we may take $B_F = \max\{B_G, B_H\}$. ■

3. Manin Maps

In this section we will construct homomorphism $\psi_r : G(K^{sep}) \to U_r(K^{sep})$ which in co-ordinates are polynomials in $\{\partial_m X_i\}$ and have $\ker \psi_r = [p^r]G(K^{sep})$. It was observed in the introduction to [8] that the existence of these maps follows from elimination of quantifiers and imaginaries for the the theory of separably closed fields of imperfection degree one in the differential language. Buium and Voloch have constructed such maps for ordinary abelian varieties in the case of $r = 1$ using jet space and explicit p-descent methods [5]. We will construct these maps using a strictly model theoretic argument and also by using jet spaces. Of course, these methods come to the same thing. One could also construct these maps via cohomology (fppf or crystalline) or by an analysis of the formal groups. We will leave these points of view to another paper.

3.1. **Model Theoretic Construction of Manin Maps.** All of what is said in this section can be done with only the hypothesis $1 < [K : K^p] < \infty$ by merely changing the notation slightly, but to avoid the use of multi-indices and because we only need the case of $[K : K^p] = p$, we will work only in this case.

Let $t \in K \setminus K^p$. For any r, $\{t^i\}_{i=0}^{p^j-1}$ is a basis for K over K^{p^j}. In fact, for any L/K a separable extension satisfying $[L : L^p] = p$ this set is still a basis for L over L^p. Define co-ordinate functions by the formula

$$x \quad = \quad \sum_{i=0}^{p^j-1} \xi_i^j(x)^{p^j} t^i$$

The stability of the theory of separably closed fields was first proved by Wood and Shelah [17]. Quantifier elimination in the language with the co-ordinate functions was proved by Delon [7]. Elimination of imaginaries was proved by Messmer [11]. See [12] for a more complete discussion of the model theory of separably closed fields. As noted in the introduction to [8], one can deduce the existence of the Manin maps from these model theoretic properties of separably closed fields.

Lemma 3.1. *Let G be a commutative algebraic group over L a separably closed field with $[L : L^p] = p$ and fixed a p-basis given by $t \in L \setminus L^p$. For any positive integer r, there are a unipotent algebraic group H_r and a group homomorphism $\psi_r : G(L) \to H_r(L)$ where ψ_r is given piecewise as a rational function in the ξ co-ordinate functions such that* $\ker \psi_r = [p^r]G(L)$.

■ Without loss of generality, we may assume G is connected. Working in co-ordinates, we may take G to be a definable (in the field language) group. $[p^r]G(L)$ is definable by the formula $x \in [p^r]G \iff (\exists y \in G)\ [p^r]y = x$. By elimination of imaginaries, there is a definable function $\psi : G(L) \to L^m$ for some m such that the fibres of ψ are the cosets of $[p^r]G(L)$. By elimination of quantifiers, ψ may be given piecewise as a rational function in the ξ co-ordinate functions. By the Weil-Hrushovski group chunk theorem [2], the image of ψ embeds into a definable group H such that the generic type of $G(L)$ maps to the generic type of H. By [11], there is an embedding $\phi : H \to W$ of H into an algebraic group. Again, ϕ may be given by rational functions in the ξ functions. Replacing W with the Zariski closure of the image of ϕ, we may assume that that the generic type of H maps to the field theoretic generic type of W. In the statement of the theorem, $\psi_r = \phi \circ \psi$ and $H_r = W$. Since the exponent of $G(K)/[p^r]G(K)$ is $\leq p^r$, the same is true of W. This implies that W is unipotent. ■

3.2. **Jet Space Construction of Manin Maps.** We now change the language slightly so that this map may be understood as a differential rational map. We choose an iterative stack of Hasse derivations having the property that $\ker \partial_1 = K^{(p)}$. To be explicit, Let $t \in K \setminus K^{(p)}$ and take the stack determined by the equations $\partial_n t^m = \binom{m}{n} t^{m-n}$. Since ∂_n is linear over $K^{(p^{\lceil \log_p(n)+1 \rceil})}$, these equations do fully determine the stack of HS derivations and also show how to calculate the functions $\partial_n(x)$ in terms of the functions $\xi_i^j(x)$. If t is fixed as a parameter, then one can calculate the ξ-functions in terms of the HS derivations as well.

It is shown in [13] that the theory of K^{sep} given with the stack of derivations (but without necessarily fixing t) still admits quantifier elimination and elimination of imaginaries.

For any scheme over a ring R with a stack of HS derivations we can produce a projective system of jet scheme $\nabla_r X$. Let $\varphi : R \to R[[\epsilon]]$ be the map given by the HS derivations. Denote by φ_n the composite map

$$R \xrightarrow{\varphi} R[[\epsilon]] \longrightarrow R[[\epsilon]]/(\epsilon^{n+1}) = R[\epsilon]/(\epsilon^{n+1})$$

Define X_n by the following Cartesian square.

$$\begin{array}{ccc} X & \longleftarrow & X_n \\ \downarrow & & \downarrow \\ \mathrm{Spec} R & \xleftarrow{\varphi_n^*} & \mathrm{Spec} R[\epsilon]/(\epsilon^{n+1}) \end{array}$$

Define $\nabla_n X$ to be the Weil restriction of X_n from $R[\epsilon]/(\epsilon^{n+1})$ to R. $\nabla_n X$ is known to be a scheme when X is quasi-projective over R (see Theorem 4 of Section 7.6 of [1]).

Let us now use the language of jet schemes to re-interpret the construction of the Manin maps.

We use the model theoretic results at only one point.

Lemma 3.2. *Let K be a separably closed field of imperfection degree one. Let $\{\partial_n\}_{n=0}^{\infty}$ be a stack of HS derivations on K with* $\ker \partial_1 = K^{(p)}$*. Let G be a commutative algebraic group over K. For any $r \in \mathbb{N}$ there is some $N_r \in \mathbb{N}$ and a constructible set $Y_r \subseteq \nabla_{N_r} G$ such that $[p^r]G(K) = \nabla_{N_r}^{-1} Y_r(K)$.*

■ Theorem 3.12 of [13] shows that the theory of K in the differential language admits elimination of quantifiers. This implies that the solution set to the formula $\phi(x) = \lceil x \in G(K) \& (\exists y \in G(K))[p^r]y = x \rceil$ is equivalent to a quantifier-free formula in x. Such formulas correspond to Boolean combinations of differential equations. A differential equation is simply an algebraic equation on $\nabla_N(x)$ for $N \gg 0$. Y_r is the constructible subset of $\nabla_N X$ describing these equations. ■

Let us fix some notation. If $f : X \to Y$ is a morphism of varieties over a field L, then $f_* X$ will denote the image of X in Y computed over L^{alg}. In general, $f_* X$ need not be closed in Y, but in case X and Y are both group varieties and f is a homomorphism, then $f_* X$ is itself a closed subgroup variety of Y.

Proposition 3.3. *Let K be a separably closed field with $[K : K^{(p)}] = p$. Let $\{\partial_n\}_{n=0}^{\infty}$ be a stack of HS derivations on K with* $\ker \partial_1 = K^{(p)}$*. Let G be a commutative algebraic group over K. Let $r \in \mathbb{N}$. Then there is a unipotent group W_r and a function $\psi_r : G(K) \to W_r(K)$ which is locally a HS-differential-polynomial – in fact, ψ_r is of the form $\phi_r \circ \nabla_{N_r}$ for $\phi_r : \nabla_{N_r} X \to W_r$ a regular function – such that* $\ker \psi_r = [p^r]G(K)$*.*

■ Before proceeding, we need a little more information about Y_r.

Claim 3.4. *Y_r in Lemma 3.2 may be taken to be a group variety. In fact, we may take $Y_r = [p^r]_* \nabla_{N_r} G$.*

✠ Any Zariski closed subvariety of Y_r containing the image of $[p^r]G(K)$ under ∇_{N_r} will work. So we might as well take the Zariski closure of this image. By the very definition of the jet space, $\nabla_{N_r}(G(K))$ is Zariski dense in $\nabla_{N_r}G$. Hence, $[p^r]\circ\nabla_{N_r}(G(K)) = \nabla_{N_r}([p^r]G(K))$ is Zariski dense in the algebraic group $[p^r]_*\nabla_{N_r}G$. ✠

Let W_r be the quotient $\nabla_{N_r}G/[p^r]_*\nabla_{N_r}G$ and let $\phi_r : \nabla_{N_r}G \to W_r$ be the quotient map. The map ψ_r is then $\phi_r \circ \nabla_{N_r}$. Since $W_r(K^{sep})$ has exponent at most p^r, it must be unipotent. ■

4. Uniformities in the Function Field Mordell-Lang Conjecture

We will need to make concrete some of the uniformities inherent in Hrushovski's Theorem [8]. Let us first restate the main theorem of [8].

Theorem 4.1 (Hrushovski)**.** *Let K be a separably closed field of characteristic p. Assume the $1 < [K : K^{(p)}] < \infty$. Let G be a semi-abelian variety over K. Let L be a separable separably closed extension of K with the property that $L = L^{(p)}K$ and $[L : L^{(p)}] = [K : K^{(p)}]$. Define $[p^\infty]G(L) := \bigcap_{n=1}^\infty [p^n]G(L)$. Let $X \subseteq G$ be a subvariety of G defined over L. Assume that X is general relative to $\bigcap_{n=1}^\infty L^{(p^n)}$. Then there finitely many group subvarieties $G_1, \ldots, G_n$ of G and points $a_1, \ldots, a_n \in G(L)$ such that $X \cap [p^\infty]G(L) = (\bigcup_{i=1}^n a_i + G_i) \cap [p^\infty]G(L)$.*

We observe that one may replace "semi-abelian variety" by "commutative algebraic group" in the hypotheses on G in Hrushovski's theorem since for any commutative algebraic group G the algebraic group $[p^r]_*G$ is a semi-abelian variety for $r \gg 0$.

In the next proposition we will use the compactness theorem of first order logic to re-interpret the above statement to give a uniformity result over K.

Proposition 4.2. *Let K be a separably closed field of characteristic p with $1 < [K : K^{(p)}] < \infty$. Let $k = \cap K^{p^n}$. Let G be a commutative algebraic group over K. Let $X \subseteq G$ be a subvariety of G defined over some L a separably closed separable extension of K having the same p-basis. Assume that X is general with respect to $\bigcap_{n=0}^\infty L^{(p^n)}$. Then there is a finite set Ξ of semi-abelian subvarieties of G and integers N and M such that for any point $a \in G(L)$*

$$(X + a) \cap [p^N]G(L) \quad = \quad \bigcup_{i=1}^m (a_i + H_i) \cap [p^N]G(L)$$

with $0 \le m \le M$, $H_i \in \Xi$, and $a_i \in G(L)$.

■ If this proposition were false, then for each natural number N and finite set of semi-abelian subvarieties $\Xi = \{G_1, \ldots, G_n\}$ of G (possibly listed with multiplicity) defined over K, it would be consistent with the theory of L that

$$(\exists b)(\forall a_1, \ldots, a_n)(X + b) \cap [p^N]G \neq (\bigcup_{i=1}^n a_i + G_i) \cap [p^N]G$$

By the compactness theorem, the following set of formulas has a model:

(1) the elementary diagram of L

(2) for each natural number N and finite sequence of semi-abelian subvarieties of G defined over K, $G_1, \ldots, G_n$, the formula

$$(\forall a_1, \ldots, a_n \in G)(\exists y \in G)(\exists z \in G)[y = [p^N]z \quad \text{and} \quad (y - \mathbf{c} \in X \setminus \bigcup_{i=1}^{n} a_i + G_i \quad \text{or} \quad y - \mathbf{c} \in [\bigcup_{i=1}^{n} a_i + G_i) \setminus X])]$$

Let M be such a model which is $\aleph_1$-saturated and let $\mathbf{c} \in G(M)$ be the point interpreting the formal symbol $\mathbf{c}$.

Claim 4.3. (1) *M is a separable separably closed extension of K with $M = M^{(p)}K$ and $[M : M^{(p)}] = [M : M^{(p)}]$.*

(2) *There is no finite sequence $G_1, \ldots, G_n$ of semi-abelian subvarieties of G defined over K and points $a_1, \ldots, a_n \in G(M)$ such that $\mathbf{c} + X \cap [p^\infty]G(M) = (\bigcup_{i=1}^{n} a_i + G_i) \cap [p^\infty]G(M)$.*

✠

(1) Since M is a model of the elementary diagram of L, the extension M/L is elementary and hence M/K is elementary. The property of being separably closed is first-order so M is separably closed. The other property may be expressed by fixing a basis B for K over $K^{(p)}$ and insisting that B also be a basis for M over $M^{(p)}$.

(2) Suppose that $G_1, \ldots, G_n$ are semi-abelian subvarieties of G defined over K and $a_1, \ldots, a_n \in G(M)$ such that $(X + \mathbf{c}) \cap [p^\infty]G(M) = (\bigcup_{i=1}^{m} a_i + G_i) \cap [p^\infty]G(M)$. Since M is $\aleph_1$-saturated, for N sufficiently large we must have $(X + \mathbf{c}) \cap [p^N]G(M) = (\bigcup_{i=1}^{m} a_i + G_i) \cap [p^N]G(M)$. This violates a condition on $\mathbf{c}$.

✠

Since every semi-abelian subvariety G is defined over the separable closure of the field of definition of G, Hrushovski's theorem implies that in fact $(X + \mathbf{c}) \cap [p^\infty]G(M) = \bigcup_{i=1}^{m} (a_i + G_i) \cap [p^\infty]G(M)$ for some $a_i \in G(M)$ and G_i semi-abelian subvarieties defined over K. This gives the contradiction. ■

5. Main Theorem

For the rest of this paper we revert to the notation of Theorem 1.4. Recall that we equipped K with a stack of HS derivations via Lemma 2.10.

Lemma 5.1. *Let $a \in G(K)$. Let $r \in \mathbb{Z}_+$. Then there is a bound B_r such that for any $P \in \Gamma \setminus (a + [p^r]G(K^{sep}))$ and any $x \in C(k)$ one has $d_{v_x}(P, a) \le B_r\}$.*

■ By replacing the group operation on G with $+_a$ defined by $Q +_a R := Q + R - a$, we may assume that $a = 0$.

Let $\psi_r : G(K) \to U_r(K)$ be the map of Proposition 3.1 with kernel $G(K) \cap [p^r]G(K^{sep})$. The underlying variety of U_r is an affine space. Let $\tau : U_r \to U_r$ be the translation (with respect to the usual additive group structure on affine space) which takes $\psi_r(0)$ to the origin. On any particular affine open V_i in the fixed cover G containing 0, we may translate by some ρ so that in co-ordinates 0 corresponds to the origin. Set $\phi_{r,i} := \tau \circ \psi_r \circ \rho_i$.

By our hypothesis on Γ, $\Gamma/(\Gamma \cap [p^r]G(K^{sep}))$ is finite. Thus $\phi_{r,i}(\Gamma)$ is a finite set.

On the affine patch V_i, let $\vartheta_i : V_i \to \mathbb{A}^N$ give the affine co-ordinates.

For any particular $\mathbf{b} \in \mathbb{A}^n(K) \setminus \{(0, \ldots, 0)\}$, there is a constant C such that $-C \leq v_x(\mathbf{b}) \leq C$ for $x \in U(k)$. Let C be the maximum over these constants for the non-zero elements of $\phi_{r,i}(\Gamma)$. By Lemma 2.11, for $P \in V(K) \setminus [p^r]G(K^{sep})$ and $x \in U(k)$ either $v_x(\vartheta_i(P)) < 0$ or we have $C \geq v_x(\phi_{r,i}(P)) \geq v_x(P) - B_{\phi_{r,i}}$. Let $B_r := \max_i B_{r,i}$. The bound is then $\max\{C + B_r, 0\}$. ■

Lemma 5.2. *Let $H \subseteq G$ be an algebraic subgroup. Let $a \in G(K)$. Let $r \in \mathbb{Z}_+$. Then there is a bound B_r such that for any $x \in C(k)$ and any $P \in \Gamma \setminus [(a + H(K)) + [p^r]G(K^{sep})]$, one has $d_{v_x}(P, a + H) \leq B_r$.*

■ Apply Lemma 5.1 to the algebraic group G/H. ■

The next Lemma appeared as Proposition 6.3 in [8] for the case of a single valuation. A more general version of this Lemma appears as Proposition 4.2.3 in [14].

Lemma 5.3. *Let $Y, Z \subseteq \mathbb{A}^n_K$ be subvarieties of affine n-space over K. Let $\Xi \subseteq \mathbb{A}^n_K$ be defined by differential equations. Assume that for any HS-differential field extension L of K that $Y(L) \cap \Xi(L) = Z(L) \cap \Xi(L)$. Then there is a constant $m \in \mathbb{N}$ such that for any point $P \in \Xi(K)$ and any $x \in U(k)$ if $v_x(P) \geq 0$ then $d_{v_x}(P, Y) \leq n \cdot (d_{v_x}(P, Z) + 1)$.*

■

If the lemma were false, then for each $n \in \mathbb{N}$ we could find a point $x \in U(k)$ corresponding to a valuation $v_n := v_x$ a point $P_n \in \Xi(\mathcal{O}_{K,v_n})$ such that $d_{v_n}(P_n, Y) > n \cdot (d_{v_n}(P_n, Z) + 1)$.

Let $(\mathbf{K}, \mathbf{v}, \mathbf{\Gamma})$ be a non-principal ultraproduct $\prod_{/\mathcal{F}}(K, v_n, \mathbb{Z})$.

Let $\mathbf{P}$ be the image of (P_n) in $\mathcal{O}_{\mathbf{K}}$.

Let $\xi := d_{\mathbf{v}}(\mathbf{P}, Y) + 1$.

Let $\mathfrak{p} := \{x \in R : (\forall n \in \mathbb{Z}_+) \ \mathbf{v}(x) > n \cdot \xi\}$.

Claim 5.4. *$\mathfrak{p}$ is prime.*

✠ Let $x, y \in \mathcal{O}_{\mathbf{K}} \setminus \mathfrak{p}$. We have $\mathbf{v}(x) \leq n \cdot \xi$ and $\mathbf{v}(y) \leq m \cdot \xi$ for some $m, n \in \mathbb{Z}_+$. Thus, $v(xy) \leq (n + m)\xi$ so that $xy \notin \mathfrak{p}$. ✠

Claim 5.5. *$\mathfrak{p}$ is an HS differential ideal.*

✠ Let $x \in \mathfrak{p}$. Let $n \in \mathbb{Z}_+$. For any N, by Lemma 2.10 and Łos' Lemma, $\mathbf{v}(\partial_N x) \geq (n + N)\xi - B_N \geq n\xi$ so that $\partial_N x \in \mathfrak{p}$ as well. ✠

The localization of $\mathcal{O}_{\mathbf{K}}$ at $\mathfrak{p}$ is $\mathcal{O}_{\mathbf{K},\mathfrak{p}} = \{x \in \mathbf{K} : (\exists n \in \mathbb{Z}) \ v(x) > n\xi\}$. By Lemma 2.10, $\mathcal{O}_{\mathbf{K},\mathfrak{p}}$ is a sub-HS-differential-ring of $\mathbf{K}$. Since for each $z \in K^\times$ we have that $\{v_x(y) : x \in U(k)\}$ is bounded in $\mathbb{Z}$, we have that $K^\times \hookrightarrow \mathcal{O}_{\mathbf{K},\mathfrak{p}}^\times$ via the diagonal map so that composing with the quotient map we obtain a map of HS-differential fields $K \to L := \mathcal{O}_{\mathbf{K},\mathfrak{p}}/\mathfrak{p}$.

Let $\mathbf{P}$ continue to denote its image in $\Xi(L)$. By construction, $\mathbf{P} \in (Z \cap \Xi)(L) \setminus (Y \cap \Xi)(L)$. This is a contradiction. ■

Lemma 5.6. *If X is a quasi-compact variety over K, $Y, Z \subseteq X$ are subvarieties, $\Xi \subseteq X(K)$ is a subset defined Zariski-locally by differential equations, and $\Sigma \subseteq X(K)$ is an almost $U(k)$-integral subset, then there is an integer n such that for any $P \in \Sigma \cap \Xi$ one has $d_{v_x}(P, Y) \leq n \cdot \max\{d_{v_x}(P, Z), 1\}$ for $x \in U(k)$.*

■ After a change of co-ordinates, the hypotheses of Lemma 5.3 apply on each affine patch. Since there are only finitely many patches involved, we may take a maximum over the constants calculated on each chart. ■

We can turn now to the proof of the main theorem.

■ Let N be large enough so that each translate of $[p^N]G(K^{sep})$ meets X as does a finite union of translates of group subvarieties. Let Ξ be the finite set of group varieties of Proposition 4.2.

Since the statement is stronger for r larger, we may assume that $r \geq N$.

Let Σ be a set of coset representatives for $\Gamma \cap [p^N]G(K^{sep}))$ in Γ. For $\sigma \in \Sigma$ let $G_1^\sigma, \ldots, G_{n_\sigma}^\sigma \in \Xi$ and $a_1^\sigma, \ldots, a_{n_\sigma}^\sigma \in G(K^{sep})$ such that

$$X(K^{sep}) \cap ([p^N]G(K^{sep}) + \sigma) \quad = \quad [\bigcup_{i=1}^{n_\sigma} a_i^\sigma + G_i^\sigma(K^{sep})] \cap [p^N]G(K^{sep})$$

Extend K so that each $a_i^\sigma + G_i^\sigma$ is defined over K. Since this extension is finite separable, the distance estimates calculated with respect to the extension field imply such estimates for the original K.

Since $\#\Gamma/(\Gamma \cap [p^N]G(K^{sep}))$ is finite, it suffices to show for each $\sigma \in \Sigma$ that there is some $C_r^\sigma \in \mathbb{N}$ such that for any $x \in U(k)$ and any $P \in [([p^N]G(K^{sep}) \cap \Gamma) + \sigma] \setminus [(X(K) \cap \Gamma) + [p^r]G(K^{sep})]$ one has $d_{v_x}(P, X) \leq C_r^\sigma$. We can then set $C_r = \max_{\sigma \in \Sigma} C_r^\sigma$.

By Lemma 5.6, for $P \in \Gamma \cap ([p^N]G(K^{sep}) + \sigma)$, the distance to X is uniformly (in P and in v_x) comparable to the distance to $\bigcup_{i=1}^{n_\sigma} a_i^\sigma + G_i^\sigma$.

It suffices to bound the distance to $a_i^\sigma + G_i^\sigma$.

By Lemma 5.2, for $P \in \Gamma \setminus [a_i^\sigma + G_i(K) + [p^r]G(K^{sep})]$ $\quad d_{v_x}(P, a_i^\sigma + G_i^\sigma)$ is bounded independently of P and x.

Putting this all together, the result follows. ■

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud, Néron Models, Springer-Verlag, Berlin, 1990.

[2] E. Bouscaren, Model theoretic versions of Weil's theorem on pregroups, in Model Theory of Groups (A. Pillay and A. Nesin, editors), University of Notre Dame Press, South Bend, IN, 1989.

[3] A. Buium, The *abc* theorem for abelian varieties, *Internat. Math. Res. Notices* (1994), no 5, 219 ff.

[4] A. Buium and J. F. Voloch, Lang's conjecture in characteristic p: an explicit bound, *Compositio Math.* **103** (1996), no. 1, 1 – 6.

[5] A. Buium and J. F. Voloch, Reduction of the Manin map modulo p, *J. Reine Angew. Math.* **460** (1995), 117-126.

[6] Chang and J. Keisler, *Model Theory*, North-Holland, 3rd ed, 1990.

[7] F. Delon Ideaux et types sur les corps separablement clos, *Mém. Soc. Math. France (N. S.)*, No. 33 (1988), 76 pp.

[8] E. Hrushovski, The Mordell-Lang conjecture for function fields, *J. Amer. Math. Soc.* **9** (1996), no 3, 667-90.

[9] E. Hrushovski, Contributions to stable model theory, Ph. D. thesis, UC Berkeley, 1986.
[10] H. Matsumura Commutative Ring Theory, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, Cambridge, 1986.
[11] M. Messmer, Groups and fields interpretable in separably closed fields, *Trans. Amer. Math. Soc.* **344** (1994), no 1, 361-377.
[12] M. Messmer Some model theory of separably closed fields, in Model Theory of Fields, LNL **5**, Springer, Berlin, 1996.
[13] M. Messmer and C. Wood, Separably closed fields with higher derivations, *JSL* **60** (1995), no 3, 898-910.
[14] T. Scanlon, Model theory of valued D-fields, Ph. D. thesis, Harvard University, May 1997.
[15] L. van den Dries, Weil's group chunk theorem: a topological setting, *Illinois J. Math.* **34** (1990), no. 1, 127 – 139.
[16] J. F. Voloch, Diophantine approximation on abelian varieties in characteristic p, *Amer. J. Math.* **117** (1995), no. 4, 321-5.
[17] C. Wood, Notes on the stability of separably closed fields, *JSL* **44** (1979), 412 – 416.

Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, CA 94709

E-mail address: `scanlon@msri.org`