LOCAL ANDRÉ-OORT CONJECTURE FOR THE UNIVERSAL ABELIAN VARIETY

THOMAS SCANLON

Abstract. We prove a p-adic analogue of the André-Oort conjecture for subvarieties of the universal abelian varieties containing a dense set of special points. Let g and n be integers with $n \geq 3$ and p a prime number not dividing n. Let R be a finite extension of $W[\mathbb{F}_p^{alg}]$, the ring of Witt vectors of the algebraic closure of the field of p elements. The moduli space $\mathcal{A} = \mathcal{A}_{g,1,n}$ of g-dimensional principally polarized abelian varieties with full level n-structure as well as the universal abelian variety $\pi : \mathcal{X} \to \mathcal{A}$ over $\mathcal{A}$ may be defined over R. We call a point $\xi \in \mathcal{X}(R)$ *R-special* if $\mathcal{X}_{\pi(\xi)}$ is a canonical lift and ξ is a torsion point of its fibre. We show that an irreducible subvariety of $\mathcal{X}_R$ containing a dense set of p-special points must be a special subvariety in the sense of mixed Shimura varieties. Our proof employs the model theory of difference fields.

1. Introduction

The André-Oort conjecture in its usual form asserts that if an irreducible subvariety of a Shimura variety contains a Zariski dense set of special points then it must itself be a special variety, that is to say, a component of the image of a Shimura variety under a Hecke correspondence (see [17] and the appendix of [1]). In initially proposing his version of this conjecture, André relaxed the usual definition of "Shimura variety" allowing, for instance, abelian varieties and more generally universal abelian varieties over moduli spaces as ambient varieties (see [18] for a general development of mixed Shimura varieties). The conjecture even with the restriction to pure Shimura varieties, and even restricted to the case that the ambient Shimura variety is the moduli space of principally polarized abelian varieties of dimension g with full level n (which we shall always assume to be at least three) structure, $\mathcal{A}_{g,1,n}$ (which we write as $\mathcal{A}$ when the subscripts are understood), is still open, though important special cases have been proven by many people [2, 7, 8, 9] and Moonen has proven the natural p-adic analogue of the André-Oort conjecture for $\mathcal{A}$ [15]. We formulate and prove the p-adic version of the André-Oort conjecture for the universal abelian variety over $\mathcal{A}$.

The special points on and the special subvarieties of $\mathcal{A}$ may be interpreted in terms of moduli: a special point is nothing other than the moduli

Partially supported by NSF grant DMS-0301771 and an Alfred P. Sloan Fellowship.

point of a CM-abelian variety (with the requisite additional structure) and a special subvariety is a submoduli variety, that is, it represents a submoduli problem given by some constraints on the Hodge structure of the abelian variety. Likewise, the special points on and special subvarieties of the universal abelian variety $\pi : \mathcal{X} \to \mathcal{A}$ over $\mathcal{A}$ may be described in a similar manner. A point $x \in \mathcal{X}(\mathbb{C})$ is special if and only if $\mathcal{X}_{\pi(x)}$ is a CM-abelian variety and x is a torsion point of $\mathcal{X}_{\pi(x)}(\mathbb{C})$. The special subvarieties are, essentially, translates of universal abelian varieties over special subvarieties of $\mathcal{A}$. More precisely, if $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is special, then $\pi Y \subseteq \mathcal{A}_{\mathbb{C}}$ is a special subvariety of the moduli space and for some natural number M, the variety $[M](Y) \subseteq \mathcal{X}_{\mathbb{C}}$ is an abelian subscheme of $\mathcal{X}_{\pi Y}$. As with special subvarieties of Shimura varieties in the traditional sense, there are other characterizations of *special subvariety of* $\mathcal{X}$ in terms of its complex uniformization and preservation under sufficiently many Hecke correspondences.

The universal abelian variety $\pi : \mathcal{X}_{g,1,n} \to \mathcal{A}_{g,1,n}$ is actually over $\mathbb{Z}[\frac{1}{n}]$ so that as long as p is a prime not dividing n, we may regard $\pi : \mathcal{X} \to \mathcal{A}$ via base change as being over $R := W[\mathbb{F}_p^{\mathrm{alg}}]$. For Moonen, the p-adic special points on $\mathcal{A}$ were precisely the R-points corresponding to canonical lifts (of ordinary abelian varieties). For us, the p-adic special points on $\mathcal{X}$, or as we prefer to say, the *R-special points* are the R-points of $\mathcal{X}$ which are torsion on canonical lift fibres. We will have more to say about canonical lifts in the next section. For the moment, we merely note that the key to our proof is an interpretation of *canonical lift* in terms of a difference equation.

The proof presented here uses the model theory of difference fields as developed by Chatzidakis and Hrushovski in [4]. Certainly, the logical formalism is intrinsic to neither the problem nor the proofs, but it provides a coherent framework for the study of difference equations, especially where issues of uniformity intervene.

J. F. Voloch introduced me to this problem in the Spring of 1998 and the general outline of the solution presented here was sketched in conversations with him. I thank Z. Chatzidakis for pointing out that while quantifier elimination fails in ACFA, in some sense, it holds in the limit, and, in particular, in the form needed for the proof presented here. I thank the organizers of the December 2003 meeting on Special Points in Shimura Varieties at the Lorentz Center in Leiden for giving me the opportunity to speak about this material and to learn about the André-Oort conjecture from the experts.

2. Preliminaries

We start by fixing some conventions and notation. Until further notice is given, p is a fixed prime number, $k := \mathbb{F}_p^{\mathrm{alg}}$ is the algebraic closure of the field of p elements, $W[k]$ is the ring of Witt vectors over k and $\sigma : W[k] \to W[k]$ is the Witt-Frobenius. That is, σ is the unique ring endomorphism of R satisfying the congruence $\sigma(x) \equiv x^p \pmod{p}$ universally. We fix an embedding $W[k] \hookrightarrow \mathbb{C}$ of R into the complex numbers and an extension

of σ to an automorphism of $\mathbb{C}$ (which we will continue to call σ) so that $(\mathbb{C}, +, \times, \sigma)$ is an $\aleph_1$-saturated model of ACFA_0 (see [4] for the essentials of the theory of difference closed fields of characteristic zero). We fix as well a finite ramified extension R of $W[k]$ of ramification index e. As the results we aim to prove for R follow from the corresponding results for a finite extension of R, we may, and do, assume that σ preserves R. Note that on R the automorphism σ still satisfies the congruence $\sigma(x) \equiv x^p \mod \mathfrak{m}_R$, though this congruence need not hold modulo p. We normalize the p-adic valuation v on the quotient field of R by $v(p) = 1 \in \mathbb{Z}$ so that the minimal positive valuation of an element of R is $\frac{1}{e}$.

For $g \geq 1$ a positive integer and $n \geq 3$ the moduli space of principally polarized abelian schemes of relative dimension g with full level n structure is a fine moduli space $\mathcal{A}_{g,1,n}$ over $\mathrm{Spec}(\mathbb{Z}[\frac{1}{n}])$ (see Theorem 7.9 and the following remark in [16]). As such, there is a universal abelian variety $\pi : \mathcal{X}_{g,1,n} \to \mathcal{A}_{g,1,n}$ (also over $\mathrm{Spec}(\mathbb{Z}[\frac{1}{n}])$). In what follows, we write $\mathcal{X}$ ($\mathcal{A}$, respectively) for $\mathcal{X}_{g,1,n}$ ($\mathcal{A}_{g,1,n}$, respectively) except on the rare occasions that the subscripts play some rôle. Supposing in addition that p does not divide n, then via base change to R, we may regard $\mathcal{A}_R$ as a moduli space over R and $\pi : \mathcal{X}_R \to \mathcal{A}_R$ as a universal abelian scheme over R. Likewise, via base change over our embedding $R \hookrightarrow \mathbb{C}$, we may regard $\pi : \mathcal{X}_{\mathbb{C}} \to \mathcal{A}_{\mathbb{C}}$ over $\mathbb{C}$. This embedding allows us to treat $\mathcal{X}(R)$ as a subset of $\mathcal{X}(\mathbb{C})$.

We recall the definition of *canonical lift*.

Definition 2.1. Let k' be a perfect field of characteristic p. We write the Witt-Frobenius on $W[k']$ as $\rho : W[k'] \to W[k']$. If A is an abelian scheme over $W[k']$ we say that A is a *canonical lift* if the special fibre $A_{k'}$ is ordinary and there is an isogeny $\psi : A \to A^{\rho}$ whose restriction to the special fibre is the geometric Frobenius morphism $F : A_{k'} \to A_{k'}^{(p)}$.

There are various equivalent formulations of *canonical lift*. For instance, in the case that k' is a subfield of $\mathbb{F}_p^{\mathrm{alg}}$, A being a canonical lift is equivalent to the restriction map $\mathrm{End}(A) \to \mathrm{End}(A_{k'})$ being an isomorphism. (See the appendix of [13]). The only use we have for these equivalences is the observation that if A/R is a canonical lift, then A is a CM-abelian variety.

Definition 2.2. We define a point $\xi \in \mathcal{X}(\mathbb{C})$ to be *special* if the abelian variety $\mathcal{X}_{\pi(\xi)}$ has complex multiplication and ξ is a torsion point of $\mathcal{X}_{\pi(\xi)}(\mathbb{C})$. We say that a point $\xi \in \mathcal{X}(R)$ is *R-special* if it is a torsion point in $\mathcal{X}_{\pi(\xi)}(R)$ and the abelian scheme $\mathcal{X}_{\pi(\xi)}$ is a canonical lift.

Note that via our inclusion $\mathcal{X}(R) \subseteq \mathcal{X}(\mathbb{C})$ every R-special point is special. Moreover, every special point is actually algebraic.

Remark 2.3. It may make more sense to define a point $\xi \in \mathcal{X}(R)$ to be R-special if ξ is a torsion point of $\mathcal{X}_{\pi(\xi)}$ and $\mathcal{X}_{\pi(\xi)}$ is a *quasi-canonical lift*, namely, isogenous to the canonical lift of its special fibre. One might even drop the hypothesis that the special fibre be ordinary and simply define an

R-special point to be an R-valued point of $\mathcal{X}$ which happens to be special. We adopt Definition 2.2 for the technical reason that the hypotheses of Moonen's theorem include the condition that there be a dense set of canonical lifts, rather than quasi-canonical lifts. It is very plausible that the methods employed in [15] generalize to the case of varieties containing a dense set of R-rational moduli points quasicanonical lifts or even that this generalization follows formally from the published theorem. However, at this writing I do not see how to achieve this.

As with pure Shimura varieties, the universal abelian variety $\mathcal{X}_{\mathbb{C}}$ admits a complex analytic uniformization as a double coset space for a real algebraic group. If $\mathfrak{h}_g$ is the Siegel upper half space of symmetric $g \times g$ complex matrices with positive definite imaginary part, then the real symplectic group $\mathrm{Sp}_{2g}(\mathbb{R})$ acts transitively and faithfully on $\mathfrak{h}_g$ via the formula $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \tau := (A\tau + B)(C\tau + D)^{-1}$. It bears remarking that the group of symplectic similitudes, $\mathrm{CSp}_{2g}(\mathbb{R})$, acts on $\mathfrak{h}_g$ via the same formula, but, of course, the action is no longer faithful.

Via the standard embedding $\rho : \mathrm{CSp}_{2g} \hookrightarrow \mathrm{GL}_{2g}$ we have an action of CSp_{2g} on $\mathbb{G}_a^{2g}$ and with respect to this action we may form the semidirect product $G := \mathbb{G}_a^{2g} \rtimes \mathrm{CSp}_{2g}$. The group $G(\mathbb{R})$ acts on $\mathbb{R}^{2g} \times \mathfrak{h}_g$ via $(x;\gamma) \cdot (z;\tau) := (x + \rho(\gamma)(z); \gamma \cdot \tau)$. Real analytically, we may identify $\mathbb{R}^{2g} \times \mathfrak{h}_g$ with $\mathbb{C}^g \times \mathfrak{h}_g$ via $(x_1, \ldots, x_{2g}; \tau_1, \ldots, \tau_g) \mapsto (x_1 + x_{g+1}\tau_1, \ldots, x_g + x_{2g}\tau_g; \vec{\tau})$. Via this identification, the action of $G(\mathbb{R})$ on $\mathbb{C}^g \times \mathfrak{h}_g$ is via complex analytic functions. If $\Gamma_n := \{g \in \mathrm{Sp}_{2g}(\mathbb{Z}) \mid g \equiv \mathrm{Id}_{2g} \pmod{n}\}$, then one may identify $\mathcal{X}(\mathbb{C})$ with $(\mathbb{Z}^{2g} \rtimes \Gamma_n)\backslash(\mathbb{C}^g \times \mathfrak{h}_g)$.

It is sometimes convenient to work with an intermediate analytic covering. Recalling the identification of $\mathbb{R}^{2g} \times \mathfrak{h}_g$ with $\mathbb{C}^g \times \mathfrak{h}_g$, we may see $\mathfrak{X}_g := \mathbb{Z}^{2g}\backslash(\mathbb{C}^g \times \mathfrak{h}_g)$ as $(\mathbb{R}/\mathbb{Z})^{2g} \times \mathfrak{h}_g$ (again, real analytically) and the covering of $\mathcal{X}(\mathbb{C})$ factors through $\nu : \mathfrak{X}_g \to \mathcal{X}$. We write $\widetilde{\pi} : \mathfrak{X}_g \to \mathfrak{h}_g$ for the second projection function. Note that $\widetilde{\pi}$ is holomorphic and descends to the map $\pi : \mathcal{X} \to \mathcal{A}$.

Definition 2.4. We say that an irreducible subvariety $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is *special* if its image in $\mathcal{A}_{\mathbb{C}}$, πY, is a special subvariety (or a "variety of Hodge type") in the sense of [15] and for some positive integer M, the variety $[M](Y)$ is an abelian subscheme of $\mathcal{X}_{\pi Y}$.

Remark 2.5. We adopt Definition 2.4 because amongst the various equivalent definitions of *special subvariety* it fits most closely to our method of proof. One might define a special subvariety to be a component of an image of a mixed Shimura variety under a generalized Hecke correspondence (see [19]). What we call a *special subvariety* would be a *weakly special subvariety* containing a special point in Pink's terminology. Towards the end of our proof, we implicitly use another characterization of special subvarieties, namely, that they are preserved by Hecke correspondences of the form T_{ℓ^m}

(see below for a discussion of the Hecke correspondences on $\mathcal{X}$) for arbitrarily large primes ℓ (and positive integers $m \in \mathbb{Z}_+$, possibly depending on ℓ).

For any positive integer $m \in \mathbb{Z}_+$ the group element γ_m be the analytic automorphism of $\mathbb{C}^g \times \mathfrak{h}_g$ given by $(z;\tau) \mapsto (z;\frac{1}{m}\tau)$ which descends to an algebraic correspondence $\widetilde{T}_m$ on $\mathcal{X}$, and via $\pi : \mathcal{X} \to \mathcal{A}$, to an algebraic correspondence T_m on $\mathcal{A}$. These correspondences have modular interpretations. Recall that via the principal polarization, the Weil pairing $\mathcal{X}_x[m] \times \check{\mathcal{X}}_x[m] \to \mu_m$ may be regarded as a pairing on $\mathcal{X}_x[m]$ itself. The correspondence T_m may be described as follows.

$$\langle x, y\rangle \in T_m(\mathbb{C}) \quad \Leftrightarrow \quad \begin{cases} \exists \psi : \mathcal{X}_x \to \mathcal{X}_y \\ \text{ an isogeny of ppav's with level structure having} \\ \mathcal{X}_x[\psi] \leq \mathcal{X}_x[m] \text{ a maximal isotropic subgroup of } \mathcal{X}_x[m] \end{cases}$$

The isotropy hypothesis on $\mathcal{X}_x[\psi]$ is equivalent to saying that $\#\mathcal{X}_x[m] = m^g$ and the restriction of the Weil pairing to $\mathcal{X}_x[\psi]$ is trivial.

The correspondence $\widetilde{T}_m$ may be expressed via the following identity.

$$\langle x, y\rangle \in \widetilde{T}_m(\mathbb{C}) \quad \Leftrightarrow \quad \begin{cases} \exists \psi : \mathcal{X}_{\pi(x)} \to \mathcal{X}_{\pi(y)} \\ \text{ an isogeny of ppav's with level structure having} \\ \mathcal{X}_{\pi(x)}[\psi] \leq \mathcal{X}_{\pi(x)}[m] \text{ maximal isotropic and } \psi(x) = y \end{cases}$$

Note that if A/R is a canonical lift and $\psi : A \to A^{\sigma^m}$ is an isogeny lifting the Frobenius $F^m : A_k \to A_k^{(p^m)}$, then as the special fibre of $A[\psi]$ is $A_k[F^m]$, $A[\psi]$ is a maximal isotropic subgroup of $A[p^m]$ so that if $x \in \mathcal{A}(R) \subseteq \mathcal{A}(\mathbb{C})$ is a moduli point of A (with some extra structure), then $\langle x, \sigma^m(x)\rangle \in T_{p^m}(\mathbb{C})$.

At this point we may state our main theorem.

Theorem 2.6. *If $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is an irreducible subvariety containing a Zariski dense set of R-special points, then Y is a special subvariety of $\mathcal{X}_{\mathbb{C}}$.*

As a special case of Theorem 2.6, we have the following corollary about sections of families of abelian varieties.

Corollary 2.7. *Let S be a variety over R and $\pi : A \to S$ an abelian scheme over S. Suppose that $f : S \to A$ is a section of π and that the set of points $\xi \in S(R)$ for which A_ξ is a canonical lift and $f(\xi) \in A_\xi(R)$ is torsion is Zariski dense in S. Then f is a torsion section.*

3. Proof of main theorem

As mentioned in the introduction, we prove Theorem 2.6 by converting the problem into a question about difference varieties. For $m \in \mathbb{Z}_+$ a positive integer we define

$$\begin{aligned}\Phi_m &:= \{x \in \mathcal{X}(\mathbb{C}) \mid \langle x, \sigma^m(x)\rangle \in \widetilde{T}_{p^m}(\mathbb{C})\}\\ \Psi_m &:= \{x \in \mathcal{A}(\mathbb{C}) \mid \langle x, \sigma^m(x)\rangle \in T_{p^m}(\mathbb{C})\}\end{aligned}$$

We prove Theorem 2.6 by analyzing sets of the form $Z(\mathbb{C}) \cap \Phi_m$ where $Z \subseteq \mathcal{X}_{\mathbb{C}}$ is a subvariety. The difference varieties Φ_m do not quite contain the R-special points, but they do not miss by much.

We recall a result on bounds on the number of torsion points near zero in an abelian scheme over a p-adic ring.

Proposition 3.1. *Given a prime ℓ and a positive interger r there is a bound $B = B(\ell, r) = \ell^{\lfloor \frac{r}{\ell-1} \rfloor}$ so that if S is a discrete valuation ring of mixed characteristic $(0, \ell)$ of absolute ramification degree at most e and A is an abelian scheme over S, then every torsion point in the kernel of the reduction map $A(S) \to A_{\mathfrak{k}}(\mathfrak{k})$ (where $\mathfrak{k} = S/\mathfrak{m}$ is the residue field) has order dividing B. Indeed, if w is the discrete valuation on S and $I := \{x \in S \mid w(x) > \frac{w(\ell)}{\ell-1}\}$, then reduction map $A(S) \to A(S/I)$ is injective on torsion.*

Proof. Expressing the kernel of reduction in terms of the formal group law of A, this is a slight elaboration of the theorems of Mattuck in [12]. For the details, see Proposition 7 of [5]. □

With Proposition 3.1 in place, we show that the R-special points satisfy a difference equation.

Lemma 3.2. *Let $m \in \mathbb{Z}_+$ be a positive integer and $B := B(p, e)$ be the bound of Theorem 3.1. Set $\widehat{\Phi}_m := \{x \in \mathcal{X}(\mathbb{C}) \mid [B](x) \in \Phi_m\}$. Then $\widehat{\Phi}_m$ contains all the R-special points.*

Proof. Let $\xi \in \mathcal{X}(R)$ be an R-special point. We write X for $\mathcal{X}_{\pi(\xi)}$. Let $\psi : X \to X^\sigma$ be the lifting of the Frobenius $F : X_k \to X_k^{(p)}$ witnessing that X is a canonical lift. Then the isogeny $\vartheta := \psi^{\sigma^{m-1}} \circ \cdots \circ \psi : X \to X^{\sigma^m}$ witnesses that $\pi(x) \in \Psi_m$.

Now, on the R-points, both $\vartheta : \mathcal{X}_{\pi(x)}(R) \to \mathcal{X}^{\sigma^m}_{\pi(x)}(R)$ and $\sigma^m : \mathcal{X}_{\pi(x)}(R) \to \mathcal{X}^{\sigma^m}_{\pi(x)}(R)$ reduce to the Frobenius map $F^m : X \to X^{(p^m)}$. Thus, the image of the group homomorphism $(\vartheta - \sigma^m) : \mathcal{X}_{\pi(x)}(R) \to \mathcal{X}^{\sigma^m}_{\pi(x)}(R)$ is contained in the kernel of reduction. Of course, this map takes torsion to torsion. Hence, by our choice of B, we have $[B](\vartheta - \sigma^m)(\xi) = 0$. That is, $\vartheta([B]\xi) = \sigma^m([B]\xi)$. That is, $[B]\xi \in \Phi_m$ as claimed. □

While there are other points in $\widehat{\Phi}_m$, every algebraic point is special (though not necessarily R-special). For this proof we need a lemma on finite subgroups of abelian varieties.

Lemma 3.3. *Let A be a principally polarized abelian variety over $\mathbb{C}$, $m > 1$ an integer, $\Xi \leq A[m](\mathbb{C})$ a maximal isotropic subgroup of the m torsion on A, and $B \leq A$ an abelian subvariety. Then $B(\mathbb{C}) \cap \Xi$ is nontrivial.*

Proof. Let $\phi : \mathbb{C}^g \to A(\mathbb{C})$ be a complex uniformization of $A(\mathbb{C})$ with kernel Λ. As Ξ is maximal isotropic, via a change of variables of $\mathbb{C}^g$, we may choose a symplectic basis $t_1, \ldots, t_g, \tau_1, \ldots, \tau_g$ for Λ for which t_i is the standard i^{th} unit vector (for each $i \leq g$) and $\phi^{-1}\Xi = \sum_{i=1}^g \mathbb{Z}t_i + \sum_{j=1}^g \mathbb{Z}\frac{\tau_j}{m}$. Let $E : \mathbb{C}^g \to (\mathbb{C}^\times)^g$ be the exponential map $(x_1, \ldots, x_g) \mapsto (\exp(2\pi i x_1), \ldots, \exp(2\pi i x_g))$. Then ϕ factors through E giving a covering $\widetilde{\phi} : (\mathbb{C}^\times)^g \to A(\mathbb{C})$ for which $\widetilde{\phi}^{-1}\Xi$ is the group generated by $(\mu_m)^g$ and $E(\sum_{i=1}^g \mathbb{Z}\tau_i)$. The connected component $\widetilde{B}$ of $\widetilde{\phi}^{-1}(B(\mathbb{C}))$ is an algebraic torus of dimension $g' := \dim B$. As such, $\widetilde{B} \cap \mu_m^g \cong (\mathbb{Z}/m\mathbb{Z})^{g'}$. As $\widetilde{\phi}$ is injective on torsion, $\#(B(\mathbb{C}) \cap \Xi) = m^{g'} > 1$ as claimed. □

Lemma 3.4. *For any positive integer m the set $\widehat{\Phi}_m \cap \mathcal{X}(\mathbb{Q}_p^{\text{alg}})$ consists entirely of special points.*

Proof. If $\xi \in \mathcal{X}(\mathbb{Q}_p^{\text{alg}})$, then for some $s \in \mathbb{Z}_+$ we have $\sigma^s(\xi) = \xi$. Suppose in addition that $\xi \in \widehat{\Phi}_m$. Let $\psi : \mathcal{X}_{\pi(\xi)} \to \mathcal{X}_{\pi(\xi)}^{\sigma^m}$ be an isogeny with $\psi([B]\xi) = \sigma^m([B]\xi)$ witnessing that $\xi \in \widehat{\Phi}_m$. Set $\theta := \psi^{\sigma^{(s-1)m}} \circ \cdots \circ \psi^{\sigma^m} \circ \psi : \mathcal{X}_{\pi(\xi)} \to \mathcal{X}_{\pi(\xi)}^{\sigma^{ms}}$. Then θ witnesses that $\langle \pi(\xi), \pi(\xi) \rangle \in T_{sm}(\mathbb{C})$. Any such point is a CM-moduli point. Moreover, $[B](\theta - 1)(\xi) = 0$. As the kernel of θ is a maximal isotropic subgroup of $\mathcal{X}_{\pi(\xi)}[p^{sm}]$, by Lemma 3.3 the restriction of θ to any abelian subvariety has positive degree. In particular, the map $[B](\theta - 1)$ is an isogeny. Thus, ξ is a torsion point on a CM fibre. That is, ξ is a special point. □

Now that we know that the difference varieties $\widehat{\Phi}_m$ capture the R-special points, we analyze the structure of these difference varieties. We begin with an observation about subgroups of abelian varieties defined by equations of the form $\psi(x) = \sigma^m(x)$ where ψ is an isogeny.

Lemma 3.5. *Let $m \in \mathbb{Z}_+$ be a positive integer, A an abelian variety over $\mathbb{C}$ and $\psi : A \to A^{\sigma^m}$ an isogeny. We suppose that for every abelian subvariety $B \leq A$ the restriction of ψ to B has a nontrivial kernel. Then if $Y \subseteq A$ is an irreducible subvariety for which the set $\{y \in Y(\mathbb{C}) \mid \sigma^m(y) = \psi(y)\}$ is Zariski dense, then Y is a translate of an abelian subvariety of A.*

Proof. This follows from the main dichotomy theorem of [4]. (See Section 4.1 of [11]. For an algebraic proof, see Theorem 2.4 of [20].) □

We may restate Lemma 3.5 for general subvarieties of A.

Corollary 3.6. *With $\psi : A \to A^{\sigma^m}$ as in Lemma 3.5, if $Z \subseteq A$ is any subvariety, then the Zariski closure of the set $\{z \in Z(\mathbb{C}) \mid \sigma^m(z) = \psi(z)\}$ is a finite union of translates of abelian subvarieties of A.*

We return now to the set $\widehat{\Phi}_m$. For each point $a \in \Psi_m$, the fibre $(\widehat{\Phi}_m)_a$ is a finite union of groups commensurable with groups of the form $\{x \in \mathcal{X}_a(\mathbb{C}) \mid \sigma^m(x) = \psi(x)\}$ where ψ ranges amongst the (finitely many) isogenies

$\psi : \mathcal{X}_a \to \mathcal{X}_{\sigma^m(a)}$ with $\mathcal{X}_a[\psi]$ a maximal isotropic subgroup of $\mathcal{X}_a[p^m]$. By Lemma 3.3 all of these isogenies satisfy the hypothesis of Corollary 3.6. Hence, combining this observation with Corollary 3.6 we have the following proposition.

Proposition 3.7. *Let $m \in \mathbb{Z}_+$ be a positive integer and $Y \subseteq \mathcal{X}_{\mathbb{C}}$ any subvariety. Then for any $a \in \mathcal{A}(\mathbb{C})$ the set $Y(\mathbb{C}) \cap (\widehat{\Phi}_m)_a$ is a finite union of cosets of subgroups of $\mathcal{X}_a(\mathbb{C})$.*

We can do better than to say that the intersection $Y(\mathbb{C}) \cap \widehat{\Phi}_m$ is fibrewise a finite union of cosets. It follows on general principles that the degree (with respect to some fixed quasi-projective embedding) of the Zariski closure of $Y(\mathbb{C}) \cap (\widehat{\Phi}_m)_a$ is bounded independently of $a \in \mathcal{A}(\mathbb{C})$. It then follows that the abelian varieties appearing as the stabilizers of the various components of the Zariski closure of $Y(\mathbb{C}) \cap (\widehat{\Phi}_m)_a$ fall into finitely many algebraic families. We approach the issue of describing the Zariski closure of $Y(\mathbb{C}) \cap \widehat{\Phi}_m$ in a different manner.

We recall the definition of the Ueno locus.

Definition 3.8. Let A be an abelian variety over $\mathbb{C}$ and $Y \subseteq A$ a closed subvariety. We define the Ueno locus of Y, $\mathrm{Ueno}(Y)$, by

$$\mathrm{Ueno}(Y)(\mathbb{C}) \quad := \quad \begin{cases} \{y \in Y(\mathbb{C}) \mid \exists B \leq A \\ \text{ an abelian subvariety for which } y + B \subseteq Y\} \end{cases}$$

From its definition, $\mathrm{Ueno}(Y)(\mathbb{C})$ is just a subset of the $\mathbb{C}$-rational points of Y. However, it is actually a closed subvariety of Y. More is true: if Y varies in an algebraic family, then so does $\mathrm{Ueno}(Y)$.

Proposition 3.9. *If $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is a closed subvariety of the universal abelian variety, then there is a closed subvariety $\mathrm{Ueno}(Y) \subseteq Y$ for which $\mathrm{Ueno}(Y)_a = \mathrm{Ueno}(Y_a)$ for all $a \in \mathcal{A}(\mathbb{C})$.*

Proof. That the set $\mathrm{Ueno}(Y)(\mathbb{C}) := \{y \in Y(\mathbb{C}) \mid y \in \mathrm{Ueno}(Y_{\pi(y)})\}$ is constructible and that each fibre of $\mathrm{Ueno}(Y)$ is closed was noted in Lemma 11 of [10]. We claim that $\mathrm{Ueno}(Y)$ itself is actually closed. Write $\mathrm{Ueno}(Y) = \bigcup Z_i \smallsetminus V_i$ where each Z_i is a closed irreducible subvariety of Y and $V_i \subsetneq Z_i$ is a proper closed subvariety. Let $Z = Z_i$ be one of the components of the Zariski closure of $\mathrm{Ueno}(Y)$. Let B be the fibrewise stabilizer of Z. That is, $B(\mathbb{C}) := \{x \in \mathcal{X}(\mathbb{C}) \mid \pi(x) \in \pi(Z) \& x + Z_{\pi(x)} = Z_{\pi(x)}\}$. For a general point $a \in \pi(Z)(\mathbb{C})$ the fibre B_a is a positive dimensional algebraic subgroup of $\mathcal{X}_a$. As B is a closed subvariety of $\mathcal{X}$ and dimension is uppersemicontinuous, it follows that for any $a \in \pi(Z)(\mathbb{C})$ the fibre B_a is a positive dimensional algebraic subgroup of $\mathcal{X}_a$. Thus, for any such a the fibre Z_a is contained in the Ueno locus of Y_a. Thus, $\mathrm{Ueno}(Y)$ is closed. $\square$

So, our finiteness result on intersections of subvarieties of $\mathcal{X}_{\mathbb{C}}$ with $\widehat{\Phi}_m$ can take another form.

Proposition 3.10. *If $m \in \mathbb{Z}_+$ is a positive integer and $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is a closed subvariety, then for all $a \in \Psi_m$ the set $[Y(\mathbb{C}) \smallsetminus \mathrm{Ueno}(Y)(\mathbb{C})] \cap (\widehat{\Phi}_m)_a$ is finite.*

At this point, we interpret Proposition 3.10 in terms of algebraicity in difference fields. Recall that we say that an element b of some $\mathcal{L}$-structure $\mathfrak{M}$ (for some first-order language $\mathcal{L}$) is model theoretically algebraic over the tuple $a = \langle a_1, \ldots, a_n \rangle$ if there is some $\mathcal{L}$-formula $\phi(x; y_1, \ldots, y_n)$ having free variables $x, y_1, \ldots, y_n$ for which $\phi(b; a)$ holds in $\mathfrak{M}$ but there are only finitely many b' from $\mathfrak{M}$ with $\phi(b'; a)$ holding. Proposition 3.10 says that the elements (or, more precisely, their coordinates) of $[Y(\mathbb{C}) \smallsetminus \mathrm{Ueno}(Y)(\mathbb{C})] \cap (\widehat{\Phi}_m)_a$ are model theoretically algebraic over a in $\mathcal{L}(+, \times, \sigma^m, \vec{c})$ where $\vec{c}$ is a sequence of generators for a field of definition of Y. Recall (see Proposition 1.7 of [4]) that in an existentially closed difference field, the model theoretic algebraic closure of a set is the usual algebraic closure of the inversive difference field generated by that set. If $a \in \Psi_m$, then $\sigma^m(a)$ and $\sigma^{-m}(a)$ are algebraic over a (as $\langle a, \sigma^m(a) \rangle \in T_{p^m}(\mathbb{C})$ so that $\langle \sigma^{-m}(a), a \rangle \in T_{p^m}(\mathbb{C})$ as well). Thus, in this case, being model theoretically algebraic over a is the same as being algebraic in the usual sense. The upshot of these observations is the following lemma.

Lemma 3.11. *Let $Y \subseteq \mathcal{X}_{\mathbb{C}}$ be a closed subvariety and $m \in \mathbb{Z}_+$ a positive integer. Then there is a closed subvariety $Z \subseteq Y$ each component of which is generically finite over its image in $\mathcal{A}_{\mathbb{C}}$ for which $Y(\mathbb{C}) \cap \widehat{\Phi}_m \subseteq \mathrm{Ueno}(Y)(\mathbb{C}) \cup Z(\mathbb{C})$.*

Proof. It suffices to work in a local affine chart $U \subseteq \mathcal{X}_{\mathbb{C}}$ and show that such a $Z \subseteq Y \cap U$ exists. Choose coordinates so that $U \subseteq \mathbb{A}^s \times \mathbb{A}^t$ with $\pi \restriction U$ being given by the projection onto the first s coordinates. By the above observations, for each $a \in \Psi_m \cap \pi U(\mathbb{C})$ there are polynomials $f_1(x_1, y_1, \ldots, y_s), \ldots, f_t(x_t, y_1, \ldots, y_s) \in \mathbb{Z}[x, y]$ so that $f_j(x; a) \not\equiv 0$ (for all $j \leq t$) and for any $b = \langle a; b_1, \ldots, b_t \rangle \in \widehat{\Phi}_m \cap Y(\mathbb{C})$ we have $f_j(b_j; a) = 0$ (for all $j \leq t$). Applying $\aleph_1$-compactness of $(\mathbb{C}, \sigma)$ and taking products, we see that one may choose the polynomials f_j independently from a. Let $Z := Y \cap V(f_1(x_1, y), \ldots, f_t(x_t, y))$. $\square$

Lemma 3.11 permits us to presume that if $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is an irreducible subvariety containing a Zariski dense set of R-special points, then either $\pi \restriction Y$ is generically finite or Y has a nontrivial Ueno fibration. With the next lemma we note that in the latter situation one may pass to a quotient thereby reducing to the former case.

Lemma 3.12. *Suppose $Y \subseteq (\mathcal{X}_{g,1,n})_{\mathbb{C}}$ is a counter-example to Theorem 2.6. That is, Y is a non-special irreducible subvariety containing a Zariski dense set of R-special points. Then there is a counter-example $Z \subseteq (\mathcal{X}_{g',1,n})_{\mathbb{C}}$ with $\dim Z \leq \dim Y$ and $\pi \restriction Z$ generically finite.*

Proof. By Lemma 3.11, if this lemma is not already true with $Z = Y$, then $Y = \mathrm{Ueno}(Y)$. As $\pi : \mathcal{X} \to \mathcal{A}$ is proper, $\pi Y \subseteq \mathcal{A}$ is a closed subvariety. Let $B := \mathrm{Stab}_{\mathcal{X}_{\pi Y}}(Y)^0$ be the connected component of the stabilizer of Y. Then $B \leq \mathcal{X}_{\pi Y}$ is an abelian subscheme of $\mathcal{X}_{\pi Y}$ of relative dimension $d > 0$. One would like to take Z to be the quotient of Y by B. Unfortunately, while for every $a \in \pi Y(\mathbb{C})$ the abelian variety $\mathcal{X}_a$ is principally polarized, the quotient $\mathcal{X}_a/B_a$ need not be principally polarized. However, it does inherit a polarization from $\mathcal{X}_a$ so that using Zahrin's trick (see, for instance, Remark 16.12 of [14]) we may regard it as an abelian subvariety of a principally polarized abelian variety of dimension $g' := 8(g-d)$. Let $\psi : Y \to (\mathcal{X}_{g',1,n})_{\mathbb{C}}$ be the map given by the quotient modulo B followed by the inclusion given by Zahrin's trick. Let Z be the image of Y under ψ.

As Y contains a Zariski dense set of R-special points, it is defined over R. Thus, B is also defined over Y. It follows that ψ is defined over R. Thus, the R-special points in Y are taken to R-special points in Z and are therefore dense in Z. Visibly, Z has a fibrewise finite stabilizer. By Lemma 3.11, $\pi \restriction Z$ is generically finite. □

So, the last interesting case to consider is that of $Y \subseteq \mathcal{X}_{\mathbb{C}}$ irreducible, containing a Zariski dense set of R-special points, and $\pi \restriction Y$ generically finite. With our next two lemmata we finish our analysis of this case and thereby conclude the proof of Theorem 2.6.

Recall that for an algebraic variety W over $\mathbb{C}$ one may define the σ-Zariski topology on $W(\mathbb{C})$ by taking the closed sets to be those defined locally by the vanishing of difference polynomials. Recall that this topology is Noetherian. (See Theorem 3.8.5 of [6].)

Lemma 3.13. *If there is a counter-example $Y \subseteq \mathcal{X}_{\mathbb{C}}$ to Theorem 2.6, with $\pi \restriction Y$ generically finite, then there is such a counter-example with $Y(\mathbb{C}) \cap \widehat{\Phi}_1$ irreducible in the σ-Zariski topology.*

Proof. Let $Y \subseteq \mathcal{X}_{\mathbb{C}}$ be a potential counter-example to Theorem 2.6. As the σ-Zariski topology on Y is Noetherian, we may write $Y(\mathbb{C}) \cap \widehat{\Phi}_1$ as a finite union $\bigcup_{i=1}^m Y_i$ of σ-irreducible difference varieties. For N sufficiently large, we may write each Y_i as

$$Y_i := \{x \in \mathcal{X}_{\mathbb{C}}(\mathbb{C}) \mid \langle x, \sigma(x), \ldots, \sigma^N(x)\rangle \in Z_i(\mathbb{C})\}$$

where $Z_i \subseteq \mathcal{X}_{\mathbb{C}} \times \mathcal{X}_{\mathbb{C}}^{\sigma} \times \cdots \times \mathcal{X}_{\mathbb{C}}^{\sigma^N}$ is an irreducible variety. Passing to a subvariety if need be, we may assume that $\{\langle x, \sigma(x), \ldots, \sigma^N(x)\rangle \mid x \in Y_i\}$ is Zariski dense in Z_i.

Since $\mathcal{X}$ is defined over the fixed field of σ, we see that $\mathcal{X}^{\sigma^i} = \mathcal{X}$ for any i. Moreover, by identifying the $(N+1)$-tuple of abelian varieties encoded by an element of $\mathcal{X}^{N+1}$ with their product, we may regard $(\mathcal{X}_{g,1,n})^{N+1}$ as a subscheme of $\mathcal{X}_{(N+1)g,1,n}$.

As for each $a \in \widehat{\Phi}_1$ the elements $\sigma^i(a)$ are algebraic over a, it follows that via the natural projection map $\rho : \mathcal{X}^{N+1} \to \mathcal{X}$ that each Z_i is generically

finite over Y. Moreover, because Y is irreducible, the map $\rho \restriction Z_i : Z_i \to Y$ is dominant.

The function $x \mapsto \langle x, \sigma(x), \ldots, \sigma^N(x)\rangle$ takes R-special points to R-special points. It follows that for at least one $i \leq m$ that the R-special points are dense in Z_i. Fix one such and set $Z := Z_i$.

Now, if Z were special, then Y would be special as well for πY would be the image of the special variety πZ under a map of Shimura varieties and on fibres ρ is a map of group varieties so that it would take the torsion variety Z to a torsion variety. Thus, if Y is a counter-example to Theorem 2.6, so is Z. □

The key observation in the next lemma was pointed out to the author by Z. Chatzidakis.

Lemma 3.14. *If $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is a subvariety containing a Zariski dense set of R-special points, for which the restriction of π to Y is generically finite, and $Y(\mathbb{C}) \cap \widehat{\Phi}_1$ is σ-irreducible, then there is a Zariski open and dense set $U \subseteq \pi Y$ so that for every R-special point $\xi \in U(\mathbb{C})$ the fibre $Y_\xi(\mathbb{C})$ consists entirely of torsion points.*

Proof. Let $d := \deg(\pi \restriction Y)$ be the generic degree of π restricted to Y and set $m := d!$. Let $K \subseteq \mathbb{C}$ be a countable algebraically closed inversive difference field over which Y is defined. As Y contains a dense set of algebraic points, we could take $K = \mathbb{Q}^{\mathrm{alg}}$. Let $a \in Y(\mathbb{C}) \cap \widehat{\Phi}_1$ be a Weil-generic point. That is, the transcendence degree of $K(a)$ over K is equal to $\dim Y$. Such a point exists by $\aleph_1$-saturation. Set $a' := \pi(a) \in (\pi Y)(\mathbb{C}) \cap \Psi_1$. Let $b \in (\pi Y)(\mathbb{C}) \cap \Psi_1$ be any generic point and $c \in Y_b(\mathbb{C})$ any point in the fibre above b in Y. It suffices to show that $c \in \widehat{\Phi}_m$. Indeed, the set $\{x \in (\pi Y)(\mathbb{C}) \cap \Psi_1 \mid Y_x(\mathbb{C}) \subseteq \widehat{\Phi}_m\}$ is definable. So, if it contains all generic points, then it contains a (relatively) Zariski open and dense set.

As $Y(\mathbb{C}) \cap \widehat{\Phi}_1$ is σ-irreducible, so is $(\pi Y)(\mathbb{C}) \cap \Psi_1$. Thus, the difference fields $L := K\langle a'\rangle_\sigma$ and $L' := K\langle b\rangle_\sigma$ are isomorphic over K via an isomorphism ρ taking a' to b. Now, as Y is an irreducible variety, the *fields* $L(a)$ and $L'(c)$ are isomorphic over ρ via $a \mapsto c$. We extend this map to $L(a)^{\mathrm{alg}} = L^{\mathrm{alg}}$ and call the extension $\widetilde{\rho}$.

As $[L(a) : L] = d$, the normalization M of this extension has degree dividing $d! = m$ over L. Of course, the normalization M' of $L'(c)$ over L' is isomorphic to M via $\widetilde{\rho}$. The group generated by σ in $\mathrm{Aut}(L^{\mathrm{alg}})$ (respectively, $\mathrm{Aut}((L')^{\mathrm{alg}})$) acts on $\mathrm{Gal}(M/L)$ (respectively, $\mathrm{Gal}(M'/L')$) by conjugation. As the order of $\mathrm{Gal}(M/L)(\textit{respectively}, \mathrm{Gal}(M'/L'))$ divides m, we see that σ^m acts trivially. In particular, on M, $\widetilde{\rho}$ and σ^m commute.

Now, $a \in \widehat{\Phi}_m$ meaning that $\langle [B]a, [B]\sigma^m(a)\rangle \in \widetilde{T}_{p^m}(\mathbb{C})$. So that,

$$\begin{aligned}\widetilde{T}_{p^m}(\mathbb{C}) &\ni \widetilde{\rho}(\langle [B]a, [B]\sigma^m(a)\rangle)\\ &= \langle [B]\widetilde{\rho}(a), [B]\widetilde{\rho}(\sigma^m(a))\rangle\\ &= \langle [B]\widetilde{\rho}(a), [B]\sigma^m(\widetilde{\rho}(a))\rangle\\ &= \langle [B]c, [B]\sigma^m(c)\rangle\end{aligned}$$

That is, $c \in \widehat{\Phi}_m$ as claimed.

Therefore, for every generic $b \in (\pi Y)(\mathbb{C}) \cap \Psi_1$ we have $Y_b(\mathbb{C}) \subseteq \widehat{\Phi}_m$. By compactness, there is a Zariski dense and open $U \subseteq \pi Y$ so that $Y_b(\mathbb{C}) \subseteq \widehat{\Phi}_m$ for all $b \in U(\mathbb{C}) \cap \Psi_1$. By Lemma 3.4, if $\xi \in U(\mathbb{C}) \cap \Psi_1$ is special, then every algebraic point in $(\widehat{\Phi}_m)_\xi$ is special. As $Y_\xi(\mathbb{C}) \subseteq (\widehat{\Phi}_m)_\xi$, we have that $Y_\xi(\mathbb{C})$ consists entirely of torsion points. □

With all of the above ingredients in place, we conclude the proof Theorem 2.6.

Proof. By Lemma 3.14 we may reduce to the case that $Y \subseteq \mathcal{X}$ is an irreducible subvariety containing a dense set of R-special points, with the restriction of π to Y being generically finite and for which there is a Zariski open and dense set $U \subseteq \pi Y$ having the property that $Y_a(\mathbb{C})$ consists entirely of torsion points for all special points $a \in (\pi Y)(\mathbb{C}) \cap \Psi_1$.

As $\pi : \mathcal{X} \to \mathcal{A}$ is proper, the constructible set πY is a closed subvariety of $\mathcal{A}$. As the R-special points are dense in Y, they are also dense in πY. By the main theorem of [15], the variety πY is a special subvariety of $\mathcal{A}$. As πY is special, for arbitrarily large primes ℓ there are discrete valuation rings $S \subseteq \mathbb{Q}^{\mathrm{alg}}$ of residue characteristic ℓ with the set

$$C_{S,\ell,p} := \{\zeta \in U(S) \cap U(R) \mid \zeta \text{ is canonical at } p \text{ and at } \ell\}$$

being Zariski dense in $\pi(Y)$ (see Corollary 3.8 of [15]). If ℓ is sufficiently large, then $\pi \restriction Y : Y \to \pi Y$ is (generically) unramified at ℓ, say, over the Zariski open and dense set $V \subseteq \pi Y$. Hence, for $\zeta \in C_{S,\ell,p} \cap V(S)$ the fibre $Y_\zeta(\mathbb{C})$ consists entirely of ℓ-unramified torsion points. Therefore, Y contains a Zariski dense set of S-special points and is, thus, fixed by the Hecke correspondence $\widetilde{T}_{\ell^m}$ for some positive integer m. If $\mathfrak{Y} \subseteq \mathfrak{X}_g$ is a component of $\nu^{-1}(Y(\mathbb{C}))$, then $\epsilon := \gamma_{\ell^m}\delta$ fixes $\mathfrak{Y}$ setwise for some $\delta \in \Gamma_n$. Taking ℓ sufficiently large, by Theorem 6.1 of [9] each orbit of ϵ on $\widetilde{\pi}(\mathfrak{Y})$ is dense. Consequently, $\mathfrak{Y}$ is a homogenous space for its stabilizer.

Let $y \in Y(\mathbb{C})$ be a special point and $\tilde{y} \in \mathfrak{Y}$ a lifting. Let $z \in Y(\mathbb{C})$ be any other point and $\tilde{z} \in \mathfrak{Y}$ a lifting. Using the real analytic trivialization of $\mathfrak{X}_g$, write $\tilde{y} = (x_y; \tau_y)$ and $\tilde{z} = (x_z; \tau_z)$. As y is special, x_y is a torsion point, say, of order $N \in \mathbb{Z}_+$. As $\mathfrak{Y}$ is a homogenous space, there is some γ in its stabilizer with $\gamma\tilde{y} = \tilde{z}$. Fibrewise, the action on $(\mathbb{R}/\mathbb{Z})^{2g}$ is via group homomorphisms. Hence, x_z is also an N-torsion. Therefore, Y is a component of $\mathcal{X}_{\pi Y}[N]$ and is, in particular, a special variety. □

4. Refinements of the method

Our method of proof for Theorem 2.6 generalizes in several ways. Firstly, using the model theory of valued difference fields, one can transfer Theorem 2.6 to include the case of R-special points where the residue field of R is an arbitrary algebraically closed field of characteristic p. Secondly, the general theory of difference equations produces explicit (albeit enormous) bounds on the degree of the Zariski closure of solutions to difference equations in terms of geometric data describing the equations. Thirdly, these methods apply to more general mixed Shimura varieties, universal semiabelian varieties, for instance.

We explain these generalizations in less detail as we proceed. That is, we give complete statements and proofs for the generalization to arbitrary residue fields. In the case of the explicit degree bounds, we compute the bounds relative to certain geometric degree computations. We confine ourselves to the following comment about the more general mixed Shimura varieties. While it is clear that these methods are germane to the study of p-adic special points on the universal semiabelian variety, we lack a proven description of the subvarieties of the base moduli space which contain a dense set of p-adic special points.

4.1. **Transcendental special points.** For the time being, k' is an algebraically closed field of characteristic p and R' is a finite extension (of ramification index e) of the Witt vecotrs $W[k']$. We let $\sigma : W[k'] \to W[k']$ be the relative Frobenius on the Witt vectors and we assume that σ extends to an automorphism (which we continue to denote by σ) of R. We may, and do, express R' as $W[k'][x]/(P)$ where $P \in \mathbb{Z}[x]$ is a polynomial over the integers. As before, let $k = \mathbb{F}_p^{\mathrm{alg}}$ and set $R := W[k][x]/(P)$. We write K for the field of fractions of R and K' for the field of fractions of R'. We write v' for the valuation on K' and v for the valuation on K. As before, these valuations are normalized so that $v(p) = v'(p) = 1$.

Definition 2.2 generalizes immediately to a give a notion of R'-special point. A point $\xi \in \mathcal{X}(R')$ is *R'-special* if $\mathcal{X}_{\pi(\xi)}$ is a canonical lift and ξ is a torsion point of $\mathcal{X}_{\pi(\xi)}(R)$. Definition 2.4 also generalizes immediately to R', but the analogue of Theorem 2.6 would be false with this immediate generalization. Rather, we say that an irreducible subvariety $Y \subseteq \mathcal{X}_{K'}$ is R'-special if $Y(K')$ contains an R'-special point, $\pi Y \subseteq \mathcal{A}_{K'}$ is a totally geodesic subvariety in the sense of [15] and $[M](Y)$ is an abelian subscheme of $\mathcal{X}_{\pi Y}$ for some positive integer M. Equivalently, an R'-special variety is a weakly special subvariety in the sense of [19] which contains an R'-special point.

With these definitions in place we may state the R'-version of Theorem 2.6.

Theorem 4.1. *If $Y \subseteq \mathcal{X}_{K'}$ is an irreducible subvariety of $\mathcal{X}_{K'}$ containing a Zariski dense set of R'-special points, then Y is an R'-special subvariety.*

Remark 4.2. Proposition 6.4 of [15] may be seen as the special case of Theorem 4.1 where Y is defined over K and is equal to $\pi^{-1}(\pi Y)$.

The key step in our proof of Theorem 4.1 is the fact that the extension of valued difference fields, $(K, +, \times, v, \sigma) \hookrightarrow (K', +, \times, v', \sigma)$ is elementary in the sense of mathematical logic (see Corollary 10.4 of [23] or [3]). On the face of it, Theorem 2.6 is not first-order expressible, but we shall show that a failure of Theorem 4.1 may be converted to a failure of Theorem 2.6.

Lemma 4.3. *There is a formula ϕ in the language of valued difference fields for which the set of realizations of ϕ in $W[k'][\frac{1}{p}]$ is exactly the set of R'-special points in $\mathcal{X}(K')$. [NB: This includes the case of $k' = k$.]*

Proof. Strictly speaking, first-order formulae do not take points on quasi-projective schemes as arguments, but through the usual encoding tricks we may regard $\mathcal{X}(R')$ together with the reduction map $\mathcal{X}(R') \to \mathcal{X}(k')$ as part of the first-order structure.

More precisely, the ring $W[k']$ is definable in $W[k'][\frac{1}{p}]$ as the set of elements of nonnegative valuation. Using the presentation R' as $W[k'][\frac{1}{p}][x]/(P)$, we may regard any element of R' as a $d = \deg(P)$-tuple of elements of $W[k']$ and the product and sum operations on R' may be expressed in terms of these coordinates. Moreover, one may indentify those elements of R' which actually lie in $W[k]$ as those d-tuples whose last $d-1$ coordinates are all zero. The set of R'-rational points of N-dimensional projective space may be expressed as the set of $(N+1)$-tuples of elements of R' not all of which have positive valuation modulo the definable equivalence relation $x \sim y \Leftrightarrow (\exists\lambda)[v(\lambda) = 0 \ \& \ \lambda x = y]$. Using the above interpretation of R' in $W[k']$, this may be understood as a definable set of $d(N+1)$-tuples of elements of $W[k']$ modulo a definable equivalence relation. Fixing a presentation of $\mathcal{X}$ as a quasiprojective scheme over $\mathbb{Z}[\frac{1}{n}]$, we may express the condition that (the equivalence class of the $d(N+1)$-tuple of elements of $W[k]$ representing) y is an element of $\mathcal{X}(R')$ in terms of the equations and inequations defining $\mathcal{X}$. Likewise, the reduction map may be expressed in terms of the standard interpretable reduction map on R'. With these niceties in place, we work with variables ranging over $\mathcal{X}(R')$ and speak about the reduction map as if they are part of the first-order structure.

Let $\mathcal{A}'$ be the moduli space of g-dimensional principally polarized abelian varieties with full level n structure and a choice of a maximal isotropic subgroup of the p-torsion. There is a map $\vartheta : \mathcal{A}' \to \mathcal{A}$ which takes the moduli point of the quadruple $(A, \lambda, \alpha, \Gamma)$ consisting of an abelian variety A, a polarization λ, level n-structure α, and the maximal isotropic group of p-torsion Γ to the moduli point of A/Γ with the induced polarization and level structure. Over $\mathbb{Q}$, these are fine moduli spaces and the map ϑ lifts to a map on the universal abelian varieties $\widetilde{\vartheta} : (\mathcal{X}')_{\mathbb{Q}} \to \mathcal{X}_{\mathbb{Q}}$ which on the fibre over $[(A, \lambda, \alpha, \Gamma)]$ is the quotient homomorphism $A \to A/\Gamma$.

Let $\varpi : \mathcal{X}'_{\mathbb{Q}} \to \mathcal{X}_{\mathbb{Q}}$ be the natural projection map which forgets the choice of a p-torsion group. If $\varpi(x) = y$, then we can consider x as (y, Γ) where Γ is the p-torsion group encoded by x. We write this Γ as Γ_x.

Let $B = B(p, e)$ be the bound of Lemma 3.1. Let $\phi(x)$ be the formula which asserts that $\pi(x) \in \mathcal{A}(W[k'])$ and that there exists a point $\widetilde{x} \in \mathcal{X}'(K')$ so that

- $\varpi(\widetilde{x}) = x$
- $\sigma([B]x) = \widetilde{\vartheta}([B]\widetilde{x})$
- $\Gamma_{\widetilde{x}} \leq \mathcal{X}_{\pi(x)}(W[k'])$ and the reduction map on $\Gamma_{\widetilde{x}}$ is injective.

If $\phi(a)$ holds as witnessed by $\widetilde{x} = (a, \Gamma)$, then by the third condition the map $\widetilde{\vartheta}_{\pi(a)} : \mathcal{X}_{\pi(a)} \to \mathcal{X}_{\pi(\vartheta(\pi(a))}$ lifts the Frobenius and the special fibre is ordinary. By the second condition, the codomain of this map is actually $\mathcal{X}^{\sigma}_{\pi(a)}$. Thus, $\mathcal{X}_{\pi(a)}$ is a canonical lift. Exactly as in the proof of Lemma 3.2, a is a torsion point. Hence, a is an R'-special point. Conversely, if a is an R'-special point witnessed by $\psi : \mathcal{X}_{\pi(a)} \to \mathcal{X}^{\sigma}_{\pi(a)}$ a lifting of the Frobenius, then as the reduction map is injective on $[B](\mathcal{X}_{\pi(a)}(R')_{\mathrm{tor}})$ and ψ and σ agree upon reduction, $\sigma(a) = \vartheta(a, \ker \psi)$.

□

With the next lemma we transfer Theorem 2.6 from R to R' for varieties defined over K.

Lemma 4.4. *Let $Y \subseteq \mathcal{X}_K$ be an irreducible subvariety of $\mathcal{X}_K$. If $Y(K')$ contains a Zariski dense set of R'-special points, then Y is a special subvariety of $\mathcal{X}_K$.*

Proof. If Y is not a special subvariety, then by Theorem 2.6, there is a proper closed subvariety $Z \subset Y$ (defined over K) so that every R-special point in Y actually lies on Z. By Lemma 4.3, this is expressible as a first-order sentence in the language of valued difference fields with constants from K which is true in $W[k]$. As $W[k']$ is an elementary extension of $W[k]$, this sentence must also hold in $W[k']$. That is, the R'-special points are not Zariski dense in Y contradicting our hypothesis. □

If we were interested only in Zariski closures computed over K, then we would be done now, though we are in a position to finish the proof of theorem 4.1.

Proof. Let $Y \subseteq \mathcal{X}_{K'}$ be an irreducible subvariety of $\mathcal{X}_{K'}$ containing a Zariski dense set of R'-special points. By Lemma 3.3 of [24] there are a natural number N, a (possibly reducible) subvariety $Z \subseteq (\mathcal{X} \times \mathcal{X}^N)_K$, and an R'-special point $b \in \mathcal{X}^N(R')$ so that Z contains a Zariski dense set of R'-special points and $Y = Z_b$. By Lemma 4.4, Z is a special subvariety of $\mathcal{X}^{1+N}$. Of course, the variety $\mathcal{X} \times \{b\}$ is an R'-special subvariety of $\mathcal{X}^{1+N}$ and (the components of) the intersection of two weakly special varieties are again weakly special. Thus, as Y contains an R'-special point, it is R'-special. □

4.2. **Bounds.** On very general grounds, Theorem 2.6 implies uniform bounds. At the qualitative level, we have the following uniformity.

Theorem 4.5. *Fix g, n and R as in Theorem 2.6 and a quasiprojective embedding of $\mathcal{X}$. Then there is a function $f : \mathbb{N} \to \mathbb{N}$ so that for $Y \subseteq \mathcal{X}_{\mathbb{C}}$ a subvariety of degree d, the degree of the Zariski closure of the set of R-special points on Y is at most $f(d)$.*

Proof. By Theorem 2.6 applied to the Cartesian powers of $\mathcal{X}^N$, every irreducible subvariety of $\mathcal{X}_{\mathbb{C}}^N$ containing a Zariski dense set of R-special points is R-special. If C is a component of the intersection of two R-special varieties and C contains an R-special point, then C is R-special. Thus, by Theorem 2.4 of [24] the set of R-special points on $\mathcal{X}$ satisfies automatic uniformity and the function f may be computed using Chow varieties. □

In the course of proving Theorem 2.6 we did not completely describe the sets of form $Y(\mathbb{C}) \cap \Psi_m$ where $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is a closed subvariety. We suggest the following conjecture.

Conjecture 4.6. *If $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is an irreducible subvariety and $Y(\mathbb{C}) \cap \Psi_m$ is Zariski dense in Y, then Y is weakly special.*

If Conjecture 4.6 holds, then our method of proof for Theorem 2.6 provides a method for computing the function f of Theorem 4.5.

Proposition 4.7. *Assume Conjecture 4.6 holds. Fix g, n, and R as in Theorem 2.6 and a quasiprojective embedding of $\mathcal{X}$. Let δ be the degree of $\widetilde{T}_p$ (with respect to this particular embedding). If $Y \subseteq \mathcal{X}_{\mathbb{C}}$ is a subvariety of degree $\deg(Y)$, then the degree of the Zariski closure of the set of R-special points on Y is at most $[(\deg(Y))^2\delta]^{2^{\min\{\frac{g^3+g}{2}, 2\dim(Y)\}}}$.*

Proof. Using the notation of our proof Theorem 2.6, by Proposition 1.2.2 of [11], the degree of Z, the Zariski closure of $Y(\mathbb{C}) \cap \Psi_1$, is at most $(\deg(\widetilde{T}_p)\deg(Y)^2)^{2^{\min\{\dim(\widetilde{T}_p), 2\dim(Y)\}}}$, which is the bound stated in the Proposition. If Conjecture 4.6 holds, then every component of the Zariski closure, Z', of the set of R-special points on Y is a component of Z. Hence, $\deg(Z') \leq \deg(Z)$ and the desired inequality holds. □

Since we have captured the R-special points by difference equations involving the relative Frobenius, there are uniform bounds on the p-adic proximity from R-special points to subvarieties of X. We recall the definition of proximity to a variety.

Definition 4.8. Let (K, v) be a valued field. Let $X \subseteq \mathbb{A}_K^N$ be an affine variety over K with a fixed choice $F_1, \ldots, F_\ell$ of generators of its ideal of definition. For a point $a \in \mathbb{A}_K^N$ we define the proximity of a to X to be $\lambda_v(X, a) := \max\{0, \min\{v(F_i(a))\}\}$.

If Y is a finitely presented algebraic variety over K with a finite affine covering $Y = \bigcup U_i$ and $X \subseteq Y$ is a closed subvariety, then for any $a \in Y(K)$

we define $\lambda_v(X, a)$ to be the minimum value of $\lambda_v(X \cap U_i, a)$ read in the affine charts.

The definition of proximity depends on the choice of generators of $I(X)$ and the covering of Y, but these dependencies are irrelevant to the following statements. If the variety X has a good integral model, then it would be reasonable to fix integral generators for the ideal of definition of X in the definition of the proximity to X function. In so doing, for an integral point a of the ambient space, $\lambda(X, a) = \gamma$ just in case the reduction modulo the ideal $I_\delta := \{y \in \mathcal{O}_K \mid v(y) > \delta\}$ lies in the reduction of X if and only if $\delta < \gamma$.

Proposition 4.9. *With the notation as in Theorem 2.6, if $Z \subseteq \mathcal{X}_K$ is a closed subvariety of $\mathcal{X}_K$, then there is a constant $C \in \mathbb{Z}$ that if $\xi \in \mathcal{X}(R)$ is an R-special point, then either $\xi \in Z(R)$ or $\lambda(Z, \xi) \leq C$.*

Proof. This proof follows the general outline of the proof of Theorem 0.3 of [21]. This proof is composed of two claims.
Claim 1: If Y is the Zariski closure of the set of R-special points on Z, then there is a number $N \in \mathbb{N}$ so that for any R-special point $\xi \in \mathcal{X}(R)$ one has $\lambda(Z, \xi) \leq N(\lambda(Y, \xi) + 1)$.
Proof of Claim 1: Suppose that the claim fails. For each natural number N let ξ_N be an R-special point with $\lambda(Z, \xi_N) > N(\lambda(Y, \xi_N) + 1)$. Let R^* be a nonprincipal ultrapower of R and $\widetilde{\xi} \in \mathcal{X}(R^*)$ the image of the infinite tuple $\langle \xi_N \rangle_{N \in \mathbb{N}}$ under the quotient map $\prod_{N \in \mathbb{N}} R \to R^*$.

We continue to denote the (Krull) valuation on the fraction field of R^* by v. Let $I := \{y \in R^* \mid (\forall N \in \mathbb{N})\ v(y) > N(\lambda(Y, \widetilde{\xi}) + 1)\}$. Since each ξ_i is integral, there is an integer M such that $\lambda(Y, \widetilde{\xi}) > M$. Thus, I is a non-unit ideal of R^* and under the usual diagonal embedding of R into the ultrapower, $I \cap R$ is the zero ideal. Set $\overline{R} := R^*/I$ and let $\overline{\xi}$ be the image of $\widetilde{\xi}$ under the quotient map. By the above observation, the natural map from R to $\overline{R}$ is an embedding.

The formula ϕ of Lemma 4.3 is closed under the specialization $R^* \to \overline{R}$ so that $\overline{\xi}$ is $\overline{R}$-special. By the main theorems of [23] or [3], the extension $R \hookrightarrow \overline{R}$ is elementary. As every R-special point in Z is contained in Y, the same must be true of $\overline{R}$-special points, but by construction $\overline{\xi} \in Z(\overline{R}) \smallsetminus Y(\overline{R})$. $\square$

Claim 2: If $Y \subseteq \mathcal{X}$ is an R-special subvariety (not necessarily irreducible) and $\xi \in \mathcal{X}(R)$ is an R-special point not on Y, then, provided that we compute proximity to Y with respect to generators of its ideal over R, $\lambda(Y, \xi) \leq \frac{1}{p-1}$.

Proof of Claim 2: As the proximity to a finite union is the minimum of the proximities to each set, we may assume that Y is irreducible. If $B \leq \mathcal{X}_Y$ is the stabilizer of Y, and $g : Y \to Y/B \subseteq \mathcal{X}'$ is the quotient map, then

$\lambda(Y,\xi) \leq \lambda(Y/B, \pi(\xi))$. So, it suffices to consider the case that the fibres of Y over $\pi(Y)$ are finite, hence, (because Y is R-special) torsion.

Let L be an algebraic closure of $R[\frac{1}{p}]$ and continue to denote by v the extension of the valuation to L. Write $\mathcal{O}_L := \{x \in K \mid v(x) \geq 0\}$ for the ring of integers in K and set $J := \{x \in K \mid v(x) > \frac{1}{p-1}\}$. Let $\nu : \mathcal{O}_K \to \mathcal{O}_K/J$ be the quotient map and continue to denote by ν the reduction maps $\nu : \mathcal{X}(\mathcal{O}_K) \to \mathcal{X}(\mathcal{O}_K/I)$ and $\nu : \mathcal{A}(\mathcal{O}_K) \to \mathcal{A}(\mathcal{O}_K/I)$. Then each such ν is injective on the set of R-special points. In fact, if $\Xi := \{\zeta \in \mathcal{X}(\mathcal{O}_K) \mid \mathcal{X}_{\pi(\zeta)}$ is a canonical lift and ζ is torsion $\}$, then ν is injective on Ξ. Thus, if $\nu(\xi) \in Y(\mathcal{O}_K/J)$, then $\xi \in Y(R)$. □

The result follows by combining the two claims, taking $C = 2N$.

□

In the course of proving Claim 2 we actually showed that for a special subvariety $Y \subseteq \mathcal{X}_R$ the uniform bound on the proximity to Y is valid over the set of points (over $\mathbb{Q}_p^{\mathrm{alg}}$) which are torsion points on canonical lift fibres. We conjecture that the restriction to Y special is unnecessary.

Conjecture 4.10. *Let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$ with v the extension of the p-adic valuation to $\mathbb{C}_p$ and $\mathcal{O} = \mathcal{O}_{\mathbb{C}_p} := \{x \in \mathbb{C}_p \mid v(x) \geq 0\}$ the ring of integers in $\mathbb{C}_p$. Let $Z \subseteq \mathcal{X}_{\mathbb{C}_p}$ be a closed subvariety of $\mathcal{X}_{\mathbb{C}_p}$. Let $\lambda(Z,\cdot)$ be a p-adic proximity function for Z. Then there is a rational number $q \in \mathbb{Q}$ so that for any point $\xi \in \mathcal{X}(\mathbb{C}_p)$ which is a torsion point of a canonical lift fibre either $\xi \in Z(\mathbb{C}_p)$ or $\lambda(Z,\xi) \leq q$.*

There are many natural strengthenings of Conjecture 4.10. For instance, one might require of ξ only that it is an integral special point (thereby including quasi-canonical fibres) or one might ask for the bound to hold for *all* special points. While this last formulation may seem particularly dangerous since one would have to deal with families of abelian varieties having bad reduction, it should be noted that if $Z \subseteq (\mathcal{X}_a)_{\mathbb{C}_p}$ where $a \in \mathcal{A}(\mathbb{Q}_p^{\mathrm{alg}})$, then, in fact, such a bound exists (see the Main Theorem of [22]).

References

[1] Y. André, **G-Functions and geometry**, Aspects of Mathematics, **E13**, Friedr. Vieweg & Sohn, Braunschweig, 1989. xii+229 pp.

[2] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.* **505** (1998), 203–208.

[3] L. Bélair, A. Macintyre, and T. Scanlon, Model theory of Frobenius on Witt vectors, preprint, 2002,
available at `https://www.math.berkeley.edu/~scanlon/papers/papers.html`.

[4] Z. Chatzidakis and E. Hrushovski, Model theory of difference fields, *Trans. Amer. Math. Soc.* **351** (1999), no. 8, 2997–3071.

[5] P. Clark, Bounds for torsion on abelian varieties with integral moduli, preprint, 2004, `arXiv:math.NT/0407264`.

[6] R. M. Cohn, **Difference algebra**, Interscience Publishers John Wiley & Sons, New York-London-Sydeny 1965 xiv+355 pp.

[7] B. Edixhoven, Special points on the product of two modular curves, *Compositio Math.* **114** (1998), no. 3, 315–328.

[8] B. Edixhoven, On the André-Oort conjecture for Hilbert modular surfaces, **Moduli of abelian varieties** (Texel Island, 1999), 133–155, Progr. Math., **195**, Birkhäuser, Basel, 2001.

[9] B. Edixhoven and A. Yafaev, Subvarieties of Shimura varieties, *Ann. of Math. (2)* **157** (2003), no. 2, 621–645.

[10] E. Hrushovski, Proof of Manin's theorem by reduction to positive characteristic, in **Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture**, (Elisabeth Bouscaren, ed.), Springer **LNM 1696**, Berlin 1998, 197 – 205.

[11] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, *Ann. Pure Appl. Logic* **112** (2001), no. 1, 43–115.

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

[13] W. Messing, **The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes**, Lecture Notes in Mathematics **264**, Springer-Verlag, Berlin, 1972.

[14] J. S. Milne, Abelian varieties, in **Arithmetic Geometry**, (Gary Cornell and Joseph H. Silverman, eds.), Springer-Verlag, New York, 1986, 103 – 150.

[15] B. Moonen, Linearity properties of Shimura varieties, part II, *Compositio Math.* **114** (1998), no. 1, 3–35.

[16] D. Mumford, J. Fogarty, and F. Kirwan, **Geometric Invariant Theory**, third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete **34**, Spinger-Verlag (New York), 1994.

[17] F. Oort, Canonical liftings and dense sets of CM-points, in **Arithmetic geometry** (Cortona, 1994), 228–234, Sympos. Math., XXXVII, Cambridge Univ. Press, Cambridge, 1997.

[18] R. Pink, **Arithmetical Compactifications of Mixed Shimura Varieties**, Ph.D. thesis, Friedrich-Wilhelms-Universität, Bonner Mathematische Schriften **209**, 1989.

[19] R. Pink, A Combination of the Conjectures of Mordell-Lang and André-Oort, preprint, August 2004, available at
`https://www.math.ethz.ch/~pink/preprints.html`

[20] R. Pink and D. Roessler, On Hrushovski's proof of the Manin-Mumford conjecture, Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002), 539–546, Higher Ed. Press, Beijing, 2002.

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

[22] T. Scanlon, The conjecture of Tate and Voloch on p-adic proximity to torsion, *International Mathematics Research Notices* **1999**, no. 17, 909 – 914.

[23] T. Scanlon, Quantifier elimination for the relative Frobenius, in **Valuation Theory and Its Applications Volume II**, conference proceedings of the International Conference on Valuation Theory (Saskatoon, 1999), Franz-Viktor Kuhlmann, Salma Kuhlmann, and Murray Marshall, eds., Fields Institute Communications Series, (AMS, Providence), 2003, 323 - 352.

[24] T. Scanlon, Automatic uniformity, *International Mathematics Research Notices*, (to appear).

University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley, CA 94720-3480, USA

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