THE CONJECTURE OF TATE AND VOLOCH ON p-ADIC PROXIMITY TO TORSION

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 torsion points on semi-abelian varieties over ${\mathbb{Q}_p}^{alg}$ using methods of algebraic model theory and a result of Sen on Galois representation of Hodge-Tate type.

As a generalization of their theorem on linear forms in p-adic roots of unity, Tate and Voloch conjectured:

Conjecture: (Tate, Voloch) *Let G be a semi-abelian variety over $\mathbb{C}_p$. Let $X \subseteq G$ be a subvariety defined over $\mathbb{C}_p$. Then there is a constant $N \in \mathbb{N}$ such that for any torsion point $\zeta \in G(\mathbb{C}_p)_{\text{tor}}$ either $\zeta \in X$ or $\lambda(\zeta, X) \leq N$.*

In the above statement, $\mathbb{C}_p$ denotes the completion of the algebraic closure of $\mathbb{Q}_p$ and $\lambda(\cdot, X)$ is the p-adic proximity to X function.

In [Sc] this conjecture was proved under the assumptions that G is defined over ${\mathbb{Q}_p}^{alg}$ and that ζ is a torsion point of order prime-to-p. It was suggested that the same method of proof would work without the latter restriction. This suggestion is carried out in this note. The main theorem is the following.

Main Theorem: *Let K be a finite extension of $\mathbb{Q}_p$. Let G be a semi-abelian variety defined over K. Let $X \subseteq G$ be a closed subvariety defined over $\mathbb{C}_p$. There is a constant $N \in \mathbb{N}$ depending only on X such that for any torsion point $\zeta \in G(\mathbb{C}_p)_{\text{tor}}$ either $\zeta \in X$ or $\lambda(\zeta, X) \leq N$.*

In the above statement, $\lambda(\cdot, X)$ is the p-adic proximity to X function. In [Sc], this function was denoted by "$d(\cdot, X)$" and called a "distance function," but to match the notation common in the literature, we revert to "λ" instead of "d."

The proof of the Main Theorem passes through an analysis (due to Sen) of the action of the inertia group on the Tate module of the p-divisible group of G and is completed by combining this argument with the main theorem of [Sc].

Date: 4 February 1999, revised 20 March 1999.

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

Supported by an NSF MSPRF. The research for this paper took place at MSRI during the Spring 1998 Model Theory of Fields program.

I thank B. Mazur for alerting me to Sen's work and J. F. Voloch for discussing this problem with me. I thank MSRI for providing excellent working conditions during my research for this paper.

1. Notation

Our notation is for the most part standard. $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$ equipped with the natural extension of the p-adic valuation, v_p. For K a subfield of $\mathbb{C}_p$. $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K)$ denotes the group of p-adically continuous field automorphisms of $\mathbb{C}_p$ fixing K. Note that for $\sigma \in \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K)$ and $x \in \mathbb{C}_p$ one has $v_p(x) = v_p(\sigma(x))$. $\mathrm{Aut}(\mathbb{C}_p/K)$ denotes the group of all field automorphisms of $\mathbb{C}_p$ fixing K. By K^{unr} we mean the maximal unramified extension of K inside $\mathbb{C}_p$. For H an abelian group and $n \in \mathbb{Z}$ an integer we denote the subgroup of n-torsion by $H[n] := \{h \in H : nh = 0\}$. The torsion subgroup of H is $H_{\mathrm{tor}} := \bigcup_{n=1}^{\infty} H[n]$. For p a prime number, the p-Tate module of H is $T_pH := \varprojlim H[p^n]$ where as usual the maps in the inverse system are given by $p^m : H[p^{n+m}] \to H[p^n]$. T_pH is naturally a $\mathbb{Z}_p$-module and we denote its rank by $\mathrm{rk}_{\mathbb{Z}_p}T_pH$. By $H_{p'-\mathrm{tor}}$ we mean the prime-to-p torsion group of H, $\bigcup_{(n,p)=1} H[n]$. We denote the group of p-power torsion by $H[p^\infty]$.

2. Proof of Main Theorem

In order to prove the main theorem we prove a refined version via induction. The refined version is the following.

Main Theorem: (inductive version) *Let K be a finite extension of $\mathbb{Q}_p$ considered as a subfield of $\mathbb{C}_p$. Let G be a semi-abelian variety over K. Let $\Gamma \leq G(\mathbb{C}_p)_{\mathrm{tor}}$ be a $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})$-submodule of the torsion group of $G(\mathbb{C}_p)$. Let $X \subseteq G$ be a subvariety of G defined over $\mathbb{C}_p$. There is an integer $N \in \mathbb{Z}_+$ such that for any $\zeta \in \Gamma$ either $\zeta \in X(\mathbb{C}_p)$ or $\lambda(\zeta, X) \leq N$.*

The main theorem is an instance of this version by taking $\Gamma = G(\mathbb{C}_p)_{\mathrm{tor}}$ and this version certainly follows from the main theorem. We will prove this refined version by induction on $\mathrm{rk}_{\mathbb{Z}_p}T_p(\Gamma/(\Gamma \cap G(K^{unr}))$ at the end of this section. Before proving this theorem we draw some consequences about the existence of continuous automorphism of $\mathbb{C}_p$ satifying reasonable equations on Γ from a theorem of Sen.

For the reader's convenience we reproduce the statement of the theorem of Sen in the form we use (see Theorem 1 of [Sen] or Théorème 2 of [Ser]).

Fact 2.1 (Sen). *Let K be a complete discretely valued subfield of $\mathbb{C}_p$. Let H be a p-divisible group over K. Let $\rho : \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr}) \to \mathrm{Aut}_{\mathbb{Z}_p}(T_pH(\mathbb{C}_p))$ be the inertial Galois representation associated to H. Then the image of ρ is an open subgroup of the $\mathbb{Q}_p$ points of an algebraic group. Moreover, the Zariski closure of the image of ρ is generated (as an algebraic group) by the $\mathrm{Aut}(\mathbb{C}_p/K)$ conjugates of an algebraic torus defined over $\mathbb{C}_p$.*

Lemma 2.2. *Let G be an algebraic subgroup of GL_n defined over $\mathbb{Q}_p$. Let $H \subseteq G(\mathbb{Q}_p)$ be an open subgroup of the $\mathbb{Q}_p$-points of G. Suppose that G*

contains an algebraic torus of dimension g over $\mathbb{C}_p$. Then there is some $h \in H$ such that

(1) *The characteristic polynomial of h is $P(T)(T-1)^m \in \mathbb{Q}[T]$ where for any root of unity $\zeta \in \mathbb{C}$ the polynomial P does not vanish at ζ and $m \leq n - g$ and*
(2) *h is semi-simple.*

PROOF: G contains a nontrivial maximal torus T defined over $\mathbb{Q}_p$ (See section 34.4 of [Hu]). The dimension of T is at least g as G contains a torus of dimension g over $\mathbb{C}_p$. Since H is open in $G(\mathbb{Q}_p)$, $H \cap T(\mathbb{Q}_p)$ is open in $T(\mathbb{Q}_p)$. Replace H with $H \cap T(\mathbb{Q}_p)$ and work inside T.

Regard the function which assigns to an element of GL_n its characteristic polynomial as a regular function $\psi : \mathrm{GL}_n \to \mathbb{A}^n$. Let C_T be the Zariski closure of $\psi(T(\mathbb{C}_p))$. Since $T(\mathbb{C}_p)$ is conjugate to an algebraic subgroup $\Delta(\mathbb{C}_p)$ of the diagonal subgroup of $\mathrm{GL}_n(\mathbb{C}_p)$ over $\mathbb{C}_p$ and the characteristic polynomial is invariant under conjugation, C_T may also be described as the Zariski closure of $\psi(\Delta(\mathbb{C}_p))$. As $\psi|_\Delta$ is a finite map, the dimension of C_T is that of T.

Δ is defined over $\mathbb{Q}$ as every connected subgroup of the diagonal is defined by character equations. Δ is a rational variety split over $\mathbb{Q}$ as it is defined over $\mathbb{Q}$ and has a point (namely the identity). Visibly, ψ is defined over $\mathbb{Q}$. Hence, $C_T(\mathbb{Q})$ is dense in $C_T(\mathbb{Q}_p)$ in a neighborhood of $\psi(\mathrm{id})$.

The dimension of $T(\mathbb{Q}_p)$ as a p-adic Lie group is equal to its dimension as an algebraic group. Because $\psi|_T$ is a finite map, $\psi(T(\mathbb{Q}_p))$ contains a p-adic manifold of full dimension. In fact, $\psi(T(\mathbb{Q}_p))$ is of full dimension at every point in its image.

Let m be the exponent of $(X-1)$ in the characteristic polynomial of a general element of $T(\mathbb{C}_p)$. Note that $m \leq n - g$. The Zariski closure of the subset of $C_T(\mathbb{Q})$ corresponding to polynomials with rational co-efficients and more than m factors (counting multiplicity) of the form $(X - \zeta)$ for ζ a root of unity is a finite union, Σ, of subsets of co-dimension at least one in C_T. [The key point here is that there are only finitely many roots of unity which may satisfy a polynomial of degree n over $\mathbb{Q}$.] Since $C_T(\mathbb{Q})$ is dense near $\psi(\mathrm{id})$ in $C_T(\mathbb{Q}_p)$, we can find $h \in H$ such that $\psi(h) \in C_T(\mathbb{Q}) \setminus \Sigma(\mathbb{Q})$. $\square$

Lemma 2.3. *Let K be a discretely valued subfield of $\mathbb{C}_p$. Let G be a semi-abelian variety over K. Ler $\Gamma \leq G(\mathbb{C}_p)_{\mathrm{tor}}$ be a $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})$-submodule. Assume that $\mathrm{rk}_{\mathbb{Z}_p} T_p\Gamma/T_p(\Gamma \cap G(K^{unr})) > 0$. Then there is a continuous automorphism $\sigma \in \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})$ and a polynomial $P(T) \in \mathbb{Z}[T]$ with no cyclotomic roots such that*

(1) *$G(\mathrm{Fix}(\sigma)) + \{\zeta \in G(\mathbb{C}_p) : P(\sigma)(\zeta) = 0\} \supseteq \Gamma$ and*
(2) *σ acts non-trivially on $T_p(\Gamma/(G(K^{unr}) \cap \Gamma))$.*

PROOF: The hypothesis that $\Gamma[p^\infty] \subseteq G[p^\infty](\mathbb{C}_p)$ is $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})$ stable implies that there is a p-divisible subgroup H of $G[p^\infty]$ over K^{unr}

such that $H(\mathbb{C}_p)$ is of finite index in $\Gamma[p^\infty]$. Let $\rho : \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr}) \to \mathrm{Aut}_{\mathbb{Z}_p}(T_pH(\mathbb{C}_p))$ be the inertial Galois representation associated to H. The hypothesis that $\mathrm{rk}_{\mathbb{Z}_p} T_p\Gamma/T_p(G(K^{unr}) \cap \Gamma) > 0$ implies that the image of ρ is infinite. By Sen's theorem this implies that the algebraic hull of the image of ρ contains an algebraic torus of positive dimension over $\mathbb{C}_p$. Apply Lemma 2.2 to the algebraic hull of the image of ρ to find some $\tau \in \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})$ with $\rho(\tau)$ having characteristic polynomial $Q(T)(T-1)^m$ on $T_pH(\mathbb{C}_p)$ for $Q(T) \in \mathbb{Q}[T]$ having no cyclotomic factors and $m < \mathrm{rk}_{\mathbb{Z}_p}(T_p(\Gamma/(\Gamma \cap G(K^{unr}))))$. Replace τ by $\sigma := \tau^N$ with $N = \#\Gamma[p^\infty]/H(\mathbb{C}_p)$ so that τ acts trivially on $\Gamma/H(\mathbb{C}_p)$. If $Q(T)$ factors as $\prod(T - \alpha_i)$ over $\mathbb{C}$, then let $\tilde{P}(T) := \prod(T - \alpha_i^N) \in \mathbb{Q}[T]$. Let $P(T) = d\tilde{P}(T) \in \mathbb{Z}[T]$ where d is the least common multiple of the denominators of the co-efficients of $\tilde{P}$. □

Lemma 2.4. *Let $\mathfrak{G}$ be a group and let M be a $\mathfrak{G}$-module. For $s, g \in \mathfrak{G}$ write s^g for $g^{-1}sg$. Let $s \in \mathfrak{G}$. Then $M^{s^{\mathfrak{G}}} := \{x \in M : (\forall g \in G) s^g x = x\}$, the set of elements of M fixed by every conjugate of s, is a $\mathfrak{G}$-submodule of M.*

Proof: Since $\mathfrak{G}$ acts by endomorphisms of M, $M^{s^{\mathfrak{G}}}$ is certainly an abelian group. Let us check that it is closed under the action of $\mathfrak{G}$. Let $h \in \mathfrak{G}$ and $x \in M^{s^{\mathfrak{G}}}$. We need to show that $hx \in M^{s^{\mathfrak{G}}}$. Let $g \in \mathfrak{G}$. Because $x \in M^{s^{\mathfrak{G}}}$, $h^{-1}g^{-1}sghx = s^{gh}x = x$. Act by h on each side of this equation to obtain $s^g hx = hx$. □

With the above lemmas in place we can now prove the Main Theorem in the inductive form.

Proof of Main Theorem: The truth value of the statement of the theorem does not change if for a given G we replace K by a finite extension or we replace G with an isogenous semi-abelian variety. So, we may assume without loss of generality that G is isomorphic over K to a product of extensions of simple abelian varieties by split tori.

We work by induction on $\mathrm{rk}_{\mathbb{Z}_p} T_p(\Gamma/(\Gamma \cap G(K^{unr})))$. When this rank is zero, then after replacing K with a finite extension we have $\Gamma \leq G(K^{unr}) + G(\mathbb{C}_p)_{p'-\mathrm{tor}}$. The theorem we aim to prove is, under the current hypotheses, the main theorem of [Sc]. [The theorem is stated there only for prime-to-p torsion points but all unramified torsion points are contained in the group defined by the Frobenius equation, called $\Lambda(\mathbb{C}_p, \sigma)$ in [Sc] where σ is a relative Frobenius.]

Large chunks of the remainder of this proof are identical to portions of the proof of Theorem 2.3 in [Sc]. That theorem was meant as a template from which the main theorem of this note could be deduced, but it is not quite general enough.

We work by Noetherian induction on X. Since the proximity to a union of two varieties is the maximum of the proximities to each of the varieties separately, we may assume that X is irreducible.

Let $H := \mathrm{Stab}_G^0(X)$ be the connected component of the stabilizer of X in G and let $\pi : G \to G/H$ be the quotient map. We may choose coverings so that for any $x \in G(\mathbb{C}_p)$ we have $\lambda(x, X) = \lambda(\pi(x), \pi(X))$. Since G is split over K, we have $(G/H)(K^{unr}) = \pi(G(K^{unr}))$. Thus, $\mathrm{rk}_{\mathbb{Z}_p} T_p(\pi(\Gamma)/(\pi(\Gamma) \cap (G/H)(K^{unr}))) \leq \mathrm{rk}_{\mathbb{Z}_p} T_p(\Gamma/(G(K^{unr}) \cap \Gamma))$. So, if $\dim H > 0$, by induction we will have a bound on the proximity from points in $\pi(\Gamma)$ not in $\pi(X)$ to $\pi(X)$ which implies the same bound on the proximity from points in Γ not in X to X.

So we may assume now that X has a finite stabilizer in G.

Let $\sigma \in \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})$ and $P(T) \in \mathbb{Z}[T]$ be the field automorphism and integral polynomial produced by Lemma 2.3 for Γ. Let $\Lambda(\mathbb{C}_p, \sigma) := \ker P(\sigma) : G(\mathbb{C}_p) \to G(\mathbb{C}_p)$ and $\Phi(L, \sigma) := \ker(\sigma - 1) : G(\mathbb{C}_p) \to G(\mathbb{C}_p)$. With this notation, the proof of Theorem 2.3 of [Sc] goes through with just a couple of minor changes.

The first change worth remarking occurs in the penultimate multi-line paragraph. Our reduction to the case that X has a finite stabilizer ensures that there is a finite set $A \subseteq \Gamma$ such that if $\zeta \in \Gamma \setminus X(\mathbb{C}_p)$ and $\lambda(\zeta, X) > \gamma'$ (in the notation used there), then for any conjugate τ of σ it is possible to write $\zeta = a + b$ with $a, b \in \Gamma$, $\tau(b) = b$, and $a \in A$. Let m be the least common multiple of the orders of $a \in A$. We conclude that if $\zeta \in \Gamma \setminus X(\mathbb{C}_p)$ and $\lambda(\zeta, X) > \gamma'$, then $[m]\zeta \in \bigcap_{g \in \mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})} \Phi(\mathbb{C}_p, g^{-1}\sigma g) \cap \Gamma = \Gamma^{s^{\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})}} =: \Psi$ which is a proper $\mathrm{Gal}_{\mathrm{cont}}(\mathbb{C}_p/K^{unr})$-submodule of Γ by Lemma 2.4. Since σ acts non-trivially on $T_p(\Gamma/(\Gamma \cap G(K^{unr}))$ we have $\mathrm{rk}_{\mathbb{Z}_p} T_p(\Psi/(G(K^{unr}) \cap \Psi)) = \mathrm{rk}_{\mathbb{Z}_p} T_p(\Psi/(G(K^{unr}) \cap \Gamma)) \leq \mathrm{rk}_{\mathbb{Z}_p} T_p(\Gamma \cap \Phi(\mathbb{C}_p, \sigma)/(G(K^{unr}) \cap \Gamma) < \mathrm{rk}_{\mathbb{Z}_p} T_p(\Gamma/(G(K^{unr}) \cap \Gamma))$. So by induction, there is some $\delta \in \mathbb{Z}$ such that for any $\xi \in [m]^{-1}\Psi \setminus X(\mathbb{C}_p)$ we have $\lambda(\xi, X) \leq \delta$. The bound for Γ is then $\max\{\delta, \gamma'\}$. ✠

References

[Hu] J. Humphreys Linear Algebraic Groups, GTM **21**, Springer-Verlag, New York, 1981.

[Sc] T. Scanlon, p-adic distance from torsion points of semi-abelian varieties, *J. Reine Angew. Math.* **499** (1998), 225 – 236.

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

[Ser] 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.

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

University of California at Berkeley, Department of Mathematics, Evans Hall, Berkeley, CA 94720, USA

E-mail address: `scanlon@math.berkeley.edu`