p-ADIC DISTANCE FROM TORSION POINTS OF SEMI-ABELIAN VARIETIES

THOMAS SCANLON

Abstract. Tate and Voloch have conjectured that the p-adic distance from torsion points of semi-abelian varieties over $\mathbb{C}_p$ to subvarieties may be uniformly bounded. We prove this conjecture for prime-to-p torsion points on semi-abelian varieties over $\mathbb{Q}_p^{alg}$ using methods of algebraic model theory.

Let $\mathbb{C}_p$ denote the completion of the algebraic closure of the p-adic numbers with p-adic valuation v normalized to have $v(p) = 1$. Tate and Voloch proved the following approximation theorem on linear forms in p-adic roots of unity in [14]:

Theorem 0.1 (Tate, Voloch)**.** *Let $(a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbb{C}_p)$. Then there is a constant $N \in \mathbb{Z}$ such that for any sequence $(\zeta_1, \ldots, \zeta_n)$ of roots of unity, either $\sum_{i=1}^n a_i\zeta_i = 0$ or $v(\sum_{i=1}^n a_i\zeta_i) \leq N$.*

They observed that this theorem may be interpreted as a special case of the following conjecture.

Conjecture 0.2 (Tate, Voloch)**.** *Let G be a semi-abelian variety over $\mathbb{C}_p$. Let $X \subseteq G$ be a closed subscheme defined over $\mathbb{C}_p$. There is a constant $N \in \mathbb{Z}$ such that for any torsion point $\zeta \in G(\mathbb{C}_p)_{tor}$ either $\zeta \in X$ or $d(\zeta, X) \leq N$.*

In the above conjecture, "$d(\zeta, X)$" refers to the p-adic distance from P to X which will be defined precisely in Section 1.

In the case that X is a single point, Conjecture 0.2 is a theorem of Mattuck [8]. Other instances of this conjecture have been proved by Buium, Hrushovski, Tate, and Voloch [1, 6, 14, 16]. With the exception of Mattuck's theorem, all previous results require G to have an integral model with good reduction.

We prove Conjecture 0.2 under two restrictions. First, G must be defined over $\mathbb{Q}_p^{alg}$. Secondly, we restrict to torsion points of order prime to p. The first restriction is intrinsic to the particular method used here, but this method should give a proof without the second restriction. We discuss possible strategies for a proof in Section 4.

The main result of this paper is

Theorem 0.3. *Let K be a finite extension of $\mathbb{Q}_p$. Let G be a semi-abelian variety over K. Let $X \subseteq G$ be a closed subvariety of G defined over $\mathbb{C}_p$. There is a constant $N \in \mathbb{Z}$ such that for any prime to p torsion point $\zeta \in G(\mathbb{C}_p)_{p'-tor}$ either $\zeta \in X(\mathbb{C}_p)$ or $d(\zeta, X) \leq r$.*

The results in this paper appear as a chapter in my Ph. D. thesis written under the direction on E. Hrushovski [9]. I thank him and B. Mazur for their advice and suggestions on this topic. I thank also the referee who suggested many improvements in the presentation of this paper.

Date: 21 January 1998.

1991 *Mathematics Subject Classification.* Primary: 11D88; Secondary: 03C60, 11U09.

1. Distance Functions

In this section we give a precise definition of the p-adic distance to a subvariety. For more information on these distance functions consult [15].

Definition 1.1. Let K be a valued field with valuation v and value group vK. Let $X \subseteq \mathbb{A}^N_K$ be a subvariety of affine N-space over K with defining ideal I_X. If $\zeta \in \mathbb{A}^N(K)$, then the v-adic distance from ζ to X is

$$d_v(\zeta, X) \quad := \quad \min\{v(f(\zeta)) : f \in I_X \cap \mathcal{O}_K[x_1, \ldots, x_n]\}$$

If X is a quasi-compact variety over K, $Y \subseteq X$ is a closed subvariety, and $\mathcal{U} := \{(U_i, \varphi_i : U_i \to \mathbb{A}^n)\}$ is a finite affine cover, then for $\zeta \in X(K)$ the v-adic distance from ζ to Y with respect to $\mathcal{U}$ is

$$d^{\mathcal{U}}_v(\zeta, Y) \quad := \quad \min\{d_v(\varphi_i(\zeta), \varphi_i(Y \cap U_i)) : \zeta \in U_i\}$$

When v is the p-adic valuation, we will call this distance function the p-adic distance. We will drop v and $\mathcal{U}$ from the notation because v will be clear from context and a change in $\mathcal{U}$ results in a constant additive change. That is, if $\mathcal{U}$ and $\mathcal{V}$ are two finite affine covers, then there is a constant $C \in vK$ such that $d^{\mathcal{U}}_v(\zeta, Y) \leq d^{\mathcal{V}}_v(\zeta, Y) + C$ for any $\zeta \in X(K)$.

If we work over the ring of integers, then these distance functions have a more geometric definition. As above, let K be a valued field with ring of integer $\mathcal{O}_K$. For each non-negative element of the value group γ let $I_\gamma := \{x \in \mathcal{O}_K : v(x) \geq \gamma\}$. Let $S := \operatorname{Spec} \mathcal{O}_K$, $S_\gamma := \operatorname{Spec} \mathcal{O}_K/I_\gamma$, and $\eta := \operatorname{Spec} K$. If X is a scheme over S, let $X_\gamma := X \times_S S_\gamma$ and let $\pi_\gamma : X(S) \to X_\gamma(S_\gamma)$ be the natural reduction map. If $\zeta \in X(S)$, then define the geometric distance from ζ to Y to be

$$d^g_v(\zeta, Y) \quad := \quad \inf\{\gamma : \pi_\gamma(\zeta) \notin Y_\gamma(S_\gamma)\}$$

The reader may notice that in some circumstances this is not well-defined (for instance, if the ideal sheaf of Y is not finitely presented and the value group is not archimedian, then the infimum need not exist; so, in general it may be better to define the distance as a cut in the value group), but it is well-defined when $K = \mathbb{C}_p$ or when the generic fibre Y_η of Y is dense in Y.

When Y_η is reduced and dense in Y, for any finite affine cover $\mathcal{U}$ of X_η coming from an affine cover of X one has $d^g_v(\zeta, Y) = d^{\mathcal{U}}_v(\zeta, Y_\eta)$ for any point $\zeta \in X(S)$.

2. A More General Formulation

We prove Theorem 0.3 as a special case of a theorem on groups defined by difference equations over valued fields.

In this section K is a general valued field of characteristic zero with valuation v and value group vK. (L, v) denotes an algebraically closed valued field extending (K, v). We will consider a version of Theorem 0.3 for torsion subgroups of semi-abelian varieties over K satisfying certain (seemingly unnatural) conditions which in section 3 we will verify are true in the situation of Theorem 0.3.

Throughout this section G denotes a semi-abelian variety defined over K. We will suppose that there are only finitely many torsion points in $G(K)$

We list this as a hypothesis.

Hypothesis 1. *There are only finitely many torsion points in $G(K)$.*

For K a finite extension of $\mathbb{Q}_p$, this hypothesis is true of any G. For other valued fields ($\mathbb{C}((t))$ for instance) this hypothesis may fail for some G.

If R is a K-algebra and $\sigma : R \to R$ is a K-algebra homomorphism, then σ induces a group homomorphism (which we will continue to denote by σ) $\sigma : G(R) \to G(R)$. Likewise, any power of σ also induces a group homomorphism. If $P(X) \in \mathbb{Z}[X]$ is any polynomial with integer co-efficients, then we may interpret $P(\sigma)$ as a group homomorphism $P(\sigma) : G(R) \to G(R)$. That is, if $P(X) = \sum n_i X^i$, then $P(\sigma)(\zeta) := \sum [n_i]\sigma^i(\zeta)$ where the sum is taken with respect to the group law on G.

Fix now some $P(X) \in \mathbb{Z}[X]$. We assume that P has no cyclotomic factors.

Hypothesis 2. *$P(\zeta) \neq 0$ for all roots of unity $\zeta \in \mathbb{C}$.*

With such a G and P fixed we define functors which assign to a K-algebra R with a specified K-algebra endomorphism certain subgroups of $G(R)$.

Definition 2.1. If R is a K-algebra and $\sigma : R \to R$ is a K-algebra endomorphism, then define:

$$\begin{aligned} \Omega(R,\sigma) &:= \ker G(R) \xrightarrow{P(\sigma)\circ(\sigma-1)} G(R) \\ \Lambda(R,\sigma) &:= \ker G(R) \xrightarrow{P(\sigma)} G(R) \\ \Phi(R,\sigma) &:= \ker G(R) \xrightarrow{\sigma-1} G(R) \end{aligned}$$

These symbols should suggest respectively the universal, locally modular, and fixed field parts. We will observe later that when (R,σ) is an existentially closed difference field extending (K, id), then Ω is the direct sum (up to finite index) of Λ and Φ and that Λ is locally modular. These terms and their importance will be explained in due course.

Let Γ be a torsion subgroup of $G(L)$. In the application to Theorem 0.3 it will be the group of prime-to-p torsion points. To simplify some of our arguments, we will assume that if Γ contains a nontrivial ℓ-torsion point, then it is ℓ-pure inside $G(L)$.

Hypothesis 3. *$\Gamma \subseteq G(L)_{tor}$ is a subgroup of the torsion subgroup of $G(L)$. For any integer n, if $\Gamma \cap G[n](L) \neq 0$, then for any $\zeta \in G(L)$, if $[n]\zeta \in \Gamma$, then $\zeta \in \Gamma$.*

Only certain special automorphisms of L will play a role in the proving distribution properties of Γ. We make the following definition with respect to all the data indicated so far in this section (L, v, G, Γ, and P).

Definition 2.2. An automorphism σ of L is called *good* if

- for every $x \in L^\times$ one has $v(x) = v(\sigma(x))$,
- $\sigma|_K = \mathrm{id}_K$, and
- $\Gamma \subseteq \Omega(L,\sigma)$.

If in addition one has $\Gamma \subseteq \Lambda(L,\sigma)$, then σ is called *very good*.

With these definitions and hypotheses in place we can state the Theorem 2.3, an axiomatic version of Theorem 0.3.

Theorem 2.3. *Let K, L, G, Γ and P be as above. Assume either that there exists a very good automorphism of L or that that the common fixed field of the good automorphisms is K.*

Then for any subvariety $X \subseteq G$ defined over L there is some constant $\gamma \in vL$ such that for any point $\zeta \in \Gamma$ either $\zeta \in X$ or $d(\zeta, X) \leq \gamma$.

Remark 2.4. Theorem 2.3 in the case that a very good automorphism exists is a theorem of Hrushovski [6]. We include this case for the sake of completeness. The

hypotheses in this case may be weakened somewhat. For instance, the hypothesis that there are few torsion points of G over K is unnecessary.

Remark 2.5. Theorem 0.1 may be seen as a consequence of Theorem 2.3. Take $K = \mathbb{Q}_p$ and $L = \mathbb{C}_p$ with the p-adic valuation, $G = \mathbb{G}_m^r$, $\Gamma = \{(\zeta_1, \ldots, \zeta_r) : \zeta_i^n = 1 \text{ for some } n \in \mathbb{Z}_+\}$, and $P(X) = (X - p)(X - \ell)$ where ℓ is some prime different from p. Since the extension of $\mathbb{Q}_p$ given by adjoining all the p-power roots of unity is linearly disjoint over $\mathbb{Q}_p$ from the maximal unramified extension of $\mathbb{Q}_p$, we may find a Frobenius σ which acts as $x \mapsto x^\ell$ on p-power roots of unity and as $x \mapsto x^p$ on prime-to-p roots of unity (as all Frobenii do). Such a σ is *very good* for this situation.

We delay the verification that Theorem 0.3 follows from Theorem 2.3 until Section 3.

For the rest of this section the notation follows that of Theorem 2.3.

2.1. **Bounding the Distance to Cosets.** We will prove Theorem 2.3 by reducing to the case that X is a translate of a semi-abelian subvariety of G. In this subsection we show how to bound the distance from torsion points to cosets.

Lemma 2.6 (Mattuck)**.** *There is a constant $\gamma \in vK$ such that for any torsion point $\zeta \in G(L)_{tor}$ either $\zeta = 0$ or $d(\zeta, 0) < \gamma$.*

Proof: This is a theorem of Mattuck [8] at least in the case that K is a $\mathfrak{p}$-adic field. The proof goes through in general.

For the reader's convenience we sketch the proof.

Replace L with $\mathbf{L}$ a maximal completion. See [10] chapter 2 for a proof that $\mathbf{L}$ exists and is algebraically closed.

By the semi-stable reduction theorem for semi-abelian varieties (Theorem 3.6 of [4]), we may assume that G is the generic fibre of a semi-abelian scheme $\mathfrak{G}$ over $\mathcal{O}_L$.

If ζ does not reduce to zero, then $d(\zeta, 0) = 0$ so we need not worry about ζ.

There is a natural isomorphism $\{x \in \mathfrak{G}(\mathcal{O}_{\mathbf{L}}) : \pi_0(x) = 0\} \cong \widehat{\mathfrak{G}}(\mathfrak{m}_{\mathbf{L}})$ where $\widehat{\mathfrak{G}}$ is the formal group of $\mathfrak{G}$. There is a neighborhood of the origin in $\widehat{\mathfrak{G}}(\mathfrak{m}_{\mathbf{L}})$ on which the formal logarithm of $\widehat{\mathfrak{G}}$ converges to define a homomorphism $\log_{\widehat{\mathfrak{G}}} : \widehat{\mathfrak{G}}(\mathfrak{m}_{\mathbf{L}}) \to \widehat{\mathbb{G}}_a^M(\mathfrak{m}_{\mathbf{L}})$ for some M. Moreover, there is a neighborhood of the identity in $\widehat{\mathbb{G}}_a^M(\mathfrak{m}_{\mathbf{L}})$ on which the formal exponential of $\widehat{\mathfrak{G}}$ is defined and gives an inverse to the logarithm. Thus, a neighborhood of the identity in $\mathfrak{G}$ is isomorphic to a neighborhood of the identity in $\mathbb{G}_a^M$ so that near the origin of G there can be no other torsion points.

Lemma 2.7. *If $a \in G(L)$ is any point then there is a constant $\gamma \in vL$ such that for any torsion point $\zeta \in G(L)_{tor}$ either $\zeta = a$ or $d(\zeta, a) \leq \gamma$.*

Proof: Work again with a semi-abelian model $\mathfrak{G}$ of G over $\mathcal{O}_L$. If a does not extend to an integral point, then $d(a, \zeta) \leq 0$ for any torsion point ζ so we may assume that $a \in \mathfrak{G}(\mathcal{O}_L)$.

Let γ be the bound computed in Lemma 2.6. If ζ and ξ are distinct torsion points and $d(\zeta, a) \geq \gamma$ and $d(\xi, a) \geq \gamma$, then $\pi_\gamma(\zeta) = \pi_\gamma(\xi)$ so that $\pi_\gamma(\zeta - \xi) = 0$. That is, $d(\zeta - \xi, 0) \geq \gamma$ contradicting Lemma 2.6.

Lemma 2.8. *If H is an algebraic subgroup of G defined over L and $a \in G(L)$ is any point, then there is some $\gamma \in vL$ such that $d(\zeta, a+H) \leq \gamma$ for any torsion point $\zeta \in G(L)_{tor} \setminus (a+H)(L)$.*

PROOF: Apply Lemma 2.7 to G/H.

2.2. **Model Theory of Difference Fields.** A difference field is a field M given together with a field endomorphism $\sigma : M \to M$. An existentially closed difference field is called a *transformally closed field*. The class of transformally closed fields is elementary and its theory has been extensively studied by Chatzidakis and Hrushovski [3]. The main results are described in [5] and [2].

In this subsection we draw some consequences of their analysis for the situation at hand. The notation and conventions indicated before the statement of Theorem 2.3 are still in force.

Lemma 2.9 (Hrushovski)**.** *If $(\mathcal{K}, \sigma)$ is a transformally closed field extending (K, id) and V is any subvariety of $G \times G$, then there are varieties $Y_1, \ldots, Y_n$ and $Z_1, \ldots, Z_n$ such that*

1. *$V \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma) = (\bigcup_{i=1}^n Y_i \times Z_i) \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma)$*
2. *each Y_i is a translate of a group subvariety of G.*

PROOF: By Lemma 3.60 of [5] the group $\Lambda(\mathcal{K}, \sigma)$ is locally modular and stably embedded. Hence every definable subset is a Boolean combination of cosets of definable subgroups. By Theorem 5.5 of [3] $\Lambda(\mathcal{K}, \sigma)$ is orthogonal to the fixed field. This implies by Lemma 3.24 of [5] every definable subset of the product $(\Lambda \times \Phi)(\mathcal{K}, \sigma)$ is a Boolean combination of products of definable subsets of $\Lambda(\mathcal{K}, \sigma)$ with definable subsets of $\Phi(\mathcal{K}, \sigma)$. In the statement above $\bigcup_{i=1}^n Y_i \times Z_i$ is the Zariski closure of $V \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma)$.

Lemma 2.10. *In Lemma 2.9, if K' is a subfield of $\mathcal{K}$ closed under σ and σ^{-1} and V is defined over K', then each of the Y_i's and Z_i's are defined over K'^{alg}.*

PROOF: If $\Sigma \subseteq \mathcal{K}$ is any subset, then the algebraic closure of Σ in the model theoretic sense (ie the set of elements of $\mathcal{K}$ which satisfy a formula with parameters from Σ having only finitely many solutions) is equal to the algebraic closure in the sense of field theory of the field generated by $\{\sigma^n(x) : x \in \Sigma, n \in \mathbb{Z}\}$ (see [3] Proposition 1.7). If $\Sigma = K'$ is a field which is already closed under σ and σ^{-1}, then the model theoretic algebraic closure is just K'^{alg}.

Each Y_i and Z_i is algebraic over K' model theoretically and therefore algebraically.

Lemma 2.11. *Let $V \subseteq G \times G$ be a subvariety defined over L. There is a finite set Ξ of subvarieties of V defined over L such that*

1. *If $Y \in \Xi$, then each irreducible component of Y is of the form $W \times Z$ where W is a translate of a group subvariety of G.*
2. *If $(\mathcal{K}, \sigma)$ is a transformally closed field extending (K, id) given with a fixed embedding of L, then for some $Y \in \Xi$ one has $V \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma) = Y \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma)$.*

PROOF: This follows by the compactness theorem of first order logic from Lemmas 2.9 and 2.10.

That is, if there were no uniform choice for Ξ, then the following set of sentences would be consistent.

(1) $(\mathcal{K}, \sigma)$ is a transformally closed field extending (K, id) and is given with a field embedding of L.
(2) $\{\bigwedge_{Y \in \Xi} X \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma) \neq Y \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma) : \Xi$ a finite set of varieties as in the statement of the Lemma $\}$

By the compactness theorem, all of these sentences can be realized simultaneously. This contradicts Lemmas 2.9 and 2.10.

Lemma 2.12. *If $\sigma \in \mathrm{Gal}(L/K)$ is good, then $\Lambda(L, \sigma) + \Phi(L, \sigma) \supseteq \mathbf{\Gamma}$*

PROOF: If $(\mathcal{K}, \sigma)$ is any transformally closed field extending (L, σ), then $|\Omega(\mathcal{K}, \sigma)/[\Lambda(\mathcal{K}, \sigma) + \Phi(\mathcal{K}, \sigma)]|$ is finite (see the proof of Theorem 5.4 of [2]).

Claim 2.13.

$$\Lambda(L, \sigma) + \Phi(L, \sigma) \quad = \quad (\Lambda(\mathcal{K}, \sigma) + \Phi(\mathcal{K}, \sigma)) \cap \Omega(L, \sigma)$$

PROOF OF CLAIM: Since $\Lambda = \ker P(\sigma)$ and $\Phi = \ker(\sigma - 1)$, $\Lambda(\mathcal{K}, \sigma) \cap \Phi(\mathcal{K}, \sigma) \subseteq G[P(1)](\mathrm{Fix}(\sigma))$ which is finite because $P(1) \neq 0$. Thus if $x = a + b$ with $(a, b) \in \Lambda(\mathcal{K}, \sigma) \times \Phi(\mathcal{K}, \sigma))$, then a and b are model-theoretically algebraic over x. By the criterion for algebraicity in transformally closed fields, if $x \in G(L)$, then $a, b \in G(L)$.

Thus the map $\Omega(L, \sigma)/[\Lambda(L, \sigma) + \Phi(L, \sigma)] \longrightarrow \Omega(\mathcal{K}, \sigma)/[\Lambda(\mathcal{K}, \sigma) + \Phi(\mathcal{K}, \sigma)]$ is injective. So $m := |\Omega(L, \sigma)/[\Lambda(L, \sigma) + \Phi(L, \sigma)]| \leq |\Omega(\mathcal{K}, \sigma)/\Lambda(\mathcal{K}, \sigma)| < \infty$.

As σ is good, $\Omega(L, \sigma) \supseteq \mathbf{\Gamma}$. So $\Lambda(L, \sigma) + \Phi(L, \sigma) \supseteq [m]\Omega(L, \sigma) \supseteq [m]\mathbf{\Gamma} = \mathbf{\Gamma}$.

A version of the next lemma appears as Proposition 6.3 of [7] and in a more general form as Proposition 4.2.3 of [9].

Lemma 2.14. *Let $Y, Z \subseteq \mathbb{A}^n_L$ be subvarieties of affine n-space over L. Let σ be an automorphism of L satisfying $v(\sigma(x)) = v(x)$ for any $x \in L^\times$. Let $\mathfrak{D} \subseteq \mathbb{A}^{n(m+1)}_L$ be a subvariety of affine $n(m+1)$-space over L.*

Define $D(L, \sigma) := \{\mathbf{x} \in \mathbb{A}^n_L : (\mathbf{x}, \sigma(\mathbf{x}), \ldots, \sigma^m(\mathbf{x})) \in \mathfrak{D}(L)\}$.

If $Y(\mathcal{K}) \cap D(\mathcal{K}, \sigma) = Z(\mathcal{K}) \cap D(\mathcal{K}, \sigma)$ for any difference field $(\mathcal{K}, \sigma)$ extending (L, σ) then there are constants $n \in \mathbb{Z}_+$ and $\gamma \in vL$ such that $d(\zeta, Y) = n \cdot d(\zeta, Z) + \gamma$ for any $\zeta \in D(L) \cap \mathbb{A}^n(\mathcal{O}_L)$.

PROOF:

If the lemma were false, then for each $n \in \mathbb{N}$ and $\gamma \in vL$ there is a point $\zeta_{(n,\gamma)} \in D(\mathcal{O}_L, \sigma)$ such that $d(\zeta_{(n,\gamma)}, Y) > n \cdot d(\zeta_{(n,\gamma)}, Z) + \gamma$.
Let $\mathcal{F}$ be an ultrafilter on $\mathbb{N} \times vL$ containing $\{[(n, \gamma), \infty) := \{(m, \delta) : m \geq n, \delta \geq \gamma\} : (n, \gamma) \in \mathbb{N} \times vL\}$.
Let $(\mathbf{L}, \mathbf{v})$ be the ultrapower $\prod_{/\mathcal{F}}(L, v)$.
Let ζ be the image of $(\zeta_{(n,\gamma)})$ in $\mathcal{O}_{\mathbf{L}}$.
Let $\delta := d_{\mathbf{v}}(\zeta, Z)$.
Let $\mathfrak{p} := \{x \in R : (\forall (n, \gamma) \in \mathbb{N} \times vL)\ \mathbf{v}(x) > n \cdot \delta + \gamma\}$.

Claim 2.15. $\mathfrak{p}$ *is prime.*

PROOF OF CLAIM: Let $x, y \in \mathcal{O}_{\mathbf{L}} \setminus \mathfrak{p}$. We have $\mathbf{v}(x) \leq n \cdot \delta + \gamma$ and $\mathbf{v}(y) \leq m \cdot \delta + \gamma'$ for some $m, n \in \mathbb{N}$ and $\gamma, \gamma' \in vL$. Thus, $v(xy) \leq (n+m)\xi + (\gamma + \gamma')$ so that $xy \notin \mathfrak{p}$.

The localization of $\mathcal{O}_{\mathbf{L}}$ at $\mathfrak{p}$ is $\mathcal{O}_{\mathbf{L},\mathfrak{p}} = \{x \in \mathbf{L} : (\exists (n, \gamma) \in \mathbb{Z} \times vL)\ v(x) > n \cdot \xi + \gamma\}$. Since $v(\sigma(x)) = v(x)$ for $x \in L$, by Łos' Lemma $\mathbf{v}(x) = \mathbf{v}(\sigma(x))$ on $\mathbf{L}$.

$L^{\times} \hookrightarrow \mathcal{O}_{\mathbf{L},\mathfrak{p}}^{\times}$ via the diagonal map so that composing with the quotient map we obtain a map of difference fields $L \to \mathcal{K} := \mathcal{O}_{\mathbf{L},\mathfrak{p}}/\mathfrak{p}$.

Let ζ continue to denote its image in $D(\mathcal{K}, \sigma)$. By construction, $\zeta \in (Z \cap D)(\mathcal{K}, \sigma) \setminus (Y \cap D)(\mathcal{K}, \sigma)$. This is a contradiction.

Remark 2.16. A direct proof of Lemma 2.14 is hampered by the fact that we have information only about points of $Y \cap D$ over difference fields. If we were to take Y, Z, and $\mathfrak{D}$ to be schemes over $\mathcal{O}_L$ and to assume that $D(R, \sigma) \cap Y(R) = D(R, \sigma) \cap Z(R)$ for any difference ring (R, σ) extending $(\mathcal{O}_L, \sigma)$, then the lemma would be trivial with $n = 1$ and $\gamma = 0$.

Behind the ultraproduct argument is an analysis of the intersections $\mathfrak{D} \cap (Y \times Y^{\sigma} \times \cdots \times Y^{\sigma^m})$ and $\mathfrak{D} \cap (Z \times Z^{\sigma} \times \cdots \times Z^{\sigma^m})$. Our hypothesis does not imply that these two schemes are equal. There may be extraneous and non-reduced components.

Lemma 2.17. *Let $V \subseteq G \times G$ and let Ξ be as in Lemma 2.11. There are constants $n \in \mathbb{N}$ and $\gamma \in vL$ such that for any good σ and $Y \in \Xi$ such that $Y \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma) = V \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma)$ for any difference field $(\mathcal{K}, \sigma)$ extending (L, σ) one has $d(\zeta, V) \leq n \cdot d(\zeta, Y) + \gamma$ for $\zeta \in (\Lambda \times \Phi)(\mathcal{K}, \sigma) \cap (\mathbf{\Gamma} \times \mathbf{\Gamma})$.*

PROOF: Working with respect to a finite affine cover of $G \times G$ coming from a covering of a semi-abelian variety over $\mathcal{O}_L$, we may assume that one each affine patch each element of $\mathbf{\Gamma} \times \mathbf{\Gamma}$ is affine. By Lemma 2.14, for any particular choice of σ on each affine patch the required constants exist. Since the covering is finite, for any particular choice of σ the constants exist (and are valid for any ζ which is integral with respect to each chart). By the compactness theorem, n and γ may be found so as to be valid for all σ.

2.3. **Proof of Theorems.** We now give the proof of Theorem 2.3

PROOF: From Lemmas 2.8, 2.9, and 2.17 the case where a very good automorphism of L exists follows easily. For the rest of this argument we work under the hypothesis that the common fixed field of the good automorphisms is K.

Since with respect to a fixed cover the distance to union is the maximum of the distances to each component, we may assume that X is irreducible.

We prove the theorem by induction on the dimension of X. If $\dim X = 0$, then we are in the situation of Lemma 2.7.

In general, let $\tilde{X} := +^* X := \{(x, y) \in G \times G : x + y \in X\}$. We may choose coverings of G and of $G \times G$ so that $d((x, y), \tilde{X}) = d(x + y, X)$. Let Ξ be the set of subvarieties of $\tilde{X}$ produced by Lemma 2.11 with $V = \tilde{X}$. Let Π and Υ be the sets of irreducible varieties with the property that the irreducible components of elements of Ξ are of the form $W \times Z$ with $W \in \Pi$ and $Z \in \Upsilon$.

Each $W \in \Pi$ is a translate of a group so that by Lemma 2.8 there is some constant $\gamma_W \in vL$ such that if $\zeta \notin W$ is a torsion point, then $d(\zeta, W) \leq \gamma_W$.

By induction, if $Z \in \Upsilon$ and $\dim Z < \dim X$, then there is some constant $\gamma_Z \in vL$ so that any point $\zeta \in \mathbf{\Gamma} \setminus Z$ satisfies $d(\zeta, Z) \leq \gamma_Z$. Let n and γ be the constants produced by Lemma 2.17 so that for any transformally closed field $(\mathcal{K}, \sigma)$ extending (K, id) for which we have $\tilde{X} \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma) = Y \cap (\Lambda \times \Phi)(\mathcal{K}, \sigma)$ for some $Y \in \Xi$, then for $x \in (\Lambda \times \Phi)(L, \sigma) \cap (\mathbf{\Gamma} \times \mathbf{\Gamma})$ the inequality $d(x, \tilde{X}) \leq nd(x, Y) + \gamma$.

Let $\gamma' := \min\{n\gamma_Y + \gamma : Y \in \Pi \text{ or } (Y \in \Upsilon \text{ and } \dim Y < \dim X)\}$ holds.

Let σ be a good automorphism.

By Lemma 2.12, since σ is good, $(\Lambda(L, \sigma) \cap \mathbf{\Gamma}) + (\Psi(L, \sigma) \cap \mathbf{\Gamma}) \supseteq \mathbf{\Gamma}$. So if $\zeta \in \mathbf{\Gamma}$ and $d(\zeta, X)$ is large, there are $a \in \Lambda(L, \sigma) \cap \mathbf{\Gamma}$ and $b \in \Psi(L, \sigma) \cap \mathbf{\Gamma}$ with $a + b = \zeta$ and $d((a, b), \tilde{X})$ large.

Let $Y \in \Xi$ such that $\tilde{X} \cap (\Lambda \times \Phi)(L, \sigma) = Y \cap (\Lambda \times \Phi)(L, \sigma)$. Write $Y = \bigcup_{i=1}^{N} W_i \times Z_i$ with $W_i \in \Pi$ and $Z_i \in \Upsilon$.

By the definition of d

$$\begin{aligned} d((y, z), \bigcup_{i=1}^{n} W_i \times Z_i) &= \max d((y, z), W_i \times Z_i) \\ d((y, z), W_i \times Z_i) &= \min\{d(y, W_i), d(z, Z_i)\} \end{aligned}$$

Thus, if $\zeta \in \mathbf{\Gamma}$ and $d(\zeta, X) > \gamma'$, it must be that for any good σ one can write $\zeta = a + b$ with $(a, b) \in (\Lambda \times \Phi)(L, \sigma) \cap (\Gamma \times \Gamma)$ and

$$\begin{aligned} d(a, W) &> \frac{\gamma' - \gamma}{n} \\ &\text{and} \\ d(b, Z) &> \frac{\gamma' - \gamma}{n} \end{aligned}$$

for some $W \in \Pi$ and $Z \in \Upsilon$.

By the definition of γ', the only way we can have $d(a, W) > \frac{\gamma' - \gamma}{n}$ for a a torsion point is to have $a \in W$. If $\dim Z < \dim X$, then having $d(b, Z) > \frac{\gamma' - \gamma}{n}$ would also violate the definition of γ' unless $b \in Z$. Since $W \times Z \subseteq \tilde{X}$, if $(a, b) \in W \times Z$, then $\zeta = a + b \in X$.

So we must have $a \in W$ and $\dim X = \dim Z$. Since $W \times Z \subseteq \tilde{X}$, we have $W + Z \subseteq X$. Since X is irreducible it must be that $W = a + H$ and $Z = X - a$ where H is the stabilizer of X. Let m be the least common multiple of the orders in G/H of $y + H$ such that $y + H \in \Pi$ and $y \in \mathbf{\Gamma}$. Let $\pi : G \to G/H$ denote the quotient map. We may arrange that $d(\zeta, X) = d(\pi(\zeta), \pi(X))$ for $\zeta \in G(L)$.

Then we have that $\pi([m]\zeta) = \pi([m](a+b)) = \pi([m]b) \in \pi(\Phi(L, \sigma))$. That is, for any choice of a good σ, $\pi([m]\zeta) \in \pi(\Phi(L, \sigma))$. Since the common fixed field of the good σ's is K, $\pi([m]\zeta) \in \pi(G(K))$. Since there are only finitely many torsion points in $G(K)$, there are only finitely many choices for $\pi([m]\zeta)$ and hence for $\zeta + H$.

Let $\delta := \max\{d(\xi, X) : \xi \notin X, \pi([m]\xi) \in \pi(\mathbf{\Gamma} \cap G(K))\} \cup \{\gamma'\}$.

Then $d(\zeta, X) \leq \delta$ for $\zeta \in \mathbf{\Gamma} \setminus X$. This completes the induction.

3. Prime to p Torsion

In this section we prove that Theorem 0.3 follows from Theorem 2.3. The notation follows that of Theorem 0.3.

Fix a semi-abelian model $\mathfrak{G}$ of G over $\mathcal{O}_{\mathbb{Q}_p^{alg}}$. Without loss of generality we may assume that $\mathfrak{G}$ is over $\mathcal{O}_K$. Let $\mathbb{F}_q$ be the residue field of K. Let $\mathrm{Fr}_q \in \mathrm{Gal}(\mathbb{F}_q^{alg}/\mathbb{F}_q)$

be the q-power Frobenius $x \mapsto x^q$. Let Fr_q also denote the endomorphism of $\mathfrak{G}_0$ induced by Fr_q. Let $P(X) \in \mathbb{Z}[X]$ be the minimal polynomial over $\mathbb{Z}$ of Fr_q considered as an element of $\mathrm{End}(\mathfrak{G}_0)$.

Lemma 3.1. *$P(X)$ has no cyclotomic factors.*

Proof: By the Riemann hypothesis for semi-abelian varieties over finite fields, all the roots of P in $\mathbb{C}$ have size q or $\sqrt{q}$.

Definition 3.2. A continuous automorphism $\sigma \in \mathrm{Gal}(\mathbb{C}_p/K)$ is called a Frobenius if for every $x \in \mathcal{O}_{\mathbb{C}_p}$ one has $\sigma(x) = x^q \mod \mathfrak{m}_{\mathbb{C}_p}$.

It is well-known that Frobenii exist and that the common fixed field of the Frobenii is K.

Lemma 3.3. *If H is any semi-abelian variety over K, then $H(K)_{tor}$ is finite.*

Proof: Replacing K with a finite extension can only increase the number of torsion points, so we may assume (via semi-stable reduction) that H is the generic fibre of a semi-abelian scheme $\mathfrak{H}$ over $\mathcal{O}_K$. By Lemma 2.7, there is some γ such that for any two distinct torsion points ζ and ξ one has $d(\zeta, \xi) > \gamma$. Thus, on the torsion points the reduction map $\pi_\gamma : \mathfrak{H}(\mathcal{O}_K) \to \mathfrak{H}_\gamma(\mathcal{O}_K/I_\gamma)$ is injective. Since K is finite over $\mathbb{Q}_p$, the ring $\mathcal{O}_K/I_\gamma$ and hence the set $\mathfrak{H}_\gamma(\mathcal{O}_K/I_\gamma)$ are finite.

Lemma 3.4 (Grothendieck)**.** *Let $n := \mathrm{rk}_{\mathbb{Z}_\ell} T_\ell \mathfrak{G}_\eta - \mathrm{rk}_{\mathbb{Z}_\ell} T_\ell \mathfrak{G}_0$ for any prime $\ell \neq p$. Let $Q \in \mathbb{Z}[X]$ be the minimal polynomial of $\mathrm{Fr}_q^{n!}$ on G_0. If $\sigma \in \mathrm{Gal}(\mathbb{C}_p/K)$ is a Frobenius, then $Q(\sigma^{n!}) \circ (\sigma^{n!} - 1)$ vanishes on $G(\mathcal{O}_{\mathbb{C}_p})_{p'-tor}$.*

Proof: By Corollary 4.4 of [4] for any prime $\ell \neq p$, there is a Galois invariant submodule U of the ℓ-Tate module of $\mathfrak{G}$ which is isomorphic to $T_\ell \mathfrak{G}_0$ as a Galois module (if one identifies the Galois group of the residue field with the group $\mathrm{Gal}(K^{unr}/K)$). Moreover, the Galois group has as eigenvalues $n!$-th roots of unity on $T_\ell G/U$. The result should now be clear.

At this point we replace q with $q^{n!}$ and P with Q.
These lemmas give a proof of Theorem 0.3.

Proof: The above lemmas ensure that the hypotheses of Theorem 2.3 hold.

4. Concluding Remarks

The number theoretic cost of applying Theorem 2.3 comes from verifying the hypotheses. The main challenge in applying Theorem 2.3 to the case of $\mathbf{\Gamma} = G[p^\infty](\mathbb{C}_p)$ is finding good automorphisms. If one restricts for the moment to the considerations of points in the formal group, then one might try to find the equations as a characteristic polynomial of some element of the inertia group acting on the Tate module of the formal group. Theorems of Serre, Tate, and Sen describe the image of this Galois representation (see [13], [12], and [11]) so one might hope to deduce from their results the existence of good automorphisms. One would then like to proceed by an analysis of the monodromy of the Galois representation on the full

Tate module at p to argue that $P(\sigma) \circ (\sigma - 1)$ vanishes on $G[p^\infty]$ for some P with no cyclotomic factors and good σ.

This approach may work in general, but it seems that the current state of knowledge about the Galois representation on the Tate module of the formal group is insufficient. There are cases, however, where this will work. For instance, if the formal group has rank at most one, then it is quite easy to choose a Frobenius which acts on the formal group by multiplication by a rational integer distinct from ± 1. In general, if the maximal abelian quotient of the reduction of G is ordinary, then one can find elements of the inertia group which act on the formal group with characteristic polynomials over $\mathbb{Z}$ having no cyclotomic factors. However, once the p-rank of the reduction surpasses one, it is not clear that the automorphism may be chosen to be a Frobenius.

This brings us to another case which is closer to Conjecture 0.2. To handle the case of $\mathbf{\Gamma} = G(\mathbb{C}_p)_{tor}$ one needs to treat the p-power torsion together with the prime-to-p torsion. Ideally, we would work with Frobenii that also behaved well on the formal group. As mentioned above, even in the cases where one can find automorphisms behaving well on the formal group, it is not so easy to find Frobenii with this property. One could work with the theory of transformally closed fields with respect to several automorphisms instead. Our methods should work in this case, though the translation is not immediate.

References

[1] A. Buium, An approximation property for Teichmüller points, *Math. Res. Lett.* **3** (1996), no. 4, 453 – 457.

[2] Z. Chatzidakis, Groups definable in ACFA, *Proc. NATO-ASI Conf. Model Theory of Fields* (Fields Institute, Toronto), August 1996, (to appear). `http://boole.logique.jussieu.fr/www.zoe/`

[3] Z. Chatzidakis and E. Hrushovski, The model theory of difference fields, preprint Université Paris VII, July 1996. `http://boole.logique.jussieu.fr/www.zoe/`

[4] A. Grothendieck, Modeles de Néron et monodromie, SGA 7_I, exposeé IX.

[5] E. Hrushovski, The model theory of difference fields and the Manin-Mumford conjecture, preprint, 1996.

[6] E. Hrushovski, e-mail to J. F. Voloch, November 1996.

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

[8] A. Mattuck, Abelian varieties over p-adic ground fields, *Ann. of Math. (2)* **62**, (1955), 92 – 119.

[9] T. Scanlon, Model theory of valued D-fields, Ph. D. thesis, Harvard University, May 1997.

[10] Schilling, The Theory of Valuations, AMS Mathematical Survey # 4, 1950.

[11] S. Sen Lie algebras of Galois groups arising from Hodge-Tate modules, *Ann. of Math. (2)* **97** (1973), 160 – 170.

[12] J. P. Serre Groupes algébriques associés aux modules de Hodge-Tate, *Journées de Géométrie Algébrique de Rennes* (Rennes, 1978), Vol III, pp. 155 – 188, Astérisque 65, Soc. Math. France, Paris, 1979.

[13] J. Tate p-divisible groups, *1967 Proc. Conf. Local Fields* (Driebergen, 1966), pp. 158 – 183, Springer, Berlin.

[14] J. Tate and J. F. Voloch, Linear forms in p-adic roots of unity, *Internat. Math. Res. Notices* 1996, no. 12, 589 – 601.

[15] J. F. Voloch, Distance functions on varieties over non-Archimedian local fields, *Rocky Mtn. J. of Math.*, **27**, (1997) no. 2, 453 – 457.

[16] J. F. Voloch, Integrality of torsion points on abelian varieties over p-adic fields, *Math. Res. Lett.* **3** (1996), no. 6, 787 – 791.

Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, CA 94720, USA
E-mail address: scanlon@msri.org