THE DYNAMICAL MORDELL-LANG PROBLEM FOR ÉTALE MAPS

J. P. BELL, D. GHIOCA, AND T. J. TUCKER

Abstract. We prove a dynamical version of the Mordell-Lang conjecture for étale endomorphisms of quasiprojective varieties. We use p-adic methods inspired by the work of Skolem, Mahler, and Lech, combined with methods from algebraic geometry. As special cases of our result we obtain a new proof of the classical Mordell-Lang conjecture for cyclic subgroups of a semiabelian variety, and we also answer positively a question of Keeler/Rogalski/Stafford for critically dense sequences of closed points of a Noetherian integral scheme.

1. Introduction

Let X be a quasiprojective variety over the complex numbers $\mathbb{C}$, let $\Phi : X \longrightarrow X$ be a morphism, and let V be a closed subvariety of X. For any integer $i \geq 0$, denote by Φ^i the i^{th} iterate $\Phi \circ \cdots \circ \Phi$; for any point $\alpha \in X(\mathbb{C})$, we let $\mathcal{O}_\Phi(\alpha) := \{\Phi^i(\alpha) : i \in \mathbb{N}\}$ be the (forward) Φ-orbit of α. If $\alpha \in X(\mathbb{C})$ has the property that there is some integer $\ell \geq 0$ such that $\Phi^\ell(\alpha) \in W(\mathbb{C})$, where W is a periodic subvariety of V, then there are infinitely many integers $n \geq 0$ such that $\Phi^n(\alpha) \in V$. More precisely, if $N \geq 1$ is the period of W (the smallest positive integer j for which $\Phi^j(W) = W$), then $\Phi^{kN+\ell}(\alpha) \in W(\mathbb{C}) \subseteq V(\mathbb{C})$ for all integers $k \geq 0$. In [Den94], Denis asked the following question.

Question 1.1. *If there are infinitely many nonnegative integers m such that $\Phi^m(\alpha) \in V(\mathbb{C})$, are there necessarily integers $N \geq 1$ and $\ell \geq 0$ such that $\Phi^{kN+\ell}(\alpha) \in V(\mathbb{C})$ for all integers $k \geq 0$?*

Note that if $V(\mathbb{C})$ contains an infinite set of the form $\{\Phi^{kN+\ell}(\alpha)\}_{k\in\mathbb{N}}$ for some positive integers N and ℓ, then V contains a positive dimensional subvariety invariant under Φ^N (simply take the union of the positive dimensional components of the Zariski closure of $\{\Phi^{kN+\ell}(\alpha)\}_{k\in\mathbb{N}}$).

Denis [Den94] showed that the answer to Question 1.1 is "yes" under the additional hypothesis that the integers n for which $\Phi^n(\alpha) \in V(\mathbb{C})$ are sufficiently dense in the set of all positive integers; he also obtained results for automorphisms of projective space without using this additional hypothesis.

2000 *Mathematics Subject Classification.* Primary 14K12, Secondary 37F10.

Key words and phrases. Mordell-Lang conjecture, dynamics.

The second author was partially supported by NSERC. The third author was partially supported by NSA Grant 06G-067 and NSF Grant DMS-0801072.

Later the problem was solved completely in [Bel06] in the case of automorphisms of affine varieties X, by showing that the set of all $n \in \mathbb{N}$ such that $\Phi^n(\alpha) \in V(\mathbb{C})$ is a union of at most finitely many arithmetic progressions, and of at most finitely many numbers. In [GT09], the following conjecture was proposed.

Conjecture 1.2. *Let X be a quasiprojective variety defined over $\mathbb{C}$, let $\Phi : X \longrightarrow X$ be an endomorphism, let V be a subvariety of X, and let $\alpha \in X(\mathbb{C})$. Then the intersection $V(\mathbb{C}) \cap \mathcal{O}_\Phi(\alpha)$ is a union of at most finitely many orbits of the form $\mathcal{O}_{\Phi^N}(\Phi^\ell(\alpha))$, for some nonnegative integers N and ℓ.*

Note that the orbits for which $N = 0$ are singletons, so that the conjecture allows not only infinite forward orbits but also finitely many extra points. We view our Conjecture 1.2 as a dynamical version of the classical Mordell-Lang conjecture, where subgroups of rank one are replaced by orbits under a morphism.

Results were obtained in the case when $\Phi : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ takes the form (f, g) for $f, g \in \mathbb{C}[t]$ and the subvariety V is a line ([GTZ08]), and in the case when $\Phi : \mathbb{A}^g \longrightarrow \mathbb{A}^g$ has the form $(f, \dots, f)$ where $f \in K[t]$ (for a number field K) has no periodic critical points other than the point at infinity ([BGKT]). Also, in [GT09] a general approach to Conjecture 1.2 was developed in the case the orbit $\mathcal{O}_\Phi(P)$ intersects a sufficiently small p-adic neighborhood of a Φ-periodic point of X where the Jacobian of Φ is diagonalizable. Furthermore, in [GT09], Conjecture 1.2 was proved if X is a semiabelian variety and Φ is an algebraic group endomorphism.

The technique used in [Bel06], [BGKT] and [GT09] is a modification of a method first used by Skolem [Sko34] (and later extended by Mahler [Mah35] and Lech [Lec53]) to treat linear recurrence sequences. The idea is to show that there is a positive integer N such that for each $i = 0, \dots, N-1$ there is a p-adic analytic map θ_i on $\mathbb{Z}_p$ such that $\theta_i(k) = \Phi^{kN+i}(\alpha)$ for all sufficiently large positive integers $k \in \mathbb{N}$. Given any polynomial F in the vanishing ideal of V, one thus obtains a p-adic analytic function $F \circ \theta_i$ that vanishes on all k for which $\Phi^{kN+i}(\alpha) \in V$. Since an analytic function cannot have infinitely many zeros in a compact subset of its domain of convergence unless that function is identically zero, this implies that if there are infinitely many $n \equiv i \pmod N$ such that $\Phi^n(\alpha) \in V$, then $\Phi^{kN+i}(\alpha) \in V$ for all k sufficiently large.

In the case of [Bel06], the existence of the p-adic analytic maps θ_i is proved using properties of automorphisms of the affine plane, such as having constant determinant for their Jacobian. In [BGKT], the existence of the p-adic analytic maps θ_i is proved by using linearizing maps developed by Rivera-Letelier [RL03], while in [GT09], the existence of the θ_i's is proved using work of Hermann and Yoccoz (see [HY83]). In this paper, using methods from arithmetic geometry and p-adic analysis we surpass all of the above results, and we prove Conjecture 1.2 in the case Φ is any étale map.

Theorem 1.3. *Let $\Phi : X \longrightarrow X$ be an étale endomorphism of any quasiprojective variety defined over $\mathbb{C}$. Then for any subvariety V of X, and for any point $\alpha \in X(\mathbb{C})$ the intersection $V(\mathbb{C}) \cap \mathcal{O}_\Phi(\alpha)$ is a union of at most finitely many orbits of the form $\mathcal{O}_{\Phi^N}(\Phi^\ell(\alpha))$ for some $N, \ell \in \mathbb{N}$.*

Our result provides a positive answer to a question raised in [KRS05] regarding critically dense orbits under automorphisms of integral Noetherian schemes (see Section 5). Theorem 1.3 has the following interesting corollary.

Corollary 1.4. *Let X be an irreducible quasiprojective variety, let $\Phi : X \longrightarrow X$ be an étale endomorphism, and let $\alpha \in X(\mathbb{C})$. If the orbit $\mathcal{O}_\Phi(\alpha)$ is Zariski dense in X, then any proper subvariety of X intersects $\mathcal{O}_\Phi(\alpha)$ in at most finitely many points.*

Our result fits into Zhang's far-reaching system of dynamical conjectures (see [Zha06]). Zhang's conjectures include dynamical analogues of Manin-Mumford and Bogomolov conjectures for abelian varieties (now theorems of [Ray83a, Ray83b], [Ull98] and [Zha98]). One of the conjectures from [Zha06] asks that any irreducible projective variety X defined over a number field K has a point in $X(\overline{K})$ with a Zariski dense orbit under any "polarizable" endomorphism Φ (Zhang defines a polarizable endomorphism Φ as one for which there exists an ample line bundle L such that $\Phi^*L \cong L^{\otimes r}$ for some $r > 1$). Note in particular that any Zariski dense orbit must avoid all proper Φ-periodic subvarieties of X. Theorem 1.3 says that *any* subvariety of X containing infinitely many points of a Φ-orbit *must* contain a Φ-periodic subvariety. We hope that Theorem 1.3 represents real progress towards proving Conjecture 1.2.

We now briefly sketch the plan of our paper. In Section 2 we present the geometric setup, while in Section 3 we derive the existence of certain analytic functions which are used later to prove Theorem 4.1. In particular, our results from Section 3 provide generalizations of Rivera-Letelier's results [RL03] regarding analytic conjugation maps corresponding to quasiperiodic domains of rational p-adic functions. In Section 4 we prove our main result, while in Section 5 we present several interesting applications of our Theorem 1.3 for automorphisms of Noetherian integral schemes. In particular, we obtain a new proof of the classical Mordell-Lang conjecture for cyclic subgroups, and we provide a positive answer to [KRS05, Question 11.6].

Notation. We write $\mathbb{N}$ for the set of nonnegative integers. If K is a field, we write $\overline{K}$ for an algebraic closure of K. Given a prime number p, we denote by $|\cdot|_p$ the usual absolute value on $\mathbb{Q}_p$; that is, we have $|p|_p = 1/p$. When we work in $\mathbb{Q}_p^g$ with a fixed coordinate system, then, for $\vec{\alpha} = (\alpha_1 \ldots, \alpha_g) \in \mathbb{Q}_p^g$ and $r > 0$, we write $\mathbb{D}(\vec{\alpha}, r)$ for the open disk of radius r in $\mathbb{Q}_p^g$ centered at α. More precisely, we have

$$\mathbb{D}(\vec{\alpha}, r) := \{(\beta_1, \ldots, \beta_g) \in \mathbb{Q}_p^g \mid \max_i |\alpha_i - \beta_i|_p < r\}.$$

Similarly, we let $\overline{\mathbb{D}}(\vec{\alpha}, r)$ be the *closed* disk of radius r centered at $\vec{\alpha}$. In the case where $g = 1$, we drop the vector notation and denote our discs as $\mathbb{D}(\alpha, r)$ and $\overline{\mathbb{D}}(\alpha, r)$. We say that a function F is *(rigid) analytic* on $\mathbb{D}(\alpha, r)$ (resp. $\overline{\mathbb{D}}(\alpha, r)$) if there is a power series $\sum_{n=0}^{\infty} a_n(z-\alpha)^n$, with coefficients in $\mathbb{Q}_p$, convergent on all of $\mathbb{D}(\alpha, r)$ (resp. $\overline{\mathbb{D}}(\alpha, r)$) such that $F(z) = \sum_{n=0}^{\infty} a_n(z-\alpha)^n$ for all $z \in \mathbb{D}(\alpha, r)$ (resp. $\overline{\mathbb{D}}(\alpha, r)$). We define convergence of an analytic function f on $\mathbb{D}(\vec{\alpha}, r)$ (resp. $\overline{\mathbb{D}}(\vec{\alpha}, r)$) similarly, where $\vec{\alpha} \in \mathbb{Q}_p^g$ for any positive integer g.

Finally, all subvarieties in our paper are closed subvarieties.

2. Preliminary results from arithmetic geometry

In this Section we construct the geometric setup for the proof of Theorem 4.1 which is the main building block for proving Theorem 1.3. More precisely, Theorem 4.1 deals with the case when Φ is an unramified endomorphism of an irreducible smooth quasiprojective variety X. In the proof of Theorem 4.1 we will show that we may assume X has a model $\mathcal{X}$ over $\mathbb{Z}_p$ (for a suitable prime p) such that $\Phi : \mathcal{X} \longrightarrow \mathcal{X}$ is an unramified map. The goal of this Section is to construct a suitable analytic function associated to Φ which maps the residue class of a closed point $x \in \mathcal{X}$ into itself.

2.1. **Notation.**

- $\mathcal{X}$ is a quasiprojective scheme over $\mathbb{Z}_p$ such that both the generic fiber and special fiber are geometrically irreducible varieties (over $\mathbb{Q}_p$ and $\mathbb{F}_p$, respectively);
- $\overline{\mathcal{X}}$ is the closed fiber of $\mathcal{X}$ (i.e., it is $\mathcal{X} \times_{\mathbb{Z}_p} \mathbb{F}_p$);
- X is the generic fiber of $\mathcal{X}$ (i.e., it is $\mathcal{X} \times_{\mathbb{Z}_p} \mathbb{Q}_p$);
- $\Phi : \mathcal{X} \longrightarrow \mathcal{X}$ is an unramified map of $\mathbb{Z}_p$-schemes;
- $\overline{\Phi} : \overline{\mathcal{X}} \longrightarrow \overline{\mathcal{X}}$ is the restriction of Φ on the closed fiber;
- $r : \mathcal{X}(\mathbb{Z}_p) \longrightarrow \overline{\mathcal{X}}(\mathbb{F}_p)$ is the usual reduction map;
- x is an $\mathbb{F}_p$-point on $\mathcal{X}$ in the smooth locus of the projection to $\mathbb{Z}_p$ such that there is a point $\alpha \in \mathcal{X}(\mathbb{Z}_p)$ for which $r(\alpha) = x$.

2.2. **Completions of local rings at smooth closed points.** Let $\mathcal{O}_{\mathcal{X},x}$ be the local ring of x as a point on $\mathcal{X}$ and let $\widehat{\mathcal{O}}_{\mathcal{X},x}$ be the completion of $\mathcal{O}_{\mathcal{X},x}$ at its maximal ideal $\mathfrak{m}$; let $\widehat{\mathfrak{m}}$ be the maximal ideal in $\widehat{\mathcal{O}}_{\mathcal{X},x}$. The Cohen structure theorem (see [Mat86, Section 29] or [Bou06, Chapter IX]) then gives the following.

Proposition 2.1. *There are elements $T_1, \dots, T_g$ of $\widehat{\mathcal{O}}_{\mathcal{X},x}$ such that*

$$\widehat{\mathcal{O}}_{\mathcal{X},x} = \mathbb{Z}_p[[T_1, \dots, T_g]].$$

Proof. Since x is smooth, $\mathcal{O}_{\mathcal{X},x}$ must be a regular ring. Therefore, its completion $\widehat{\mathcal{O}}_{\mathcal{X},x}$ must be regular as well by [AM69, Proposition 11.24]. The existence of a point in $\mathcal{X}(\mathbb{Z}_p)$ that reduces to x means that there is a surjective map $g : \mathcal{O}_{\mathcal{X},x} \longrightarrow \mathbb{Z}_p$, which extends to a map $\hat{g} : \widehat{\mathcal{O}}_{\mathcal{X},x} \longrightarrow \mathbb{Z}_p$. Because

$\hat{g}$ is surjective, we conclude that $p \notin \widehat{\mathfrak{m}}^2$; thus $\widehat{\mathcal{O}}_{\mathcal{X},x}$ is unramified, in the terminology of [Mat86, Section 29]. Theorem 29.7 of [Mat86] states that any unramified complete regular Noetherian ring of characteristic 0 with a finite residue field is a formal power series ring over a complete p-ring. By [Mat86, Corollary, p. 225], $\mathbb{Z}_p$ is the only complete p-ring with residue field $\mathbb{F}_p$ (note that $\mathcal{O}_{\mathcal{X},x}$ has residue field $\mathbb{F}_p$ because we have a surjective map, induced by g, from the residue field of $\mathcal{O}_{\mathcal{X},x}$ onto $\mathbb{F}_p$). □

There is a one-to-one correspondence between the points in $\mathcal{X}(\mathbb{Z}_p)$ that reduce to x and the primes $\mathfrak{p}$ in $\mathcal{O}_{\mathcal{X},x}$ such that $\mathcal{O}_{\mathcal{X},x}/\mathfrak{p} \cong \mathbb{Z}_p$. For each such prime $\mathfrak{p}$, its completion $\hat{\mathfrak{p}}$ in $\widehat{\mathcal{O}}_{\mathcal{X},x}$ has the property that $\mathfrak{p}\widehat{\mathcal{O}}_{\mathcal{X},x} = \hat{\mathfrak{p}}$ (see [Mat86, Theorem 8.7]). Furthermore, $\hat{\mathfrak{p}}$ is a prime ideal in $\widehat{\mathcal{O}}_{\mathcal{X},x}$ with residue domain $\mathbb{Z}_p$ since the sequence

$$0 \longrightarrow \hat{\mathfrak{p}} \longrightarrow \widehat{\mathcal{O}}_{\mathcal{X},x} \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

is exact; this follows from the fact that $\widehat{\mathcal{O}}_{\mathcal{X},x}$ is flat over $\mathcal{O}_{\mathcal{X},x}$ ([Mat86, Theorem 8.8]) along with the fact that the quotient $\mathcal{O}_{\mathcal{X},x}/\mathfrak{p} \cong \mathbb{Z}_p$ is complete with respect to the $\mathfrak{m}$-adic topology. Thus, if $\mathfrak{q}$ is any prime in $\widehat{\mathcal{O}}_{\mathcal{X},x}$ with residue domain $\mathbb{Z}_p$ then $\mathfrak{q}$ must be the completion of $\mathfrak{q} \cap \mathcal{O}_{\mathcal{X},x}$, because $\dim \mathcal{O}_{\mathcal{X},x} = \dim \widehat{\mathcal{O}}_{\mathcal{X},x}$ ([AM69, Corollary 11.19]). Hence, we have a one-to-one correspondence between the points in $\mathcal{X}(\mathbb{Z}_p)$ that reduce to x and the primes $\mathfrak{q}$ in $\widehat{\mathcal{O}}_{\mathcal{X},x}$ such that $\widehat{\mathcal{O}}_{\mathcal{X},x}/\mathfrak{q} \cong \mathbb{Z}_p$. Note that primes $\mathfrak{q}$ in $\widehat{\mathcal{O}}_{\mathcal{X},x}$ for which $\widehat{\mathcal{O}}_{\mathcal{X},x}/\mathfrak{q} \cong \mathbb{Z}_p$ are simply the ideals of the form $(T_1 - pz_1, \ldots, T_g - pz_g)$ where the z_i are in $\mathbb{Z}_p$. For each $\mathbb{Z}_p$-point β in $\mathcal{X}$ such that $r(\beta) = x$, we write $\iota(\beta) = (\beta_1, \ldots, \beta_g)$ where β corresponds to the prime ideal

$$(T_1 - p\beta_1, \ldots, T_g - p\beta_g)$$

in $\widehat{\mathcal{O}}_{\mathcal{X},x}$. Note that $\iota^{-1} : \mathbb{Z}_p^g \longrightarrow \mathcal{X}(\mathbb{Z}_p)$ induces an analytic bijection between $\mathbb{Z}_p^g$ and the analytic neighborhood of $\mathcal{X}(\mathbb{Z}_p)$ consisting of points β such that $r(\beta) = x$.

Proposition 2.2. *Suppose that $\overline{\Phi}(x) = x$. Then there are power series $F_1, \ldots, F_g \in \mathbb{Z}_p[[U_1, \ldots, U_g]]$ such that*

(i) *each F_i converges on $\mathbb{Z}_p^g$;*

(ii) *for each $\beta \in \mathcal{X}(\mathbb{Z}_p)$ such that $r(\beta) = x$, we have*

$$\iota(\Phi(\beta)) = (F_1(\beta_1, \ldots, \beta_g), \ldots, F_g(\beta_1, \ldots, \beta_g)); \text{ and} \tag{2.2.1}$$

(iii) *each F_i is congruent to a linear polynomial mod p (in other words, all the coefficients of terms of degree greater than one are divisible by p).*

Proof. The map Φ induces a ring homomorphism

$$\Phi^* : \widehat{\mathcal{O}}_{\mathcal{X},x} \longrightarrow \widehat{\mathcal{O}}_{\mathcal{X},x}$$

that sends the maximal ideal $\widehat{\mathfrak{m}}$ in $\widehat{\mathcal{O}}_{\mathcal{X},x}$ to itself. For each i, there is a power series $H_i \in \mathbb{Z}_p[[T_1, \ldots, T_g]]$ such that $\Phi^* T_i = H_i$. Furthermore, since $\Phi^* T_i$

must be in the maximal ideal of $\widehat{\mathcal{O}}_{\mathcal{X},x}$, the constant term in H_i must be in $p\mathbb{Z}_p$. Then, for any $(\alpha_1,\dots,\alpha_g)\in p\mathbb{Z}_p$, we have

$$(\Phi^*)^{-1}(T_1-\alpha_1,\dots,T_g-\alpha_g)=(T_1-H_1(\alpha_1,\dots,\alpha_g),\dots,T_g-H_g(\alpha_1,\dots,\alpha_g))$$

since

$$(T_1-H_1(\alpha_1,\dots,\alpha_g),\dots,T_g-H_g(\alpha_1,\dots,\alpha_g))$$

is a prime ideal of coheight equal to one, and

$$H_i(T_1,\dots,T_g)-H_i(\alpha_1,\dots,\alpha_g)$$

is in the ideal $(T_1-\alpha_1,\dots,T_g-\alpha_g)$ for each i. Thus, if β corresponds to the prime ideal

$$(T_1-p\beta_1,\dots,T_g-p\beta_g)$$

then $\Phi(\beta)$ corresponds to the prime ideal

$$(T_1-H_1(p\beta_1,\dots,p\beta_g),\dots,T_g-H_g(p\beta_1,\dots,p\beta_g)).$$

Hence, letting

$$F_i(T_1,\dots,T_g):=\frac{1}{p}H_i(pT_1,\dots,pT_g)$$

gives the desired map. Since $H_i\in\mathbb{Z}_p[[T_1,\dots,T_g]]$, it follows that F_i must converge on $\mathbb{Z}_p$ and that all the coefficients of terms of degree greater than one of F_i are divisible by p. Since the constant term in H_i is divisible by p, we conclude that

$$F_1,\dots,F_g\in\mathbb{Z}_p[[T_1,\dots,T_g]],$$

as desired. □

Switching to vector notation, we write

$$\vec{\beta}:=(\beta_1,\dots,\beta_g)\in\mathbb{Z}_p^g,$$

and we let

$$\mathcal{F}(\vec{\beta}):=(F_1(\beta_1,\dots,\beta_g),\dots,F_g(\beta_1,\dots,\beta_g)).$$

From Proposition 2.2, we see that there is a $g\times g$ matrix L with coefficients in $\mathbb{Z}_p$ and a constant $\vec{C}\in\mathbb{Z}_p^g$ such that

$$\mathcal{F}(\vec{\beta})=\vec{C}+L(\vec{\beta})+\text{ higher order terms} \tag{2.2.2}$$

Note that since all of the higher order terms are divisible by p, we also have

$$\mathcal{F}(\vec{\beta})\equiv\vec{C}+L(\vec{\beta})\pmod{p}. \tag{2.2.3}$$

Remark 2.3. Moreover, using that $F_i(T_1,\dots,T_g)=\frac{1}{p}H_i(pT_1,\dots,pT_g)$, we obtain that for each $k_1,\dots,k_g\in\mathbb{N}$ such that $k_1+\cdots+k_g\ge 1$, the coefficient of $T_1^{k_1}\cdots T_g^{k_g}$ in F_i belongs to $p^{k_1+\cdots+k_g-1}\cdot\mathbb{Z}_p$.

Proposition 2.4. *Suppose that $\overline{\Phi}(x)=x$ and that $\overline{\Phi}$ is unramified at x. Let L be as in* (2.2.2). *Then L is invertible modulo p.*

Proof. Let $\mathcal{O}_{\overline{\mathcal{X}},x}$ denote the local ring of x on $\overline{\mathcal{X}}$ and let $\overline{\mathfrak{m}}$ denote its maximal ideal. Since $\overline{\Phi}$ is unramified, the map $\overline{\Phi}^* : \mathcal{O}_{\overline{\mathcal{X}},x} \longrightarrow \mathcal{O}_{\overline{\mathcal{X}},x}$ sends $\overline{\mathfrak{m}}$ surjectively onto itself (see [BG06, Appendix B.2]). Thus in particular it induces an isomorphism on the $\mathbb{F}_p$-vector space $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$. Completing $\mathcal{O}_{\overline{\mathcal{X}},x}$ at $\overline{\mathfrak{m}}$, we then get an induced isomorphism σ on $\widehat{\overline{\mathfrak{m}}}/\widehat{\overline{\mathfrak{m}}}^2$, where $\widehat{\overline{\mathfrak{m}}}$ is the maximal ideal in the completion of $\mathcal{O}_{\overline{\mathcal{X}},x}$ at $\overline{\mathfrak{m}}$. This isomorphism is obtained by taking the map $\Phi^* : \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2 \longrightarrow \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2$ and modding out by p, where $\widehat{\mathfrak{m}}$ is the maximal ideal of $\widehat{\mathcal{O}}_{\mathcal{X},x}$. Writing σ as a linear transformation with respect to the basis $T_1, \dots, T_g$ for $\widehat{\overline{\mathfrak{m}}}/\widehat{\overline{\mathfrak{m}}}^2$, we obtain the dual of the reduction of L mod p. Thus, if $\overline{\Phi}^*$ induces an isomorphism on $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$, then the reduction mod p of L itself must be invertible. $\square$

Remark 2.5. Note that the dual of $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ is the Zariski tangent space of the point x considered as a point on the special fiber $\overline{\mathcal{X}}$ (see [Har77, page 80]). Thus the reduction of L modulo p is simply the Jacobian of $\overline{\Phi}$ at x. Note also that $\overline{\Phi}$ is unramified at x *if and only if* L is invertible modulo p. This follows from the fact that $\overline{\Phi}^* : \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \longrightarrow \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ is surjective if and only if it is injective, by a simple dimension count; thus, $\mathcal{O}_{\overline{\mathcal{X}},x}\overline{\Phi}^*(\overline{\mathfrak{m}}) = \overline{\mathfrak{m}}$ if and only if L is invertible modulo p (see [AK70, page 112]).

Proposition 2.6. *There exists a positive integer n such that $\mathcal{F}^n(\vec{\beta}) \equiv \vec{\beta} \pmod p$ for each $\vec{\beta} \in \mathbb{Z}_p^g$.*

Proof. Because L is invertible modulo p, it means that the reduction modulo p of the affine map

$$\vec{\beta} \mapsto \vec{C} + L(\vec{\beta})$$

induces an automorphism of $\mathbb{F}_p^g$. Therefore, there exists a positive integer n such that

$$\mathcal{F}^n(\vec{\beta}) \equiv \vec{\beta} \pmod p, \tag{2.6.1}$$

for all $\vec{\beta} \in \mathbb{Z}_p$. $\square$

3. Construction of an analytic function

The goal of this Section is to construct a p-adic analytic function $U : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p^n$ such that $U(z+1) = \mathcal{F}(U(z))$, where $\mathcal{F}$ is constructed as in Section 2 for a closed point $x \in \mathcal{X}$ and an unramified endomorphism Φ of the n-dimensional smooth $\mathbb{Z}_p$-scheme $\mathcal{X}$. For this, we generalize the construction from [Bel06], and thus provide the key analytical result (see our Theorem 3.3) which will be used in the proof of Theorem 4.1.

Definition 3.1. *Given a prime p, we let B denote the ring of Mahler polynomials and let C denote the ring of Mahler series; i.e.,*

$$B \;=\; \left\{ \sum_{i=0}^{m} c_i \binom{z}{i} \;:\; c_i \in \mathbb{Z}_p, m \geq 0 \right\},$$

$$C = \left\{ \sum_{i=0}^{\infty} c_i \binom{z}{i} \ : \ c_i \in \mathbb{Z}_p, |c_i|_p \to 0 \right\}.$$

Remark 3.1. The names Mahler polynomial and Mahler series are used because of a result of Mahler [Mah58, Mah61], which states that C is precisely the collection of continuous maps from $\mathbb{Z}_p$ to itself.

More precisely, Mahler shows that B is the ring of all polynomials $f \in \mathbb{Q}_p[z]$ such that $f(\mathbb{Z}_p) \subset \mathbb{Z}_p$, while C is the ring of all power series $g \in \mathbb{Q}_p[[z]]$ which are convergent on $\mathbb{Z}_p$ and satisfy $g(\mathbb{Z}_p) \subset \mathbb{Z}_p$.

We will use the following definition.

Definition 3.2. *Let S be a set of analytic $\mathbb{Z}_p$-power series. By a $\mathbb{Z}_p$-power series with variables in S, we mean any $\mathbb{Z}_p$-power series $F(z_1, \dots, z_k)$ (for some $k \in \mathbb{N}$) where we are substituting an element of S for each variable z_i. Furthermore, for any $i, j \in \{1, \dots, k\}$ (possibly equal), when we substitute $f, g \in S$ for z_i and respectively z_j, the monomial $z_i z_j$ corresponds to the usual product $f \cdot g$, and not to the composition of those two polynomials.*

Lemma 3.2. *Let $n \in \mathbb{N}$ and let p be a prime number. We let*

$$S_n = \left\{ c + \sum_{i=1}^{n} p^i h_i(z) \mid c \in \mathbb{Z}_p, h_i(z) \in B, \deg(h_i) \le 2i - 1 \right\}$$

and

$$T_n = S_n + \left\{ \sum_{i=1}^{\infty} p^i h_i(z) \mid h_i(z) \in B, \deg(h_i) \le 2i - 2 \right\},$$

with the convention that if $n = 0$, then $S_n = \mathbb{Z}_p$.

Then the subalgebra of C generated by convergent $\mathbb{Z}_p$-power series with variables in S_n is contained in T_n.

Proof. For $n = 0$, the conclusion is immediate. So, assume $n \ge 1$.

Since S_n and T_n are both closed under addition, and T_n is closed under taking limits of polynomials which are contained in T_n, and $S_n \subseteq T_n$, it is sufficient to show that $S_n T_n \subseteq T_n$. To do this, suppose

$$H(z) = c_1 + \sum_{i=1}^{n} p^i h_i(z) \ \in \ S_n$$

and

$$G(z) = c_2 + \sum_{i=1}^{\infty} p^i g_i(z) \ \in \ T_n,$$

where $c_1, c_2 \in \mathbb{Z}_p$ and $h_i(z), g_i(z) \in B$ with $\deg(g_i) \le 2i - 2$ for $i > n$ and $\deg(g_i), \deg(h_i) \le 2i - 1$ for $i \le n$. We must show that $H(z)G(z) \in T_n$.

Notice that

$$H(z)G(z) \;=\; -c_1c_2 + c_2H(z) + c_1G(z) + \left(\sum_{i=1}^{n} p^i h_i(z)\right) \cdot \left(\sum_{j=1}^{\infty} p^j g_j(z)\right).$$

Then $(-c_1c_2 + c_2H(z) + c_1G(z)) \in T_n$ and since T_n is closed under addition, it is sufficient to show that

$$\left(\sum_{i=1}^{n} p^i h_i(z)\right) \cdot \left(\sum_{j=1}^{\infty} p^j g_j(z)\right) \;=\; \sum_{k=2}^{\infty} p^k \sum_{i=1}^{k-1} g_i(z) h_{k-i}(z)$$

is in T_n. But since $g_i(z)$ has degree at most $2i-1$ and $h_{k-i}(z)$ has degree at most $2(k-i)-1$, we see that

$$\sum_{i=1}^{k-1} g_i(z) h_{k-i}(z)$$

has degree at most $2k-2$. It follows that

$$\left(\sum_{i=1}^{n} p^i h_i(z)\right) \cdot \left(\sum_{j=1}^{\infty} p^j g_j(z)\right) \;\in\; T_n.$$

This concludes the proof of Lemma 3.2. ☐

Theorem 3.3. *Let n be a positive integer, let p be a prime number and let $\varphi_1, \dots, \varphi_n \in \mathbb{Z}_p[[x_1, \dots, x_n]]$ be convergent power series on $\mathbb{Z}_p^n$ such that for each $i = 1, \dots, n$ we have*

(a) $\varphi_i(x_i) \equiv x_i \pmod{p}$*; and*
(b) *for each $k_1, \dots, k_n \in \mathbb{N}$ such that $k_1 + \cdots + k_n \geq 2$, the coefficient of $x_1^{k_1} \cdots x_n^{k_n}$ in the power series φ_i belongs to $p^{k_1+\cdots+k_n-1} \cdot \mathbb{Z}_p$.*

Let $(\omega_1, \dots, \omega_n) \in \mathbb{Z}_p^n$ be an arbitrary point. If $p > 3$, then there exist p-adic analytic functions $f_1, \dots, f_n \in \mathbb{Q}_p[[z]]$ such that for each $i = 1, \dots, n$ we have

(i) *f_i is convergent for $|z|_p \leq 1$;*
(ii) *$f_i(0) = \omega_i$;*
(iii) *$|f_i(z)|_p \leq 1$ for $|z|_p \leq 1$; and*
(iv) *$f_i(z+1) = \varphi_i(f_1(z), \dots, f_n(z))$.*

A particular case of our result, when $n = 1$ and φ_1 is a rational p-adic function, is discussed in [RL03].

Proof of Theorem 3.3. We construct $(f_1(z), ..., f_n(z))$ by "approximation". We let B and C be the ring of Mahler polynomials and the ring of Mahler series that are convergent for $|z|_p \leq 1$ (as in Definition 3.1). We prove that for each $j \geq 0$ there exist polynomials $h_{i,j}(z) \in B$ $(1 \leq i \leq n)$ that satisfy the three conditions:

(1) for each $i = 1, \dots, n$, we have $h_{i,0}(0) = \omega_i$, while $h_{i,j}(0) = 0$ for $j \geq 1$;
(2) $h_{i,j}(z)$ has degree at most $2j-1$ for $j \geq 1$ and $1 \leq i \leq n$; and

(3) if $g_{i,j}(z) = \sum_{k=0}^{j} p^k h_{i,k}(z)$, then for each $i = 1, \ldots, n$ we have

$$g_{i,j}(z+1) \equiv \varphi_i(g_{1,j}(z), \ldots, g_{n,j}(z)) \pmod{p^{j+1}C}.$$

We define $h_{i,0}(z) = g_{i,0}(z) = \omega_i$ for $1 \le i \le n$. Because $\varphi_i(x_1, \ldots, x_n) \equiv x_i \pmod{p}$, and because each φ_i is convergent on $\mathbb{Z}_p^n$, we conclude that for every $i = 1, \ldots, n$ we have

$$g_{i,0}(z+1) \equiv \varphi_i(g_{1,0}(z), \ldots, g_{n,0}(z)) \equiv \omega_i \pmod{pC}.$$

Let $j \ge 1$ and assume that we have defined $h_{i,k}$ for $1 \le i \le n$ and $k < j$ so that conditions (1)-(3) hold. Our goal is now to construct polynomials $h_{i,j}(z) \in B$, so that conditions (1)-(3) hold. By assumption

$$g_{i,j-1}(z+1) - \varphi_i(g_{1,j-1}(z), \ldots, g_{n,j-1}(z)) = p^j Q_{i,j}(z), \tag{3.2.1}$$

with $Q_{i,j} \in C$ for $1 \le i \le n$. Using the notation of the statement of Lemma 3.2, we see that conditions (2) and (3) show that $g_{1,j-1}(z), \ldots, g_{n,j-1}(z)$ are in S_{j-1}. Thus by Lemma 3.2 we see that

$$p^j Q_{i,j}(z) \;=\; g_{i,j-1}(z+1) - \varphi_i(g_{1,j-1}(z), \ldots, g_{n,j-1}(z))$$

is in T_{j-1} (note that our hypothesis (b) implies that each

$$\varphi_i(g_{1,j-1}(z), \ldots, g_{n,j-1}(z))$$

is a convergent power series). It follows that we can write $p^j Q_{i,j}(z) = c_{i,j} + \sum_{k=1}^{\infty} p^k q_{ijk}(z)$ for some $c_{i,j} \in \mathbb{Z}_p$ and polynomials $q_{ijk}(z) \in B$ such that $\deg(q_{ijk}) \le 2k-1$ for $k \le j-1$ and $\deg(q_{ijk}) \le 2k-2$ for $k \ge j$. Consequently, $p^j Q_{i,j}(z)$ is congruent modulo $p^{j+1}C$ to the polynomial

$$c_{i,j} + \sum_{k=1}^{j} p^k q_{ijk}(z), \tag{3.2.2}$$

which is a polynomial of degree at most $2j-2$. Note that the polynomial in (3.2.2) must send $\mathbb{Z}_p$ to $p^j\mathbb{Z}_p$ since $p^j Q_{i,j}(z)$ does, so dividing out by p^j, we see by Remark 3.1 that $Q_{i,j}(z)$ is congruent to a polynomial in B of degree at most $2j-2$ modulo pC. To satisfy property (3) for j it is sufficient to find $\{h_{i,j}(z) \in B : 1 \le i \le n\}$ such that

$$g_{i,j-1}(z+1)+p^j h_{i,j}(z+1)-\varphi_i(g_{1,j-1}(z)+p^j h_{1,j}(z), \ldots, g_{n,j-1}(z)+p^j h_{n,j}(z))$$

is in $p^{j+1}C$ for $1 \le i \le n$. Modulo $p^{j+1}C$, this expression becomes

$$p^j Q_{i,j}(z)+p^j h_{i,j}(z+1) - p^j \sum_{\ell=1}^{n} h_{\ell,j}(z) \frac{\partial \varphi_i}{\partial x_\ell}(x_1, ..., x_n)\Big|_{x_1=g_{1,j-1}(z),\ldots,x_n=g_{n,j-1}(z)}.$$

It therefore suffices to solve the system

$$Q_{i,j}(z) + h_{i,j}(z+1) - \sum_{\ell=1}^{n} h_{\ell,j}(z) \frac{\partial \varphi_i}{\partial x_\ell}(x_1, ..., x_n)\Big|_{x_1=g_{1,j-1}(z),\ldots,x_n=g_{n,j-1}(z)} = 0 \tag{3.2.3}$$

modulo pC for $0 \le i \le n$. By our hypotheses (a) on φ, we have

$$\frac{\partial \varphi_i}{\partial x_\ell}(x_1, ..., x_n)\Big|_{x_1=g_{1,j-1}(z),...,x_n=g_{n,j-1}(z)} \equiv \delta_{i\ell} \ (\mathrm{mod} pC),$$

where $\delta_{i\ell}$ is usual Kronecker delta defined by $\delta_{i\ell} = 0$ for $i \ne \ell$ and $\delta_{ii} = 1$. Hence it is sufficient to solve

$$Q_{i,j}(z) + h_{i,j}(z+1) - h_{i,j}(z) \equiv 0 \pmod{pC}. \tag{3.2.4}$$

Using the identity

$$\binom{z+1}{k} - \binom{z}{k} = \binom{z}{k-1},$$

we see that since $Q_{1,j}, \ldots, Q_{n,j}$ have degree at most $2j-2$ modulo pC, there exists a solution $[h_{1,j}(z), ..., h_{n,j}(z)] \in B^n$ satisfying conditions (1) and (2). Thus conditions (1)-(3) are satisfied for j. This completes the induction step.

We now set

$$f_i(z) := \sum_{j=0}^{\infty} p^j h_{i,j}(z).$$

For $j \ge 1$, each $h_{i,j}(z)$ is of degree at most $2j-1$, and so

$$h_{i,j}(z) = \sum_{k=0}^{2j-1} c_{ijk}\binom{z}{k},$$

with $c_{ijk} \in \mathbb{Z}_p$, and $c_{ij0} = 0$ for $j \ge 1$. Thus $f_i(0) = \omega_i$ for each $i = 1, \ldots, n$ because $h_{i,0}(z) = \omega_i$. We now find that

$$\begin{aligned} f_i(z) &= \omega_i + \sum_{j=1}^{\infty} p^j \left(\sum_{k=1}^{2j-1} c_{ijk}\binom{z}{k}\right) \\ &= \omega_i + \sum_{k=1}^{\infty} b_{ik}\binom{z}{k} \qquad (3.2.5) \end{aligned}$$

in which

$$b_{ik} := \sum_{j=1}^{\infty} p^j c_{ijk}$$

is absolutely convergent p-adically, since each $c_{ijk} \in \mathbb{Z}_p$. To show the series (3.2.5) is analytic on $\mathbb{Z}_p$, we must establish that $|b_{ik}|_p/|k!|_p \to 0$ as $k \to \infty$, i.e. that for any $j > 0$ one has $b_{ik}/k! \in p^j\mathbb{Z}_p$ for all sufficiently large k (see [Rob00, Theorem 4.7, pp. 354.]). To do this, we note that $c_{ijk} = 0$ if $j < (k+1)/2$ since $\deg h_{i,j} \le 2j-1$. Hence

$$b_{ik} := \sum_{j \ge (k+1)/2} p^j c_{ijk}.$$

It follows that $|b_{ik}|_p \le p^{-(k+1)/2}$. Since $1/|k!|_p < p^{k/(p-1)}$, we see that $b_{ik}/k! \to 0$ since $p > 3$. Hence $f_1, \ldots, f_n$ are p-adic analytic maps on $\mathbb{Z}_p$.

By construction

$$f_i(z) \equiv g_{i,j}(z) \pmod{p^{j+1}C}.$$

It then follows from property (3) above that

$$f_i(z+1) \equiv \varphi_i(f_1(z), ..., f_n(z)) \pmod{p^{j+1}C}$$

Since this holds for all $j \geq 1$, we conclude that

$$f_i(z+1) = \varphi_i(f_1(z), ..., f_n(z)),$$

as desired. □

We note that the argument used in the proof of Theorem 3.3 fails if $p \leq 3$, because for such p we have $|1/k!|_p \geq p^{(k-1)/2}$ for infinitely many natural numbers k and hence we cannot guarantee that the power series we construct converge for $|z|_p \leq 1$ in these cases. In fact, one can construct explicit examples which show that the conclusion to the statement of Theorem 3.3 does not hold if one eliminates the hypothesis that p be at least 5.

4. Proof of the main result

First we prove Theorem 1.3 if X is an irreducible smooth variety.

Theorem 4.1. *Let $\Phi : X \longrightarrow X$ be an unramified endomorphism of an irreducible smooth quasiprojective variety defined over $\mathbb{C}$. Then for any subvariety V of X, and for any point $\alpha \in X(\mathbb{C})$ the intersection $V(\mathbb{C}) \cap \mathcal{O}_\Phi(\alpha)$ is a union of at most finitely many orbits of the form $\mathcal{O}_{\Phi^N}(\Phi^\ell(\alpha))$ for some nonnegative integers N and ℓ.*

Remark 4.2. Because Φ is unramified, while X is smooth, we actually have that Φ is étale (according to [Sha77, Theorem 5, page 145], we obtain an induced isomorphism on the tangent space at each point, which means that Φ is étale).

Proof of Theorem 4.1. Let V be any subvariety of X. We choose an embedding over $\mathbb{C}$ of $\rho : X \longrightarrow \mathbb{P}^M$ as an open subset of a projective variety (for some positive integer M). We write $\rho(X) = Z(\mathfrak{a}) \setminus Z(\mathfrak{b})$ for homogeneous ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathbb{C}[x_0, \ldots, x_M]$, where $Z(\mathfrak{c})$ denotes the Zariski closed subset of $\mathbb{P}^M$ on which the ideal $\mathfrak{c}$ vanishes. We choose generators $F_1, \ldots, F_m$ and $G_1, \ldots, G_n$ for $\mathfrak{a}$ and $\mathfrak{b}$, respectively. Let R be a finitely generated $\mathbb{Z}$-algebra containing the coefficients of the F_i, G_i, of the polynomials defining the variety V, and of the polynomials defining the morphism Φ and such that $\alpha \in \mathbb{P}^M(R)$. Let $\mathcal{X} \subset \mathbb{P}^M_{\mathrm{Spec}(R)}$ be the model for X over $\mathrm{Spec}\, R$ defined by $Z(\mathfrak{a}') \setminus Z(\mathfrak{b}')$ where $\mathfrak{a}'$ and $\mathfrak{b}'$ are the homogeneous ideals in $R[x_0, \ldots, x_M]$ defined by $F_1, \ldots, F_m$ and $G_1, \ldots, G_n$, respectively; similarly, let $\mathcal{V}$ be the model of V over $\mathrm{Spec}(R)$. We now prove two propositions which allow us to pass from $\mathbb{C}$ to $\mathbb{Z}_p$.

Proposition 4.3. *There exists a dense open subset U of $\mathrm{Spec}(R)$ such that the following properties hold*

(i) *there is a scheme $\mathcal{X}_U$ that is smooth and quasiprojective over U, and whose generic fiber equals X;*
(ii) *each fiber of $\mathcal{X}_U$ is geometrically irreducible;*
(iii) *Φ extends to an unramified endomorphism Φ_U of $\mathcal{X}_U$; and*
(iv) *α extends to a section $U \longrightarrow \mathcal{X}_U$.*

Proof of Proposition 4.3. We cover X by a finite set $(Y_i)_{1\le i\le \ell}$ of open subsets such that Φ restricted to each Y_i is represented by polynomials $P_{i,j}$ for $0 \le j \le M$. Let $\mathcal{B}$ be the closed subset of $\mathcal{X}$ which is the zero set of the polynomials $P_{i,j}$ for $1 \le i \le \ell$ and $0 \le j \le M$. Because Φ is a well-defined morphism on the generic fiber X, we conclude that $\mathcal{B}$ does not intersect the generic fiber of $\mathcal{X} \longrightarrow \operatorname{Spec}(R)$. Therefore $\mathcal{B}$ is contained in the pullback under $\mathbb{P}^M_{\operatorname{Spec}(R)} \longrightarrow \operatorname{Spec}(R)$ of a proper closed subset E_1 of $\operatorname{Spec}(R)$. Similarly, let $\mathcal{C}$ be the closed subset defined by the intersection of $Z(\mathfrak{b}')$ with the Zariski closure of α in $\mathbb{P}^M_{\operatorname{Spec}(R)}$. Because $\alpha \in X$, then $\mathcal{C}$ is contained in the pullback under $\mathbb{P}^M_{\operatorname{Spec}(R)} \longrightarrow \operatorname{Spec}(R)$ of a proper closed subset E_2 of $\operatorname{Spec}(R)$. Let $U' = \operatorname{Spec} R \setminus (E_1 \cup E_2)$, let $\mathcal{X}'$ be the restriction of $\mathcal{X}$ above U', and let $\Phi_{U'}$ be the base extension of Φ to an endomorphism of $\mathcal{X}'$.

There is an open subset of $\mathcal{X}'$ on which the restriction of the projection map to $\mathcal{X}' \longrightarrow U'$ is smooth, by [AK70, Remark VII.1.2, page 128] and there is an open subset of $\mathcal{X}'$ on which $\Phi_{U'}$ is unramified by [AK70, Proposition VI.4.6, page 116]. Also, [vdDS84, Theorem (2.10)] shows that the condition of being geometrically irreducible is a first order property which is thus inherited by fibers above a dense open subset of $\operatorname{Spec}(R)$. Since each of these open sets contains the generic fiber, the complement of their intersection must be contained in the pullback under $\mathcal{X}' \longrightarrow U'$ of a proper closed subset E_3 of $\operatorname{Spec}(R)$. Let $U := U' \setminus E_3$; then letting $\mathcal{X}_U$ be the restriction of $\mathcal{X}'$ above U yields the model and the endomorphism Φ_U (which is the restriction of $\Phi_{U'}$ above U) with the desired properties. □

The following result is an easy consequence of [Bel06, Lemma 3.1] (see also [Lec53]).

Proposition 4.4. *There exists a prime $p \ge 5$, an embedding of R into $\mathbb{Z}_p$, and a $\mathbb{Z}_p$-scheme $\mathcal{X}_{\mathbb{Z}_p}$ such that*

(i) *$\mathcal{X}_{\mathbb{Z}_p}$ is smooth and quasiprojective over $\mathbb{Z}_p$, and its generic fiber equals X;*
(ii) *both the generic and the special fiber of $\mathcal{X}_{\mathbb{Z}_p}$ are geometrically irreducible;*
(iii) *Φ extends to an unramified endomorphism $\Phi_{\mathbb{Z}_p}$ of $\mathcal{X}_{\mathbb{Z}_p}$; and*
(iv) *α extends to a section $\operatorname{Spec}\mathbb{Z}_p \longrightarrow \mathcal{X}_{\mathbb{Z}_p}$.*

Proof of Proposition 4.4. With the notation as in Proposition 4.3, since U is a dense open subset of $\operatorname{Spec}(R)$, there exists a nonzero element $f \in R$ which is contained in all prime ideals of $\operatorname{Spec} R \setminus U$. Therefore, there is an open affine subset of U that is isomorphic to $\operatorname{Spec}(R[f^{-1}])$ (note that R is an integral domain). Since R is finitely generated as a ring, then $R[f^{-1}]$ is as well and we may write $R[f^{-1}] := \mathbb{Z}[u_1, \dots, u_e]$ for some nonzero elements u_i of $\mathrm{Frac}(R)$. By [Bel06, Lemma 3.1], there is a prime p such that $\mathrm{Frac}(R)$ embeds into $\mathbb{Q}_p$ in a way that sends all of the u_i into $\mathbb{Z}_p$, and 6 is a unit in $\mathbb{Z}_p$ (in particular, this last condition yields that $p \geq 5$). Thus, we obtain a map $\operatorname{Spec} \mathbb{Z}_p \longrightarrow \operatorname{Spec} R[f^{-1}] \longrightarrow U$. We let $\mathcal{X}_{\mathbb{Z}_p} := \mathcal{X}_U \times_U \operatorname{Spec}(\mathbb{Z}_p)$ and let $\Phi_{\mathbb{Z}_p}$ be the base extension of Φ_U to an endomorphism of $\mathcal{X}_{\mathbb{Z}_p}$. The prime (p) in $\mathbb{Z}_p$ pulls back to a prime $\mathfrak{q}$ of $R[f^{-1}]$, so there is an isomorphism between $R[f^{-1}]/\mathfrak{q}$ and $\mathbb{Z}_p/(p)$. The fiber of $\mathcal{X}_U$ is geometrically irreducible at $\mathfrak{q}$ by Proposition 4.3, so it follows that the fiber of $\mathcal{X}_{\mathbb{Z}_p}$ at (p) is geometrically irreducible as well. Since the properties of being quasiprojective, smooth, and unramified are all preserved by base extension (see Propositions VI.3.5 and VII.1.7 of [AK70]), our proof is complete (note that the embedding of $R[f^{-1}]$ into $\mathbb{Z}_p$ automatically extends α to a section $\operatorname{Spec}(\mathbb{Z}_p) \longrightarrow \mathcal{X}_{\mathbb{Z}_p}$). $\square$

For the sake of simplifying the notation, we let $\mathcal{X} := \mathcal{X}_{\mathbb{Z}_p}$ and let Φ denote the $\mathbb{Z}_p$-endomorphism $\Phi_{\mathbb{Z}_p}$ of $\mathcal{X}_{\mathbb{Z}_p}$ constructed in Proposition 4.4. Also, we use α to denote the section $\operatorname{Spec}(\mathbb{Z}_p) \longrightarrow \mathcal{X}(\mathbb{Z}_p)$ induced in Proposition 4.4; i.e. $\alpha \in \mathcal{X}(\mathbb{Z}_p)$. Finally, we use $\mathcal{V} = \mathcal{V}_{\mathbb{Z}_p}$ to denote the $\mathbb{Z}_p$-scheme which is the Zariski closure in $\mathcal{X}$ of the original subvariety V of X.

Since the special fiber $\overline{\mathcal{X}}$ of $\mathcal{X}$ has finitely many $\mathbb{F}_p$ points, some iterate of α under Φ is in a periodic residue class modulo p. At the expense of replacing α by a suitable iterate under Φ, we may assume that the residue class of α is Φ-periodic, say of period N (note that replacing α by one of its iterates under Φ will not change the conclusion of Theorem 4.1). For each $j = 0, \dots, N-1$, we let $\vec{\alpha_j} := \iota_j(\Phi^j(\alpha)) \in \mathbb{Z}_p^g$, where ι_j^{-1} is the analytic bijection (defined as in Section 2) between $\mathbb{Z}_p^g$ and the set of points of $\mathcal{X}(\mathbb{Z}_p)$ which have the same reduction modulo p as $\Phi^j(\alpha)$.

Fix $j \in \{0, \dots, N-1\}$. Let $\mathcal{F}_j : \mathbb{Z}_p^g \longrightarrow \mathbb{Z}_p^g$ be the analytic function constructed in Proposition 2.2 corresponding to Φ^N and to the residue class of $\Phi^j(\alpha)$; this function satisfies

$$\iota_j(\Phi^N(\Phi^j(\alpha))) = \mathcal{F}_j(\vec{\alpha_j}). \tag{4.4.1}$$

As proved in Proposition 2.6.1, there exists a positive integer M_j such that

$$\mathcal{F}_j^{M_j}(\vec{\beta}) \equiv \vec{\beta} \pmod{p}, \tag{4.4.2}$$

for each $\vec{\beta} \in \mathbb{Z}_p^g$. Let $\ell \in \{0, \dots, M_j - 1\}$ be fixed. Iterating (4.4.1) yields

$$\iota_j\left(\Phi^{N(M_j k + \ell) + j}(\alpha)\right) = \mathcal{F}_j^{M_j k}(\mathcal{F}_j^{\ell}(\vec{\alpha_j})) \tag{4.4.3}$$

for each $k \in \mathbb{N}$. Using (4.4.2) (together with Remark 2.3) along with the fact that $p \geq 5$, Theorem 3.3 implies that for each $j = 0, \dots, N-1$ and for each $\ell = 0, \dots, M_j - 1$, there exists an analytic function $U_{j,\ell} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p^g$ such that

$$U_{j,\ell}(0) = \mathcal{F}_j^{\ell}(\vec{\alpha_j}) \in \mathbb{Z}_p^g \tag{4.4.4}$$

and

$$U_{j,\ell}(z+1) = \mathcal{F}_j^{M_j}(U_{j,\ell}(z)), \tag{4.4.5}$$

for each $z \in \mathbb{Z}_p$. By (4.4.4) and (4.4.5), we thus obtain

$$U_{j,\ell}(k) = \mathcal{F}_j^{M_j k}(\mathcal{F}_j^{\ell}(\vec{\alpha_j})),$$

for each $k \in \mathbb{N}$. Hence, (4.4.3) gives

$$U_{j,\ell}(k) = \iota_j\left(\Phi^{N(M_j k+\ell)+j}(\alpha)\right), \tag{4.4.6}$$

for each $k \in \mathbb{N}$. Then for each polynomial $h \in \mathbb{Z}_p[x_1, \dots, x_M]$ in the vanishing ideal of $\mathcal{V}$, the analytic function $h \circ \iota_j^{-1} \circ U_{j,\ell}$ defined on $\mathbb{Z}_p$ has infinitely many zeros $k \in \mathbb{Z}_p$ if and only if it vanishes identically (see [Rob00, Section 6.2.1]). Thus, for each $j = 0, \dots, N-1$ and each $\ell = 0, \dots, M_j - 1$, either

$$\mathcal{V}(\mathbb{Z}_p) \cap \mathcal{O}_{\Phi^{NM_j}}(\Phi^{N\ell+j}(\alpha)) \text{ is finite,}$$

or

$$\mathcal{O}_{\Phi^{NM_j}}(\Phi^{N\ell+j}(\alpha)) \subset \mathcal{V}(\mathbb{Z}_p).$$

This concludes the proof of Theorem 4.1. □

Now we extend the proof of Theorem 4.1 to cover the case of non-smooth varieties X, and thus prove our main result.

Proof of Theorem 1.3. First we show that it suffices to assume X is irreducible. Indeed, since Φ is étale, it permutes the irreducible components of X; hence, there exists a positive integer N such that for each irreducible component Y of X, the restriction of Φ^N on Y is an étale endomorphism of Y. For each $\ell = 0, \dots, (N-1)$, we let Z_ℓ be an irreducible component of X containing $\Phi^\ell(\alpha)$. Then for each $\ell = 0, \dots, (N-1)$ we have

$$V(\mathbb{C}) \cap \mathcal{O}_{\Phi^N}(\Phi^\ell(\alpha)) = (V \cap Z_\ell)(\mathbb{C}) \cap \mathcal{O}_{\Phi^N}(\Phi^\ell(\alpha)).$$

Since $\mathcal{O}_{\Phi^N}(\Phi^\ell(\alpha)) \subset Z_\ell$ and Z_ℓ is irreducible, we are done.

We proceed now by induction on $\dim(X)$. If $\dim(X) = 0$, there is nothing to prove.

Assume $\dim(X) = d \geq 1$, and that our result holds for all varieties of dimension less than d. As shown above, we may assume X is irreducible. An étale map sends smooth points into smooth points, and non-smooth points into non-smooth points (because it induces an isomorphism on the tangent space at each point). If α (and therefore $\mathcal{O}_\Phi(\alpha)$) is in the smooth locus X_{smooth} of X, then Theorem 4.1 finishes our proof because X_{smooth} is also irreducible. If $\mathcal{O}_\Phi(\alpha)$ is contained in $X_1 := X \setminus X_{\text{smooth}}$, then the inductive hypothesis finishes our proof, because $\dim(X_1) < d$ and the restriction of Φ to X_1 is étale, since the base extension of an étale morphism is étale (see [AK70, VI.4.7.(iii)]). □

5. Applications

We prove a Mordell-Lang type statement for automorphisms of any Noetherian integral scheme, which has several interesting consequences.

First, we define the *full* orbit of a point $\alpha \in X(\mathbb{C})$ under an automorphism $\Phi : X \longrightarrow X$ as the set

$$\overline{\mathcal{O}}_\Phi(\alpha) := \{\Phi^n(\alpha) : n \in \mathbb{Z}\}.$$

Theorem 5.1. *Let X be any quasiprojective variety defined over $\mathbb{C}$, and let $\Phi : X \longrightarrow X$ be an automorphism. Then for each $\alpha \in X(\mathbb{C})$, and for each subvariety $V \subset X$, the intersection $V(\mathbb{C}) \cap \overline{\mathcal{O}}_\Phi(\alpha)$ is a union of at most finitely many points and at most finitely many full orbits of the form $\overline{\mathcal{O}}_{\Phi^k}(\Phi^\ell(\alpha))$, for some positive integers k and ℓ.*

Proof. Because Φ is étale, we may apply Theorem 4.1 and derive that the intersection $\mathcal{O}_\Phi(\alpha) \cap V(\mathbb{C})$ is a union of at most finitely many points and at most finitely many orbits of the form $\mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha))$ for some $k, \ell \in \mathbb{N}$ with $k \geq 1$. Same conclusion holds if we intersect V with the orbit $\mathcal{O}_{\Phi^{-1}}(\alpha)$. So, in order to prove Theorem 5.1 it suffices to show the following Claim.

Claim 5.2. *Let Y be any quasiprojective variety defined over a field K of arbitrary characteristic, let $\Psi : Y \longrightarrow Y$ be any automorphism, let $\beta \in Y(K)$, and let W be the Zariski closure of $\mathcal{O}_\Psi(\beta)$. Then W contains $\overline{\mathcal{O}}_\Psi(\beta)$.*

Proof of Claim 5.2. For each $n \in \mathbb{N}$, we let $W_n := \Psi^n(W)$. Then W_n is the Zariski closure of the set of all $\Psi^m(\beta)$ for $m \geq n$. Hence $W_{n+1} \subset W_n$ for all $n \in \mathbb{N}$ because W_{n+1} is the Zariski closure of $\mathcal{O}_\Phi(\Phi^{n+1}(\beta)) := \{\Phi^m(\beta) : m \geq n+1\}$, and W_n contains already $\mathcal{O}_\Phi(\Phi^{n+1}(\beta))$. Since there is no infinite descending chain of closed subvarieties, we conclude that there exists $N \in \mathbb{N}$ such that $W_{N+1} = W_N$. This yields that $\Psi^{N+1}(W) = \Psi^N(W)$, and using the fact that Ψ is an automorphism, we conclude that $\Psi(W) = W$. In particular, this shows that $\overline{\mathcal{O}}_\Psi(\beta) \subset W$, as desired. □

We apply the conclusion of Claim 5.2 to any automorphism Φ^k (for some nonzero integer k) and to any point $\Phi^\ell(\alpha)$ (for some integer ℓ) such that $\mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha)) \subset V$; this yields the conclusion of Theorem 5.1. □

Special cases of Theorem 5.1 that have been previously treated include the following:

(i) X is any commutative algebraic group, Φ is the translation-by-P-map on X, where $P \in X(\mathbb{C})$, and $\alpha = 0 \in X(\mathbb{C})$ (this is a conjecture by Lang [Lan83], which was first proved by Cutkosky and Srinivas in [CS93, Theorem 7]). In particular, when X is a semiabelian variety, we obtain the case of cyclic groups in the classical Mordell-Lang conjecture (proved by Faltings [Fal94] and Vojta [Voj96]).

(ii) Φ is any automorphism of an affine variety X (this was proved by Bell in [Bel06]).

(iii) Φ is any automorphism of projective space (this was proved by Denis in [Den94]).

It would be interesting to have a theorem describing the intersection of a subvariety $V \subset X$ with a *grand orbit* of an étale map $\Phi : X \longrightarrow X$. The *grand orbit* of a point α consists of all points in $\mathcal{O}_\Phi(\alpha)$ along with all points β for which there exists $n \in \mathbb{N}$ such that $\Phi^n(\beta) = \alpha$. Although our current techniques are not sufficient to treat this more general problem, it seems natural to ask the following question, which can be seen as a dynamical analogue of McQuillan's theorem [McQ95] on the intersection of a subvariety of a semiabelian variety with the divisible hull of a finitely generated group.

Question 5.3. *Let X be a quasiprojective variety defined over $\mathbb{C}$, let $\Phi : X \longrightarrow X$ be a étale morphism, let $\alpha \in X(\mathbb{C})$, and let V be a subvariety of X. If the grand orbit of α under Φ intersects V in a Zariski dense subset, then must V be Φ-preperiodic?*

Theorem 5.1 also answers a question first posed in [KRS05, Question 11.6]. The following concept was introduced in [KRS05, Definition 3.6] (see also [CS93, Section 5]).

Definition 5.4. *Let S be an infinite set of closed points of an integral scheme X. Then we say that S is* critically dense *if every infinite subset of S has Zariski closure equal to X.*

The following result provides a positive answer to Keeler, Rogalski and Stafford's problem from [KRS05, Question 11.6].

Corollary 5.5. *If X is an irreducible quasiprojective variety over a field of characteristic 0, and $\Phi : X \longrightarrow X$ is an automorphism, then every dense orbit $\{\Phi^i(\alpha) : i \in \mathbb{Z}\}$ is critically dense.*

Proof. Theorem 5.1 yields that any closed subvariety $V \subset X$ containing infinitely many points of $\overline{\mathcal{O}}_\Phi(\alpha)$ must contain a set of the form $\overline{\mathcal{O}}_{\Phi^k}(\Phi^\ell(\alpha))$ for some $k \geq 1$. So,

$$\overline{\mathcal{O}}_\Phi(\alpha) \subset \bigcup_{i=0}^{k-1} \Phi^i(V).$$

Because we assumed that $\overline{\mathcal{O}}_\Phi(\alpha)$ is Zariski dense in X, we conclude that

$$X \subset \bigcup_{i=0}^{k-1} \Phi^i(V).$$

Now, if V is a proper subvariety of X, then $\dim(V) < \dim(X)$ (since X is an irreducible variety), and so, $\bigcup_{i=0}^{k-1} \Phi^i(V)$ is also a proper subvariety of X. This is a contradiction with the assumption that $\overline{\mathcal{O}}_\Phi(\alpha)$ is Zariski dense in X. Therefore, $\overline{\mathcal{O}}_\Phi(\alpha)$ is indeed critically dense. $\square$

A similar argument proves our Corollary 1.4.

As noted in the introduction Zhang [Zha06] has conjectured that if $f : X \longrightarrow X$ is what he calls a "polarizable" map defined over a number field, then some point $X(K)$ has a dense orbit. While automorphisms are not polarizable in general, there are examples of automorphisms of varieties X for which *every* nonpreperiodic point of X has a dense orbit. We describe a particular family of examples below.

Example 5.6. In [Sil91], Silverman studies a family of $K3$ surfaces X which have infinitely many automorphisms. He considers a group of automorphisms $\mathcal{A}$ generated by involutions σ_1, σ_2 such that $\sigma_1^2 = \sigma_2^2 = \mathrm{Id}$ and $\sigma_1\sigma_2$ has infinite order. Silverman defines the *chain* containing a point $\alpha \in X(\mathbb{C})$ as the set of all $\tau\alpha$ where $\tau \in \mathcal{A}$ and shows that any infinite chain is Zariski dense in X (this is done by showing that there are no curves in X that are preperiodic under the action of $\sigma_1\sigma_2$). Since the chain containing a point α is simply the union of the orbit of α under the action of $\sigma_1\sigma_2$ with the orbit of $\sigma_1\alpha$ under the action of $\sigma_1\sigma_2$ it follows from Corollary 1.4, that any infinite subset of a chain is Zariski dense in X. In particular, the orbit of any point $\alpha \in X(\mathbb{C})$ under the action of $\sigma_1\sigma_2$ is critically dense. It also follows from Theorem 5.1 that for any subvariety V of X and any point $\alpha \in X(\mathbb{C})$, the set of $\tau \in \mathcal{A}$ such that $\tau(\alpha) \in V$ is a union of at most finitely many cosets of subgroups of $\mathcal{A}$.

References

[AK70] A. Altman and S. Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics, Vol. 146, Springer-Verlag, Berlin, 1970.

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Bel06] J. P. Bell, *A generalised Skolem-Mahler-Lech theorem for affine varieties*, J. London Math. Soc. (2) **73** (2006), no. 2, 367–379.

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[BGKT] R. L. Benedetto, D. Ghioca, P. Kurlberg, and T. J. Tucker, *The dynamical Mordell-Lang conjecture*, submitted for publication, 2007, available online at `http://arxiv.org/abs/0712.2344`.

[Bou06] N. Bourbaki, *Éléments de mathématique. Algèbre commutative. Chapitres 8 et 9*, Springer, Berlin, 2006, Reprint of the 1983 original.

[CS93] S. D. Cutkosky and V. Srinivas, *On a problem of Zariski on dimensions of linear systems*, Ann. of Math. (2) **137** (1993), no. 3, 531–559.

[Den94] L. Denis, *Géométrie et suites récurrentes*, Bull. Soc. Math. France **122** (1994), no. 1, 13–27.

[Fal94] G. Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., no. 15, Academic Press, San Diego, CA, 1994, pp. 175–182.

[GT09] D. Ghioca and T. J. Tucker, *Periodic points, linearizing maps, and the dynamical Mordell-Lang problem*, J. Number Theory **129** (2009), no. 6, 1392–1403.

[GTZ08] D. Ghioca, T. J. Tucker, and M. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math. **171** (2008), no. 2, 463–483.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.

[HY83] M. Herman and J.-C. Yoccoz, *Generalizations of some theorems of small divisors to non-archimedean fields*, Geometric dynamics (Rio de Janeiro, 1981), Lecture Notes in Math., no. 1007, Springer-Verlag, Berlin, 1983, pp. 408–447.

[KRS05] D. S. Keeler, D. Rogalski, and J. T. Stafford, *Naïve noncommutative blowing up*, Duke Math. J. **126** (2005), no. 3, 491–546.

[Lan83] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York, 1983.

[Lec53] C. Lech, *A note on recurring series*, Ark. Mat. **2** (1953), 417–421.

[Mah35] K. Mahler, *Eine arithmetische Eigenshaft der Taylor-Koeffizienten rationaler Funktionen*, Proc. Kon. Nederlandsche Akad. v. Wetenschappen **38** (1935), 50–60.

[Mah58] ———, *An interpolation series for continuous functions of a p-adic variable*, J. Reine Angew. Math. **199** (1958), 23–34.

[Mah61] ———, *A correction to the paper "an interpolation series for continuous functions of a p-adic variable"*, J. Reine Angew. Math. **208** (1961), 70–72.

[Mat86] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1986, Translated from the Japanese by M. Reid.

[McQ95] M. McQuillan, *Division points on semi-abelian varieties*. Invent. Math. **120** (1995), no. 1, 143–159.

[Ray83a] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), no. 1, 207–233.

[Ray83b] ———, *Sous-variétés d'une variété abélienne et points de torsion*, Arithmetic and geometry, vol. I, Progr. Math., vol. 35, Birkhäuser, Boston, MA, 1983, pp. 327–352.

[RL03] J. Rivera-Letelier, *Dynamique des fonctions rationnelles sur des corps locaux*, Astérisque (2003), no. 287, 147–230, Geometric methods in dynamics. II.

[Rob00] A. M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000.

[Sha77] I. R. Shafarevich, *Basic algebraic geometry*, study ed., Springer-Verlag, Berlin, 1977, Translated from the Russian by K. A. Hirsch, Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974.

[Sil91] J. H. Silverman, *Rational points on $K3$ surfaces: a new canonical height*, Invent. Math. **105** (1991), no. 2, 347–373.

[Sko34] T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, C. r. 8 congr. scand. à Stockholm (1934), 163–188.

[Ull98] E. Ullmo, *Positivité et discrétion des points algébriques des courbes*, Ann. of Math. (2) **147** (1998), no. 1, 167–179.

[vdDS84] L. van den Dries and K. Schmidt, *Bounds in the theory of polynomial rings over fields. A nonstandard approach*, Invent. Math. **76** (1984), no. 1, 77–91.

[Voj96] P. Vojta, *Integral points on subvarieties of semiabelian varieties. I*, Invent. Math. **126** (1996), no. 1, 133–181.

[Zha98] S. Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), no. 1, 159–165.

[Zha06] S. Zhang, *Distributions in Algebraic Dynamics*, Survey in Differential Geometry, vol. 10, International Press, 2006, pp. 381–430.

Jason Bell, Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6,

E-mail address: `jpb@math.sfu.ca`

Dragos Ghioca, Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2
E-mail address: dghioca@math.ubc.ca

Thomas Tucker, Department of Mathematics, Hylan Building, University of Rochester, Rochester, NY 14627
E-mail address: ttucker@math.rochester.edu