Math. Ann. (2012) 352:1–26
DOI 10.1007/s00208-010-0621-4

Mathematische Annalen

A case of the dynamical Mordell–Lang conjecture

Robert L. Benedetto · Dragos Ghioca · Pär Kurlberg · Thomas J. Tucker

With an appendix by Umberto Zannier

Received: 16 April 2010 / Revised: 5 November 2010 / Published online: 24 December 2010

Abstract We prove a special case of a dynamical analogue of the classical Mordell–Lang conjecture. Specifically, let φ be a rational function with no periodic critical points other than those that are totally invariant, and consider the diagonal action of φ on $(\mathbb{P}^1)^g$. If the coefficients of φ are algebraic, we show that the orbit of a point outside the union of the proper preperiodic subvarieties of $(\mathbb{P}^1)^g$ has only finite intersection with any curve contained in $(\mathbb{P}^1)^g$. We also show that our result holds for indecomposable polynomials φ with coefficients in $\mathbb{C}$. Our proof uses results from p-adic dynamics together with an integrality argument. The extension to polynomials defined over $\mathbb{C}$ uses the method of specialization coupled with some new results of Medvedev and Scanlon for describing the periodic plane curves under the action of (φ, φ) on $\mathbb{A}^2$.

Mathematics Subject Classification (2000) Primary 14G25; Secondary 37F10 · 37P55

R. L. Benedetto
Department of Mathematics, Amherst College, Amherst, MA 01002, USA
e-mail: rlb@math.amherst.edu

D. Ghioca
Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
e-mail: dghioca@math.ubc.ca

P. Kurlberg (✉)
Department of Mathematics, KTH, 100 44 Stockholm, Sweden
e-mail: kurlberg@math.kth.se

T. J. Tucker
Department of Mathematics, University of Rochester, Rochester, NY 14627, USA
e-mail: ttucker@math.rochester.edu

1 Introduction

Let X be a variety over the complex numbers $\mathbb{C}$, let $\Phi : X \longrightarrow X$ be a morphism, and let V be a subvariety of X. For any integer $m \geq 0$, denote by Φ^m the mth iterate $\Phi \circ \cdots \circ \Phi$, with Φ^0 denoting the identity map. For any point $\alpha \in X$, its orbit under Φ is the set of all $\Phi^n(\alpha)$ for $n \in \mathbb{N}$. 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 $k \geq 1$ is the period of W (the smallest positive integer m for which $\Phi^m(W) \subset W$), then $\Phi^{nk+\ell}(\alpha) \in W(\mathbb{C}) \subset V(\mathbb{C})$ for all integers $n \geq 0$. In other words, if V contains a periodic subvariety W which meets the orbit of α under Φ, then there are infinitely many integers $n \geq 0$ such that $\Phi^n(\alpha) \in V$. It is natural to ask if the converse statement holds: if there exist infinitely many $n \geq 0$ such that $\Phi^n(\alpha) \in V$, must V then contain a periodic subvariety which meets the orbit of α under Φ? More precisely, given $\alpha \in X(\mathbb{C})$, if there are infinitely many integers $m \geq 0$ such that $\Phi^m(\alpha) \in V(\mathbb{C})$, are there necessarily integers $k \geq 1$ and $\ell \geq 0$ such that $\Phi^{nk+\ell}(\alpha) \in V(\mathbb{C})$ for all integers $n \geq 0$? In 2007 two of the authors proposed the following Conjecture (see [12,14]).

Conjecture 1.1 (*The cyclic case of the Dynamical Mordell–Lang Conjecture*) *Let X be a quasiprojective variety defined over $\mathbb{C}$, let Φ be an endomorphism of X, let $V \subset X$ be a closed subvariety, and let $\alpha \in X(\mathbb{C})$ be an arbitrary point. Then the set of integers $n \in \mathbb{N}$ such that $\Phi^n(\alpha) \in V(\mathbb{C})$ is a union of finitely many arithmetic progressions $\{nk + \ell\}_{n\in\mathbb{N}}$ for some nonnegative integers k and ℓ.*

Note that if Conjecture 1.1 holds for a given map Φ, variety V, and non-preperiodic point α, and if V intersects the Φ-orbit of α in infinitely many points, then V must contain a positive-dimensional subvariety W that is periodic under Φ. Indeed, the conjecture says that there are integers $k \geq 1$ and $\ell \geq 0$ such that $\Phi^{nk+\ell}(\alpha)$ lies on V for all $n \geq 0$. Since α is not preperiodic, the set $S = \{\Phi^{nk+\ell}(\alpha)\}_{n\geq 0}$ is infinite, and therefore its Zariski closure V_0 contains some positive-dimensional component W. Thus, W is positive-dimensional and is mapped into itself by some iterate of Φ, as claimed.

Note also that the arithmetic progressions for which $k = 0$ are singletons, so that Conjecture 1.1 allows not only infinite arithmetic progressions but also finitely many extra points. We view this conjecture as an analogue of the classical Mordell–Lang conjecture for arithmetic dynamics, with cyclic groups replaced by single orbits. Indeed, the classical Mordell–Lang conjecture describes the intersection between a subvariety V of a semiabelian variety X defined over $\mathbb{C}$ and a finitely generated subgroup Γ of $X(\mathbb{C})$. If Γ is a cyclic subgroup generated by some element $\gamma \in X(\mathbb{C})$, then Γ may be viewed as the orbit of the identity 0 of X under the cyclic group of automorphisms of X generated by the translation-by-γ map τ_γ on X.

In fact, the above reformulation of the cyclic case of the classical Mordell–Lang conjecture follows from a positive answer to our Conjecture 1.1. Indeed, assume V contains infinitely many points of the form $n\gamma$ with $n \in \mathbb{Z}$; without loss of generality we may assume there are infinitely many $n \in \mathbb{N}$ such that $n\gamma \in V(\mathbb{C})$. Then by Conjecture 1.1 applied to the map $\Phi = \tau_\gamma$ and the point $\alpha = 0$, we would conclude that there exist positive integers k and ℓ such that $(nk + \ell) \cdot \gamma \in V(\mathbb{C})$ for all $n \in \mathbb{N}$. In particular, this means that $-\ell\gamma + V$ contains the Zariski closure H of the set $\{nk\gamma : n \in \mathbb{N}\}$. It is easy to see that H is fixed by $\tau_{k\gamma}$, and thus H contains the entire set $\{nk\gamma : n \in \mathbb{Z}\}$. Hence V contains the entire coset $(\ell + k\mathbb{Z}) \cdot \gamma$ of the cyclic subgroup generated by $k\gamma$, as claimed.

Conjecture 1.1 is known to be true in many special cases. When X is a semiabelian variety and Φ is a multiplication-by-m map $[m]$, it follows from the Mordell–Lang conjecture, which is a theorem due to Faltings [11] and Vojta [34]. Indeed, if we let Γ be the cyclic subgroup of $X(\mathbb{C})$ spanned by α, then using the positive answer to the classical Mordell–Lang conjecture for the subvariety V of X and the subgroup Γ of $X(\mathbb{C})$, we conclude that there exist finitely many (doubly infinite) arithmetic progressions $\{nk + \ell\}_{n \in \mathbb{Z}}$ (for given $k, \ell \in \mathbb{N}$) such that $(nk + \ell) \cdot \alpha \in V(\mathbb{C})$. Turning to $\Phi = [m]$ specifically, we must determine, for each arithmetic progression $\{nk + \ell\}_{n \in \mathbb{Z}}$ above, the set of integers r for which $m^r \equiv \ell \pmod{k}$. This set is obviously a union of finitely many arithmetic progressions, thus proving Conjecture 1.1 when X is a semiabelian variety and $\Phi = [m]$.

More generally, Conjecture 1.1 holds when Φ is any endomorphism of a semiabelian variety (see [12]). Denis [9] treated the conjecture 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. Bell [5] later solved the problem completely in the case of automorphisms of affine varieties. Building on the ideas from [5], the case when Φ is any étale endomorphism of any quasiprojective variety was completely solved in [6].

One may even ask a *higher rank* version of Conjecture 1.1 by replacing the single action of Φ with the action of a semigroup of endomorphisms of X spanned by finitely many commuting endomorphisms $\Phi_1, \ldots, \Phi_r$. This leads to a more general Dynamical Mordell–Lang Conjecture which was studied in the case X is a semiabelian variety in [15]. In addition, in [14] and [16], this higher rank Dynamical Mordell–Lang problem was completely solved in the case that $X = \mathbb{A}^r$ and V is a line, and that each map Φ_i is of the form $\Phi_i(x_1, \ldots, x_r) = (x_1, \ldots, x_{i-1}, f_i(x_i), x_{i+1}, \ldots, x_r)$ for some nonlinear polynomials $f_i \in \mathbb{C}[x]$.

In [12], a general framework for attacking Conjecture 1.1 was developed and the following special case of Conjecture 1.1 was made.

Conjecture 1.2 *Let $f_1, \ldots, f_g \in \mathbb{C}[t]$ be polynomials, let Φ be their coordinatewise action on $\mathbb{A}^g$, let $(x_1, \ldots, x_g) \in \mathbb{A}^g(\mathbb{C})$, and let V be a closed subvariety of $\mathbb{A}^g$. Then the set of integers n such that $\Phi^n(x_1, \ldots, x_g) \in V(\mathbb{C})$ is a union of finitely many arithmetic progressions.*

Conjecture 1.1 fits into Zhang's far-reaching system of dynamical conjectures [36]. Zhang's conjectures include dynamical analogues of the Manin–Mumford and Bogomolov conjectures for abelian varieties (now theorems of Raynaud [25,26], Ullmo [33], and Zhang [35]). We note that two of the authors found counterexamples to Zhang's original Dynamical Manin–Mumford and Bogomolov conjectures; a reformulation of those two conjectures will soon appear due to work of Ghioca, Tucker and Zhang [13]. Also, in [36], Zhang formulates a conjecture about the Zariski density of orbits of points under fairly general maps from a projective variety to itself. Amerik, Bogomolov, and Rovinsky [1,2] have obtained partial results towards this conjecture, using p-adic methods similar to those used in this paper. This latter conjecture of Zhang takes the following form in the case of coordinatewise polynomial actions on $\mathbb{A}^g$.

Conjecture 1.3 *Let $f_1, \ldots, f_g \in \overline{\mathbb{Q}}[t]$ be polynomials of the same degree $d \geq 2$, and let Φ be their action coordinatewise on $\mathbb{A}^g$. Then there is a point $(x_1, \ldots, x_g) \in \mathbb{A}^g(\overline{\mathbb{Q}})$ such that the orbit $\mathcal{O}_\Phi((x_1, \ldots, x_g))$ of $(x_1, \ldots, x_g)$ under Φ is Zariski dense in $\mathbb{A}^g$.*

Conjectures 1.2 and 1.3 may be thought of as complementary. Conjecture 1.3 posits that there is a point in $\mathbb{A}^g$ outside the union of the preperiodic proper subvarieties of $\mathbb{A}^g$ under the action of Φ, while Conjecture 1.2 asserts if a point α lies outside this union of preperiodic subvarieties, then the orbit of α under Φ intersects any proper subvariety V of $\mathbb{A}^g$ in at most finitely many points. We also note that a stronger form of Conjecture 1.3 was proved by Medvedev and Scanlon in [23, Theorem 5.11].

In this paper, we prove Conjecture 1.2 over number fields for curves embedded in $\mathbb{A}^g$ under the diagonal action of any polynomial which has no superattracting periodic points. (A periodic point at which the derivative vanishes is said to be superattracting; see Sect. 2 for a more precise definition.) In fact, we prove the following more general statement.

Theorem 1.4 *Let $C \subset (\mathbb{P}^1)^g$ be a curve defined over $\overline{\mathbb{Q}}$, and let $\Phi := (\varphi, \ldots, \varphi)$ act on $(\mathbb{P}^1)^g$ coordinatewise, where $\varphi \in \overline{\mathbb{Q}}(t)$ is a rational function with no superattracting periodic points other than exceptional points. Then for each point $(x_1, \ldots, x_g) \in (\mathbb{P}^1)^g(\overline{\mathbb{Q}})$, the set of integers n such that $\Phi^n(x_1, \ldots, x_g) \in C(\overline{\mathbb{Q}})$ is a union of finitely many arithmetic progressions.*

See Sect. 2 for a definition of exceptional points. In particular, if φ is a polynomial of degree d, the hypothesis on superattracting points in Theorem 1.4 is satisfied if none of the at most $d-1$ critical points φ (i.e. points $\alpha \in \mathbb{C}$ such that $\varphi'(\alpha) = 0$) is periodic. We note that this condition holds for *almost all* polynomials in the following sense: the set of polynomials with periodic critical points is a countable union of proper subvarieties in the space of all complex polynomials of fixed degree; thus, over the uncountable field $\mathbb{C}$, a generic polynomial has no such points.

Using recent results of Medvedev and Scanlon [23] from model theory, we will extend Theorem 1.4 to the complex numbers, at least under the action of indecomposable polynomials. (See Definition 7.1.) Our method from Sect. 7 also extends to the case of arbitrary polynomials with complex coefficients, as long as they do not have superattracting periodic points other than exceptional points (see Remark 7.10).

Theorem 1.5 *Let $\varphi \in \mathbb{C}[t]$ be an indecomposable polynomial with no periodic superattracting points other than exceptional points, and let Φ be its diagonal action on $\mathbb{A}^g$ (for some $g \geq 1$). Then for each point $P \in \mathbb{A}^g(\mathbb{C})$, and for each curve $C \subset \mathbb{A}^g(\mathbb{C})$, the set of integers n such that $\Phi^n(P) \in C(\mathbb{C})$ is a union of finitely many arithmetic progressions.*

When the function φ is a quadratic polynomial, we can prove a similar result for subvarieties of any dimension.

Theorem 1.6 *Let $V \subset \mathbb{A}^g$ be a subvariety defined over $\overline{\mathbb{Q}}$, and let $\Phi := (f, \dots, f)$ act on $\mathbb{A}^g$ coordinatewise, where $f \in \overline{\mathbb{Q}}[t]$ is a quadratic polynomial with no periodic superattracting points in $\overline{\mathbb{Q}}$. Then for each point $(x_1, \dots, x_g) \in \mathbb{A}^g(\overline{\mathbb{Q}})$, the set of integers n such that $\Phi^n(x_1, \dots, x_g) \in V(\overline{\mathbb{Q}})$ is a union of finitely many arithmetic progressions.*

For quadratic polynomials over the rational numbers, we can remove the hypothesis on superattracting points and obtain a stronger result.

Theorem 1.7 *Let $V \subset \mathbb{A}^g$ be a subvariety defined over $\mathbb{Q}$, and let $\Phi := (f, \dots, f)$ act on $\mathbb{A}^g$ coordinatewise, where $f \in \mathbb{Q}[t]$ is a quadratic polynomial. Then for each point $(x_1, \dots, x_g) \in \mathbb{A}^g(\mathbb{Q})$, the set of integers n such that $\Phi^n(x_1, \dots, x_g) \in V(\overline{\mathbb{Q}})$ is a union of finitely many arithmetic progressions.*

Using results of Jones [18], we can prove the corresponding result for maps of the form $\Phi = (f_1, \dots, f_g)$, without the restriction that $f_i = f_j$, if each f_j is of the form $f_j(t) = t^2 + c_j$ with $c_j \in \mathbb{Z}$.

Theorem 1.8 *Let $V \subset \mathbb{A}^g$ be a subvariety defined over $\mathbb{Q}$, and let $\Phi := (f_1, \dots, f_g)$ act on $\mathbb{A}^g$ coordinatewise, where $f_i(t) = t^2 + c_i$ with $c_i \in \mathbb{Z}$ for each i. Then for each point $(x_1, \dots, x_g) \in \mathbb{Z}^g$, the set of integers n such that $\Phi^n(x_1, \dots, x_g) \in V(\overline{\mathbb{Q}})$ is a union of finitely many arithmetic progressions.*

Our method of proof involves an interplay between arithmetic geometry and p-adic dynamics. It is based in part on a nonlinear analogue of Skolem's technique [32] (later extended by Mahler [22] and Lech [21]) for treating linear recurrence sequences of complex numbers. The starting point of Skolem's approach is to find a suitable prime p in order to obtain a p-adic analytic parametrization for the elements in a linear recurrence sequence. When the sequence consists of algebraic numbers, it turns out that one may find a p-adic analytic parametrization of the sequence for all but finitely many primes p. However, unlike in the linear case, finding a suitable prime p in our case is more difficult and involves the application of Silverman's dynamical Siegel theorem for $\mathbb{P}^1$ [31]; see Sect. 4. We also use Rivera-Letelier's classification [27] of dynamics on p-adic Fatou sets to deal with the nonlinearity; see Sect. 3. More precisely, we find an arithmetic progression $\mathcal{S}$ of integers, a prime p, a p-adic disk U containing $\mathcal{S}$, and a p-adic analytic map $\theta : U \to \mathbb{A}^g(\mathbb{C}_p)$ such that on the one hand, $\Phi^m(\alpha)$ lies on V for infinitely many $m \in \mathcal{S}$, but on the other hand, $\theta(m) = \Phi^m(x_1, \dots, x_g)$ for *every* $m \in \mathcal{S}$. Then, for any polynomial F that vanishes on V, we have $F(\theta(m)) = 0$ for infinitely many m. Since the zeros of a nontrivial p-adic analytic function are isolated, $F \circ \theta$ must vanish at *all* $m \in \mathcal{S}$. We use Silverman's result to prove the existence of an integer ℓ and a place p at which $\varphi^\ell(x_i)$ is in a p-adic quasiperiodicity disk for each i. (A quasiperiodicity disk is a periodic residue class on which the derivative has absolute value equal to one; see Definition 3.1.) Then, the existence of $\mathcal{S}$ and θ follows from Rivera-Letelier's work.

The Skolem–Mahler–Lech technique has also appeared in other work done on this subject. Bell's [5] and Denis's [9] work on automorphisms may be viewed as algebro-geometric realizations of the Skolem–Mahler–Lech theorem. Evertse, Schlickewei, and Schmidt [10] have given a strong quantitative version of the Skolem–Mahler–Lech theorem. It may be possible to use their result to give quantitative versions of the theorems of this paper.

The same Skolem–Mahler–Lech technique was used again in [12] to prove the Dynamical Mordell–Lang Conjecture for endomorphisms of a semiabelian variety and in [6] to prove the Dynamical Mordell–Lang conjecture for unramified endomorphisms Φ of quasiprojective varieties X. However, the significant novelty of our present paper is that we are able to deal with the case of a ramified endomorphism $\Phi = (\varphi, \ldots, \varphi)$ (where each φ is a rational map), as long as the ramification of φ is *not too wild*, in the sense that φ does not have superattracting periodic points. To our knowledge, the only papers in literature dealing with the ramification of the endomorphism Φ for the Dynamical Mordell–Lang Conjecture in *both* the cyclic and non-cyclic cases are [14] and [16]. In the cyclic case, however, the results of the present paper are somewhat more general, because our techniques allow the subvariety V to be an arbitrary curve, rather than a line as in [14] and [16]. For more general subvarieties, the only other result we know of is from our paper [7], in which we proved that in any counterexample to the coordinatewise cyclic case of the conjecture, the sequence of iterates n for which $\Phi^n(\alpha) \in V$ must grow extremely rapidly.

We exclude the case that the rational function φ has superattracting points because we have been unable, thus far, to extend the method of Skolem–Mahler–Lech to this situation. Although φ is locally conjugate to $z \mapsto z^m$ in a neighborhood of such a point (see [27, Proposition 3.3]), the conjugation is still not amenable to our proof, unlike Rivera-Letelier's more powerful conjugation to $z \mapsto z + k$ on subsets of quasi-periodicity disks (see Sect. 3). While superattracting points may behave quite simply from a dynamical perspective, it is perhaps not surprising that their inherent ramification presents difficulties in the diophantine context. In the cases of endomorphisms of semiabelian varieties (see [11,12,15,34]), of automorphisms of affine varieties (see [5,9]), or of étale endomorphisms in general (see [6]), the underlying maps have no ramification.

Thus, at this point, the main obstacle to proving Conjecture 1.1 is overcoming the difficulties that ramification presents. Roughly speaking, our approach is to show that there are primes of good reduction at which the relevant Φ-orbit contains no ramified points. In Sect. 4, this is done via what is essentially a one-variable diophantine method, one which appears unlikely to generalize to higher dimensions. In the appendix, by Umberto Zannier, a result similar to but stronger than Proposition 4.2 is proved by an alternative method, using Siegel's Theorem and some local analysis of curves in $\mathbb{P}^2$. This method connects our strategy to dynamical questions about integral points on surfaces, and it suggests a possible approach to treating dynamical Mordell–Lang problems for more general maps than those studied here.

The outline of our paper is as follows. In Sect. 2 we introduce our notation. Section 3 provides necessary lemmas from p-adic dynamics, while Sect. 4 provides necessary lemmas from diophantine geometry, derived from a result of Silverman [31]. In Sect. 5, we prove Theorem 1.4, while in Sect. 6, we prove Theorems 1.6, 1.7, and 1.8. In Sect. 7, we describe the results of [23] and use them to deduce Theorem 1.5. Finally, as mentioned above, the appendix written by Umberto Zannier provides an alternative, and possibly more general, approach to some of the results of Sect. 4.

2 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, the field $\mathbb{C}_p$ will denote the completion of an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, the field of p-adic rationals. We denote by $|\cdot| := |\cdot|_p$ the usual absolute value on $\mathbb{C}_p$. Given $a \in \mathbb{C}_p$ and $r > 0$, we write $D(a, r)$ and $\overline{D}(a, r)$ for the open disk and closed disk (respectively) of radius r centered at a.

If K is a number field, we let $\mathfrak{o}_K$ be its ring of algebraic integers, and we fix an isomorphism π between $\mathbb{P}^1_K$ and the generic fibre of $\mathbb{P}^1_{\mathfrak{o}_K}$. For each nonarchimedean place v of K, we let k_v be the residue field of K at v, and for each $x \in \mathbb{P}^1(K)$, we let $x_v := r_v(x)$ be the intersection of the Zariski closure of $\pi(x)$ with the fibre above v of $\mathbb{P}^1_{\mathfrak{o}_K}$. (Intuitively, x_v is x modulo v.) This map $r_v : \mathbb{P}^1(K) \longrightarrow \mathbb{P}^1(k_v)$ is the *reduction map* at v.

If $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ is a morphism defined over the field K, then (fixing a choice of homogeneous coordinates) there are relatively prime homogeneous polynomials $F, G \in K[X, Y]$ of the same degree $d = \deg \varphi$ such that $\varphi([X, Y]) = [F(X, Y) : G(X, Y)]$. (In affine coordinates, $\varphi(t) = F(t, 1)/G(t, 1) \in K(t)$ is a rational function in one variable.) Note that by our choice of coordinates, F and G are uniquely defined up to a nonzero constant multiple. We will need the notion of good reduction of φ, first introduced by Morton and Silverman in [24].

Definition 2.1 Let K be a field, let v be a nonarchimedean valuation on K, let $\mathfrak{o}_v$ be the ring of v-adic integers of K, and let k_v be the residue field at v. Let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a morphism over K, given by $\varphi([X, Y]) = [F(X, Y) : G(X, Y)]$, where $F, G \in \mathfrak{o}_v[X, Y]$ are relatively prime homogeneous polynomials of the same degree such that at least one coefficient of F or G is a unit in $\mathfrak{o}_v$. Let $\varphi_v := [F_v, G_v]$, where $F_v, G_v \in k_v[X, Y]$ are the reductions of F and G modulo v. We say that φ has *good reduction* at v if $\varphi_v : \mathbb{P}^1(k_v) \longrightarrow \mathbb{P}^1(k_v)$ is a morphism of the same degree as φ.

If $\varphi \in K[t]$ is a polynomial, we can give the following elementary criterion for good reduction: φ has good reduction at v if and only if all coefficients of φ are v-adic integers, and its leading coefficient is a v-adic unit.

Definition 2.2 Two rational functions φ and ψ are *conjugate* if there is a linear fractional transformation μ such that $\varphi = \mu^{-1} \circ \psi \circ \mu$.

In the above definition, if φ and ψ are polynomials, then we may assume that μ is a polynomial of degree one.

Definition 2.3 If K is a field, and $\varphi \in K(t)$ is a rational function, then $z \in \mathbb{P}^1(\overline{K})$ is a *periodic point* for φ if there exists an integer $n \geq 1$ such that $\varphi^n(z) = z$. The smallest such integer n is the *period* of z, and $\lambda = (\varphi^n)'(z)$ is the *multiplier* of z. If $\lambda = 0$, then z is called *superattracting*. If $|\cdot|_v$ is an absolute value on K, and if $|\lambda|_v < 1$, then z is called *attracting*.

Let z be a periodic point of φ. If $\varphi = \mu^{-1} \circ \psi \circ \mu$, then $\mu(z)$ is a periodic point of ψ, and by the chain rule, it has the same multiplier. In particular, we can define the multiplier of a periodic point at $z = \infty$ by changing coordinates. Also by the chain rule, the multiplier of $\varphi^\ell(z)$ is the same as that of z, because $(\varphi^k)'(z) = \prod_{i=0}^{k-1}(\varphi'(\varphi^i(z))) = (\varphi^k)'(\varphi^\ell(z))$.

Whether or not z is periodic, we say z is a *ramification point* or *critical point* of φ if $\varphi'(z) = 0$. If $\varphi = \mu^{-1} \circ \psi \circ \mu$, then z is a critical point of φ if and only if $\mu(z)$ is a critical point of ψ; in particular, coordinate change can again be used to determine whether $z = \infty$ is a critical point. Note that a periodic point z is superattracting if and only if at least one of $z, \varphi(z), \varphi^2(z), \dots, \varphi^{n-1}(z)$ is critical, where n is the period of z.

Let $\varphi : V \longrightarrow V$ be a map from a variety to itself, and let $z \in V(\overline{K})$. The (*forward*) *orbit* $\mathcal{O}_\varphi(z)$ of z under φ is the set $\{\varphi^k(z) : k \in \mathbb{N}\}$. We say z is *preperiodic* if $\mathcal{O}_\varphi(z)$ is finite. If μ is an automorphism of V, and if $\varphi = \mu^{-1} \circ \psi \circ \mu$, note that $\mathcal{O}_\varphi(z) = \mu^{-1}(\mathcal{O}_\psi(\mu(z)))$.

We say z is *exceptional* if there are only finitely many points w such that $z \in \mathcal{O}_\varphi(w)$ (i.e. the backward orbit of z is finite). Of course, the image and inverse image of an exceptional point consist only of exceptional points. It is a classical result in dynamics (e.g., see [4], Theorem 4.1.2) that a morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree larger than one has at most two exceptional points. Moreover, it has exactly two if and only if φ is conjugate to the map $t \mapsto t^n$, for some integer $n \in \mathbb{Z}$; and it has exactly one if and only if φ is conjugate to a polynomial but not to any map $t \mapsto t^n$. In particular, φ has at least one exceptional point if and only if φ^2 is conjugate to a polynomial.

3 Quasiperiodicity disks in p-adic dynamics

As in [12], we will need a result on non-preperiodic points over local fields. By an *open disk in* $\mathbb{P}^1(\mathbb{C}_p)$, we will mean either an open disk in $\mathbb{C}_p$ or the complement (in $\mathbb{P}^1(\mathbb{C}_p)$) of a closed disk in $\mathbb{C}_p$. Equivalently, an open disk in $\mathbb{P}^1(\mathbb{C}_p)$ is the image of an open disk $D(0, r) \subseteq \mathbb{C}_p$ under a linear fractional transformation $\gamma \in \mathrm{PGL}(2, \mathbb{C}_p)$. Closed disks are defined similarly.

The following definition is borrowed from [27, Sect. 3.2], although we have used a simpler version that suffices for our purposes.

Definition 3.1 Let p be a prime, let $r > 0$, let $\gamma \in \mathrm{PGL}(2, \mathbb{C}_p)$, and let $U = \gamma(D(0, r))$. Let $f : U \to U$ be a function such that

$$\gamma^{-1} \circ f \circ \gamma(t) = \sum_{i \geq 0} c_i t^i \in \mathbb{C}_p[[t]],$$

with $|c_0| < r$, $|c_1| = 1$, and $|c_i| r^i \leq r$ for all $i \geq 1$. Then we say U is a *quasiperiodicity disk* for f.

The conditions on f in Definition 3.1 mean precisely that f is p-adic analytic and maps U bijectively onto U. In particular, the preperiodic points of f in U are in fact periodic. By [27, Corollaire 3.12], our definition implies that U is indeed a quasiperiodicity domain of f in the sense of [27, Définition 3.7].

The main result of this section is the following.

Theorem 3.2 *Let p be a prime and $g \geq 1$. For each $i = 1, \dots, g$, let U_i be an open disk in $\mathbb{P}^1(\mathbb{C}_p)$, and let $f_i : U_i \to U_i$ be a map for which U_i is a quasiperiodicity disk. Let Φ denote the action of $f_1 \times \cdots \times f_g$ on $U_1 \times \cdots \times U_g$, let $\alpha = (x_1, \dots, x_g) \in U_1 \times \cdots \times U_g$ be a point, and let $\mathcal{O}$ be the Φ-orbit of α. Let V be a subvariety of $(\mathbb{P}^1)^g$ defined over $\mathbb{C}_p$. Then $V(\mathbb{C}_p) \cap \mathcal{O}$ is a union of finitely many orbits of the form $\{\Phi^{nk+\ell}(\alpha)\}_{n\geq 0}$ for nonnegative integers k and ℓ.*

Note that the conclusion of Theorem 3.2 says precisely that the set of $n \in \mathbb{N}$ such that $\Phi^n(\alpha) \in V$ is a finite union of arithmetic progressions.

The proof of Theorem 3.2 relies on the following lemma from p-adic dynamics, which in turn follows from the theory of quasiperiodicity domains in [27, Sect. 3.2].

Lemma 3.3 *Let $U \subseteq \mathbb{C}_p$ be an open disk, let $f : U \to U$ be a map for which U is a quasiperiodicity disk, and let $x \in U$ be a non-periodic point. Then there exist an integer $k \geq 1$, real numbers $r > 0$ and $s \geq |k|_p$, and, for every integer $\ell \geq 0$, a bijective p-adic analytic function $h_\ell : \overline{D}(0, s) \to \overline{D}(f^\ell(x), r)$, with the following properties*:

(i) *$h_\ell(0) = f^\ell(x)$, and*
(ii) *for all $z \in \overline{D}(f^\ell(x), r)$ and $n \geq 0$, we have*

$$f^{nk}(z) = h_\ell(nk + h_\ell^{-1}(z)).$$

Proof Write $U = D(a, R)$. By [27, Proposition 3.16(2)], there is an integer $k \geq 1$ and a neighborhood $U_x \subseteq U$ of x on which f^k is (analytically and bijectively) conjugate to $t \mapsto t + k$. That is, there are radii $r, s > 0$ (with $r < R$ and $s \geq |k|_p$) and a bijective analytic function $h_0 : \overline{D}(0, s) \to \overline{D}(x, r)$ such that $f^{nk}(z) = h_0(nk + h_0^{-1}(z))$ for all $z \in \overline{D}(x, r)$ and $n \geq 0$.

For each nonnegative integer ℓ, note that f^ℓ is a bijective analytic function from $\overline{D}(x, r)$ onto $\overline{D}(f^\ell(x), r)$. Thus, if we let $h_\ell := f^\ell \circ h_0$, then h_ℓ is a bijective analytic function from $\overline{D}(0, s)$ onto $\overline{D}(f^\ell(x), r)$. Moreover, for all $z \in \overline{D}(f^\ell(x), r)$, if we let $\zeta = f^{-\ell}(z) \in \overline{D}(x, r)$, then for every $n \geq 0$,

$$f^{nk}(z) = f^\ell(f^{nk}(\zeta)) = f^\ell(h_0(nk + h_0^{-1}(\zeta))) = h_\ell(nk + h_\ell^{-1}(z)).$$

Finally, replacing $h_\ell(z)$ by $h_\ell(z + h_\ell^{-1}(f^\ell(x)))$, we can also ensure that $h_\ell(0) = f^\ell(x)$. □

We are now ready to prove Theorem 3.2.

Proof of Theorem 3.2 By applying linear fractional transformations γ_i to each U_i, we may assume without loss that each U_i is an open disk in $\mathbb{C}_p$.

For each $i = 1, \dots, g$, consider the f_i-orbit of x_i. If x_i is periodic, let $k_i \geq 1$ denote its period, and for every $\ell \geq 0$, define the power series $h_{i,\ell}$ to be the constant $f_i^\ell(x_i)$. Otherwise, choose $k_i \geq 1$ and radii $r_i, s_i > 0$ according to Lemma 3.3, along with the associated conjugating maps $h_{i,\ell}$ for each $\ell \geq 0$.

Let $k = \operatorname{lcm}(k_1, \ldots, k_g) \geq 1$. For each $\ell \in \{0, \ldots, k-1\}$ such that $V(\mathbb{C}_p) \cap \mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha))$ is finite, we can cover $V(\mathbb{C}_p) \cap \mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha))$ by finitely many singleton orbits.

It remains to consider those $\ell \in \{0, \ldots, k-1\}$ for which there is an infinite set $\mathcal{N}$ of nonnegative integers n such that $\Phi^{nk+\ell}(\alpha) \in V(\mathbb{C}_p)$. We will show that in fact, $\Phi^{nk+\ell}(\alpha) \in V(\mathbb{C}_p)$ for *all* $n \in \mathbb{N}$.

For any $|z| \leq 1$, note that $kz \in \overline{D}(0, s_i)$ for all $i = 1, \ldots, g$. Thus, it makes sense to define $\theta : \overline{D}(0, 1) \to U_1 \times \cdots \times U_g$ by

$$\theta(z) = (h_{1,\ell}(kz), \ldots, h_{g,\ell}(kz));$$

Then for all $n \geq 0$, we have

$$\theta(n) = \Phi^{nk+\ell}(\alpha),$$

because for each $i = 1, \ldots, g$, we have $k_i | k$, and therefore

$$h_{i,\ell}(nk) = h_{i,\ell}(nk + h_{i,\ell}^{-1}(f_i^\ell(x_i))) = f_i^{nk}(f_i^\ell(x_i)) = f_i^{nk+\ell}(x_i).$$

Given any polynomial F vanishing on V, the composition $F \circ \theta$ is a convergent power series on $\overline{D}(0, 1)$ that vanishes at all integers in $\mathcal{N}$. However, a nonzero convergent power series can have only finitely many zeros in $\overline{D}(0, 1)$; see, for example, [28, Sect. 6.2.1]. Thus, $F \circ \theta$ is identically zero. Therefore,

$$F(\Phi^{nk+\ell}(\alpha)) = F(\theta(n)) = 0$$

for all $n \geq 0$, not just $n \in \mathcal{N}$. This is true for all such F, and therefore $\mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha)) \subseteq V(\mathbb{C}_p)$.

The conclusion of Theorem 3.2 now follows, because $\mathcal{O}$ is the finite union of the orbits $\mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha))$ for $0 \leq \ell \leq k-1$. □

As an immediate corollary, we have the following result, which proves Conjecture 1.2 in the case that Φ is defined over $\overline{\mathbb{Q}}$ and there is a nonarchimedean place v with the following property: for each i, the rational function f_i has good reduction at v, and $\mathcal{O}_{f_i}(x_i)$ avoids all v-adic attracting periodic points.

Theorem 3.4 *Let V be a subvariety of $(\mathbb{P}^1)^g$ defined over $\mathbb{C}_p$, let $f_1, \ldots, f_g \in \mathbb{C}_p(t)$ be rational functions of good reduction on $\mathbb{P}^1$, and let Φ denote the coordinatewise action of $(f_1, \ldots, f_g)$ on $(\mathbb{P}^1)^g$. Let $\mathcal{O}$ be the Φ-orbit of a point $\alpha = (x_1, \ldots, x_g) \in (\mathbb{P}^1(\mathbb{C}_p))^g$, and suppose that for each i, the orbit $\mathcal{O}_{f_i}(x_i)$ does not intersect the residue class of any attracting f_i-periodic point. Then $V(\mathbb{C}_p) \cap \mathcal{O}$ is a union of at most finitely many orbits of the form $\{\Phi^{nk+\ell}(\alpha)\}_{n\geq 0}$ for nonnegative integers k and ℓ.*

Proof For each i, the reduction $r_p(x_i) \in \mathbb{P}^1(\overline{\mathbb{F}_p})$ is preperiodic under the reduced map $(f_i)_p$. Replacing α by $\Phi^m(\alpha)$ for some $m \geq 0$, and replacing Φ by Φ^j for some $j \geq 1$, then, we may assume that for each i, the residue class U_i of x_i is mapped to itself by f_i. By hypothesis, there are no attracting periodic points in those residue classes; thus, by [27, Proposition 4.32] (for example), U_i is a quasiperiodicity disk for f_i. Theorem 3.2 now yields the desired conclusion. □

4 Integrality arguments for arithmetic dynamical systems

In this Section, given a number field K, we will prove several lemmas needed in the proofs of Theorems 1.6 and 1.7. We will continue to work with the same reduction maps $r_v : \mathbb{P}^1(K) \longrightarrow \mathbb{P}^1(k_v)$ as in Sect. 2, where v is a finite place of K. We begin with a lemma derived from work of Silverman [31].

Lemma 4.1 *Let K be a number field, let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a morphism of degree greater than one defined over K, let $\alpha \in \mathbb{P}^1(K)$ be a point that is not preperiodic for φ, and let $\beta \in \mathbb{P}^1(K)$ be a nonexceptional point for φ. Then there are infinitely many v such that there is some positive integer n for which $r_v(\varphi^n(\alpha)) = r_v(\beta)$.*

Proof Suppose there were only finitely many such v; let S be the set of all such v, together with all the archimedean places. We may choose coordinates $[x : y]$ for $\mathbb{P}^1$ such that β is the point $[1 : 0]$. Since $[1 : 0]$ is not exceptional for φ, we see that φ^2 is not a polynomial with respect to this coordinate system. Therefore, by [31, Theorem 2.2], there are at most finitely many n such that $\varphi^n(\alpha) = [t : 1]$ for $t \in \mathfrak{o}_S$, where $\mathfrak{o}_S$ is the ring of S-integers in K. Hence, for all but finitely many integers $n \geq 0$, there is some $v \notin S$ such that $r_v(\varphi^n(\alpha)) = r_v(\beta)$; but this contradicts our original supposition. □

Proposition 4.2 *Let K be a number field, let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a morphism of degree greater than one defined over K, and let $\alpha, \beta \in \mathbb{P}^1(K)$ be points that are not preperiodic for φ. Then there are infinitely many finite places v of K such that φ has good reduction at v and such that either*

(i) *for all $m \geq 0$, $\varphi^m(\alpha)$ and $\varphi^m(\beta)$ do not lie in the residue class of any attracting φ-periodic points*; *or*

(ii) *there are integers $k \geq 1$ and $\ell \geq 0$ and attracting periodic points $\gamma_1, \gamma_2 \in \mathbb{P}^1(K_v)$ of period k such that $r_v(\varphi^\ell(\alpha)) = r_v(\gamma_1)$, $r_v(\varphi^\ell(\beta)) = r_v(\gamma_2)$, and $(\varphi^k)'(\gamma_1) = (\varphi^k)'(\gamma_2)$.*

Proof By Lemma 4.1, there are infinitely many places v of good reduction such that there is some positive integer n for which $r_v(\varphi^n(\alpha)) = r_v(\beta)$. Fix any such v. Then for any periodic point γ, the orbit of α intersects the residue class of γ if and only if the orbit of β does. Thus, if condition (i) of the Proposition fails, we can choose an integer $\ell \geq 0$ and an attracting periodic point γ_1 such that $r_v(\varphi^\ell(\alpha)) = r_v(\gamma_1)$. By [27, Proposition 3.2], γ_1 lies in the v-adic closure of the orbit of α, and hence $\gamma_1 \in \mathbb{P}^1(K_v)$.

Set $\gamma_2 = \varphi^n(\gamma_1)$; then

$$r_v(\varphi^\ell(\beta)) = r_v(\varphi^{n+\ell}(\alpha)) = r_v(\varphi^n(\gamma_1)) = r_v(\gamma_2).$$

Finally, as noted after Definition 2.3, $(\varphi^k)'(\gamma_1) = (\varphi^k)'(\gamma_2)$. □

The following result will be used in the proof of Theorem 1.6. Recall that if φ has good reduction at v, we write φ_v for the reduction of φ at v.

Lemma 4.3 *Let K be a number field, let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a morphism of degree greater than one defined over K, and let $\alpha \in K$ be a point that is not periodic for φ. Then there are infinitely many places v of good reduction for φ such that $r_v(\alpha)$ is not periodic for φ_v.*

Proof If α is φ-preperiodic but not periodic, then the φ-orbit $\mathcal{O}_\varphi(\alpha)$ is finite. Hence, the reduction map r_v is injective on $\mathcal{O}_\varphi(\alpha)$ for all but finitely many places v, and Lemma 4.3 holds in this case.

Thus, we may assume that α is not preperiodic. After passing to a finite extension L of K, we may also assume that φ has a nonexceptional fixed point β. We extend our isomorphism between $\mathbb{P}^1_K$ and the generic fibre of $\mathbb{P}^1_{\mathfrak{o}_K}$ to an isomorphism from $\mathbb{P}^1_L$ to the generic fibre of $\mathbb{P}^1_{\mathfrak{o}_L}$; and for each place $w|v$ of L, we obtain reduction maps $r_w : \mathbb{P}^1(L) \longrightarrow \mathbb{P}^1(\ell_w)$, where ℓ_w is the residue field at w. For each such $w|v$, we have $r_v(\gamma) = r_w(\gamma)$ for any $\gamma \in \mathbb{P}^1(K)$. By Lemma 4.1, there are infinitely many places w such that there is some n for which $r_w(\varphi^n(\alpha)) = r_w(\beta)$. When $w|v$ for v a place of good reduction for φ, this means that $r_v(\varphi^m(\alpha)) = r_v(\varphi^n(\alpha)) = r_w(\beta)$ for all $m \geq n$, since β is fixed by φ. At all but finitely many of these v, we have $r_v(\alpha) \neq r_w(\beta)$, which means that there is no positive integer m such that $r_v(\varphi^m(\alpha)) = r_v(\alpha)$, as desired. □

We will also need the following result for quadratic polynomials.

Proposition 4.4 *Let K be a number field, and let $f \in K[t]$ be a quadratic polynomial with no periodic critical points other than the point at infinity. Then there are infinitely many finite places v of K such that $|f'(z)|_v = 1$ for each $z \in K$ such that $|z|_v \leq 1$ and $r_v(z)$ is f_v-periodic.*

Proof Since f is a quadratic polynomial, it only has one critical point α other than the point at infinity. By Lemma 4.3 and because α is not periodic, there are infinitely many places v of good reduction for f such that $r_v(\alpha)$ is not f_v-periodic, and such that $|\alpha|_v \leq 1$ and $|2|_v = 1$. (The last two conditions may be added because each excludes only finitely many v.) In particular, $|f'(z)|_v = |z - \alpha|_v$ for any $z \in K$.

Hence, for any such v, and for any $z \in K$ as in the hypotheses, we have $r_v(z) \neq r_v(\alpha)$, since $r_v(z)$ is periodic but $r_v(\alpha)$ is not. Thus, $|f'(z)|_v = |z - \alpha|_v = 1$. □

5 Dynamical Mordell–Lang for curves

Using Proposition 4.2, we can now prove a dynamical Mordell–Lang statement for curves embedded in $\mathbb{P}^1 \times \mathbb{P}^1$.

Theorem 5.1 *Let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be a curve defined over $\overline{\mathbb{Q}}$, and let $\Phi := (\varphi, \varphi)$ act on $\mathbb{P}^1 \times \mathbb{P}^1$, where $\varphi \in \overline{\mathbb{Q}}(t)$ is a rational function with no superattracting periodic points other than exceptional points. Let $\mathcal{O}$ be the Φ-orbit of a point $(x, y) \in (\mathbb{P}^1 \times \mathbb{P}^1)(\overline{\mathbb{Q}})$. Then $C(\overline{\mathbb{Q}}) \cap \mathcal{O}$ is a union of at most finitely many orbits of the form $\{\Phi^{nk+\ell}(x, y)\}_{n \geq 0}$ for $k, \ell \in \mathbb{N}$.*

Proof If $\deg(\varphi) = 1$, we may change coordinates so that $\varphi(\infty) = \infty$, and hence Φ induces an automorphism of $\mathbb{A}^2$. The result then follows immediately from the work of Denis [9] and Bell [5]; see also [6]. Hence, we may assume $\deg(\varphi) \geq 2$.

We may assume that C is irreducible, and that $C(\overline{\mathbb{Q}}) \cap \mathcal{O}$ is infinite. Let K be a number field over which φ, C, (x, y), and any exceptional points of φ are defined. If either x or y is φ-periodic, then the projection of C to one of the two coordinates of $\mathbb{P}^1 \times \mathbb{P}^1$ consists of a single point (which must be a φ-periodic point), and the conclusion of Theorem 5.1 would be immediate. Thus, the hypotheses of Proposition 4.2 hold for $(\alpha, \beta) = (x, y)$.

Suppose there is a place v of good reduction satisfying condition (i) of Proposition 4.2. Let $p \in \mathbb{N}$ be the prime number lying in the maximal ideal of the nonarchimedean place v, and fix an embedding of K into $\mathbb{C}_p$ respecting v. The desired conclusion is immediate from Theorem 3.4.

If no such place exists, then by Proposition 4.2, there must be a place v of good reduction meeting condition (ii) for which neither α nor β lies in the same residue class as an exceptional point. (Here, we are using the fact that there are at most two exceptional points.) It follows that the orbits of α and β also avoid the residue classes of exceptional points. In particular, the attracting periodic points γ_1 and γ_2 given in condition (ii) cannot be exceptional. By hypothesis, then, γ_1 and γ_2 are attracting but not superattracting, and therefore the Theorem follows from [12, Theorem 1.3]. □

We can now prove Theorem 1.4 as a consequence of Theorem 5.1.

Proof of Theorem 1.4 Let $\mathcal{O}$ denote the Φ-orbit of the point $(x_1, \ldots, x_g)$. We may assume that C is irreducible, and that $C(\overline{\mathbb{Q}}) \cap \mathcal{O}$ is infinite. It suffices to prove that C is Φ-periodic. Indeed, if $\Phi^k(C) = C$, then for each $\ell \in \{0, \ldots, k-1\}$, the intersection of C with $\mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha))$ either is empty or else consists of all $\Phi^{nk+\ell}(\alpha)$, for some n sufficiently large. Either way, the conclusion of Theorem 1.4 holds.

We argue by induction on g. The case $g = 1$ is obvious, while the case $g = 2$ is proved in Theorem 5.1. Assuming Theorem 1.4 for some $g \geq 2$, we will now prove it for $g + 1$. We may assume that C projects dominantly onto each of the coordinates of $(\mathbb{P}^1)^{g+1}$; otherwise, we may view C as a curve in $(\mathbb{P}^1)^g$, and apply the inductive hypothesis. We may also assume that no x_i is preperiodic, lest C should fail to project dominantly on the ith coordinate.

Let $\pi_1 : (\mathbb{P}^1)^{g+1} \to (\mathbb{P}^1)^g$ be the projection onto the first g coordinates, let $C_1 := \pi_1(C)$, and let $\mathcal{O}_1 := \pi_1(\mathcal{O})$. By our assumptions, C_1 is an irreducible curve that has an infinite intersection with $\mathcal{O}_1$. By the inductive hypothesis, C_1 is periodic under the coordinatewise action of φ on the first g coordinates of $(\mathbb{P}^1)^{g+1}$.

Similarly, let C_2 be the projection of C on the last g coordinates of $(\mathbb{P}^1)^{g+1}$. By the same argument, C_2 is periodic under the coordinatewise action of φ on the last g coordinates of $(\mathbb{P}^1)^{g+1}$.

Thus, C is Φ-preperiodic, because it is an irreducible component of the one-dimensional variety $(C_1 \times \mathbb{P}^1) \cap (\mathbb{P}^1 \times C_2)$, and because both $C_1 \times \mathbb{P}^1$ and $\mathbb{P}^1 \times C_2$ are Φ-periodic.

Claim 5.2 Let X be a variety, let $\alpha \in X(\overline{K})$, let $\Phi : X \longrightarrow X$ be a morphism, and let $C \subset X$ be an irreducible curve that has infinite intersection with the orbit $\mathcal{O}_\Phi(\alpha)$. If C is Φ-preperiodic, then C is Φ-periodic.

Proof of Claim 5.2 Assume C is not periodic. Because C is preperiodic, there exist $k_0, n_0 \geq 1$ such that $\Phi^{n_0}(C)$ is periodic of period k_0. Let $k := n_0 k_0$, and let $C' := \Phi^k(C)$, which is fixed by Φ^k. Then $C \neq C'$, since C is not periodic. Because C and C' are irreducible curves, it follows that

$$C \cap C' \text{ is finite.} \tag{5.2.1}$$

On the other hand, there exists $\ell \in \{0, \ldots, k-1\}$ such that $C \cap \mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha))$ is infinite, because $C \cap \mathcal{O}_\Phi(\alpha)$ is infinite. Let $n_1 \in \mathbb{N}$ be the smallest nonnegative integer n such that $\Phi^{nk+\ell}(\alpha) \in C$. Since $C' = \Phi^k(C)$ is fixed by Φ^k, we conclude that $\Phi^{nk+\ell}(\alpha) \in C'$ for each $n \geq n_1 + 1$. Therefore

$$C \cap \mathcal{O}_{\Phi^k}(\Phi^\ell(\alpha)) \cap C' \text{ is infinite.} \tag{5.2.2}$$

Statements (5.2.1) and (5.2.2) are contradictory, proving the claim. □

An application of Claim 5.2 with $X = (\mathbb{P}^1)^{g+1}$ now completes the proof of Theorem 1.4. □

6 Quadratic polynomials

We are now ready to prove Theorems 1.6, 1.7, and 1.8.

Proof of Theorem 1.6. Let K be a number field such that V is defined over K, the polynomial f is in $K[t]$, and $x_1, \ldots, x_g$ are all in K.

Using Proposition 4.4, we may choose a place v of K such that

(a) v is a place of good reduction for f;
(b) $|x_i|_v \leq 1$, for each $i = 1, \ldots, g$;
(c) $|f'(z)|_v = 1$ for all z such that $|z|_v \leq 1$ and $r_v(z)$ is f_v-periodic.

Indeed, conditions (a) and (b) are satisfied at all but finitely many places v, while condition (c) is satisfied at infinitely many places. Because f is a polynomial, conditions (a) and (b) together imply that $|f^n(x_i)|_v \leq 1$ for all $i = 1, \ldots, g$ and $n \geq 0$. Meanwhile, condition (c) implies that f has no attracting periodic points at v. The desired conclusion now follows from Theorem 3.4. □

Proof of Theorem 1.7 After changing coordinates, we assume that $f(t) = t^2 + c$ for some $c \in \mathbb{Q}$. Thus, 0 is the only finite critical point of f. If $c \notin \mathbb{Z}$, then there is some prime p such that $|c|_p > 1$, so that $|f^n(0)|_p \to \infty$; similarly, if $c \in \mathbb{Z} \backslash \{0, -1, -2\}$, then $|f^n(0)|_\infty \to \infty$. Either way, 0 cannot be periodic. If $c = -2$, then 0 is only f-preperiodic, but not f-periodic. In all the above cases, the hypotheses of Theorem 1.6 are met, and we are done. If $c = 0$, then $f(t) = t^2$ is an endomorphism of $\mathbb{G}_m^g$, and thus our result follows from [12, Theorem 1.8].

We are left with the case that $f(t) = t^2 - 1$. As in the proof of Theorem 1.4, we may assume (via induction on g) that no x_i is preperiodic; in particular, all x_i and $f(x_i)$ are nonzero. If $f^2(z) = 0$, then either $z = 0$, or $z = \pm\sqrt{2}$. Bearing this fact in mind, we note that there are infinitely many primes p such that 2 is not a quadratic residue modulo p; more precisely, the density of such primes p is $\frac{1}{2}$. Thus, we may choose an odd prime p such that each x_i and $f(x_i)$ is a p-adic unit, and such that 2 is not a quadratic residue modulo p. Then there is no positive integer n such that $f^n(x_i)$ is in the same residue class as 0 modulo p for any i. Therefore, $|f'(f^n(x_i))|_p = 1$ for all n, and hence $f^n(x_i)$ never lies in the same residue class as an attracting periodic point. Theorem 1.7 now follows from Theorem 3.4. □

Proof of Theorem 1.8 As before, we may assume that no x_j is preperiodic for f_j. By [18, Theorem 1.2(iii)], for each f_j that is not equal to $t^2 - 1$, the set of primes p such that there is an n for which $f_j^n(x_j) \equiv 0 \pmod{p}$ has Dirichlet density zero. Meanwhile, as noted in the proof of Theorem 1.7, the density of primes p such that -2 is a square modulo p is $1/2$, and therefore the set of primes p for which there are an n and j satisfying $f_j(t) = t^2 - 1$ and $f_j^n(x_j) \equiv 0 \pmod{p}$ must have (upper) density at most $1/2$. Hence, the set of primes p such that $f_j^n(x_j) \not\equiv 0 \pmod{p}$ for all n and all $j = 1, \dots, g$ has (lower) density at least $1/2$. Choosing such a prime p, we see that $f_j^n(x_j)$ never lies in the same residue class as an attracting periodic point for any n and any $j = 1, \dots, g$, and the result follows from Theorem 3.4. □

7 Extensions to the field of complex numbers

In this section we will use recent work of Medvedev and Scanlon [23] to prove Theorem 1.5. We begin with the following definitions.

Definition 7.1 Let K be a field, and let $\varphi \in K[t]$ be a nonconstant polynomial. We say that φ is *indecomposable* if there are no polynomials $\psi_1, \psi_2 \in \overline{K}[t]$ of degree greater than one such that $\varphi = \psi_1 \circ \psi_2$.

Generic polynomials over $\mathbb{C}$ of any positive degree are indecomposable. This is obvious for (all) polynomials of prime degree or degree one, and it is easy to prove in degree at least 6 (say by reducing to monic decompositions and counting dimensions); but it can also be shown in degree 4.

Definition 7.2 Let K be a field, and let $f \in K[t]$ be a polynomial of degree $m \geq 1$. If f is monic with trivial t^{m-1} term, we say that f is in *normal form*; that is, f is of the form

$$t^m + c_{m-2}t^{m-2} + \cdots + c_0.$$

In that case, we say that f is of *type* (a, b) if a is the smallest nonnegative integer such that $c_a \neq 0$, and b is the largest positive integer such that $f(t) = t^a u(t^b)$ for some polynomial $u \in K[t]$.

While we have introduced this definition of "type" to aid our exposition, the accompanying notion of normal form is not new. In fact, as noted in [3, Equation (2.1)], if $\operatorname{char} K = 0$ and $f \in K[t]$ is a polynomial of degree $m \geq 2$, and if K contains an $(m-1)$-st root of the leading coefficient, then there is a linear polynomial $\mu \in K[t]$ such that $\mu^{-1} \circ f \circ \mu$ is in normal form.

Definition 7.3 For each positive integer m, define $D_m \in \mathbb{Z}[t]$ to be the unique polynomial of degree m such that $D_m(t + 1/t) = t^m + 1/t^m$.

The usual Chebyshev polynomial T_m (satisfying $T_m(\cos(\theta)) = \cos(m\theta)$) is conjugate to D_m, since $D_m(2t) = 2T_m(t)$. However, D_m is in normal form.

The following result is an immediate consequence of Theorem 3.149 in [23] (see also Section 3.2 in [23]).

Theorem 7.4 (Medvedev, Scanlon) *Let K be an algebraically closed field of characteristic 0, and let $\varphi \in K[t]$ be a nonlinear indecomposable polynomial which is not conjugate to t^m or D_m for any positive integer m. Assume that φ is in normal form, of type (a, b).*

Let Φ denote the action of (φ, φ) on $\mathbb{A}^2$. Let C be a Φ-periodic irreducible plane curve defined over K. Then C is defined by one of the following equations in the variables (x, y) of the affine plane:

(i) $x = x_0$*, for a φ-periodic point x_0; or*
(ii) $y = y_0$*, for a φ-periodic point y_0; or*
(iii) $x = \zeta\varphi^r(y)$*, for some $r \geq 0$; or*
(iv) $y = \zeta\varphi^r(x)$*, for some $r \geq 0$,*

where ζ is a d-th root of unity, where $d \mid b$ and $\gcd(d, a) = 1$.

Remark 7.5 Note that if $b = 1$ or $a = 0$ in Theorem 7.4, then $d = 1$, and hence $\zeta = 1$.

Using Theorem 7.4, we can prove the following result.

Theorem 7.6 *Let $\varphi \in \mathbb{C}[t]$ be an indecomposable polynomial with no periodic superattracting points other than exceptional points, and let $\Phi := (\varphi, \varphi)$ be its diagonal action on $\mathbb{A}^2$. Let $\mathcal{O}$ be the Φ-orbit of a point (x_0, y_0) in $\mathbb{A}^2(\mathbb{C})$, and let C be a curve defined over $\mathbb{C}$. Then $C(\mathbb{C}) \cap \mathcal{O}$ is a union of at most finitely many orbits of the form $\{\Phi^{nk+\ell}(x_0, y_0)\}_{n\geq 0}$ for nonnegative integers k and ℓ.*

We will need three more ingredients to prove Theorem 7.6.

Proposition 7.7 *Fix integers $m, g \geq 1$, let $\varphi \in \mathbb{C}[t]$ be a polynomial which is a conjugate of either t^m or D_m, and let Φ be its coordinatewise action on $\mathbb{A}^g$. Let $\mathcal{O}$ be the Φ-orbit of a point $\alpha \in \mathbb{A}^g(\mathbb{C})$, and let V be an affine subvariety of $\mathbb{A}^g$ defined over $\mathbb{C}$. Then $V(\mathbb{C}) \cap \mathcal{O}$ is a union of at most finitely many orbits of the form $\{\Phi^{nk+\ell}(P)\}_{n\geq 0}$ for nonnegative integers k and ℓ.*

Proof By hypothesis, there is a linear polynomial $h(t) \in \mathbb{C}[t]$ such that either $\varphi(h(t)) = h(t^m)$ or $\varphi(h(t)) = h(D_m(t))$. In the first case, let $k(t) = h(t)$, and in the second, let $k(t) = h(t + 1/t)$. Then $\varphi(k(t)) = k(t^m)$ for some nonconstant rational function $k(t) \in \mathbb{C}(t)$. Note that in either case, $k(\mathbb{C}) \supseteq \mathbb{C}$, and the only possible poles of k are at 0 and ∞.

Let $\alpha := (x_1, \ldots, x_g)$. For each $i \in \{1, \ldots, g\}$, pick $z_i \in \mathbb{C}$ such that $k(z_i) = x_i$. Then $\mathcal{O}_\Phi(\alpha) = \{(k(z_1^{m^n}), \ldots, k(z_g^{m^n})) : n \geq 0\}$. Let W be the affine subvariety of $\mathbb{G}_m^g$ defined by the equations $f(k(t_1), \ldots, k(t_g)) = 0$, where f ranges over a set of generators for the vanishing ideal of V. (Note that W is an algebraic subvariety of $\mathbb{G}_m^g$ because k has no poles on $\mathbb{G}_m$.)

Let Ψ be the endomorphism of $\mathbb{G}_m^g$ given by $\Psi(t_1,\ldots,t_g)=(t_1^m,\ldots,t_g^m)$. Then

$$\Phi^n(x_1,\ldots,x_g)\in V(\mathbb{C})\quad\text{if and only if } \Psi^n(z_1,\ldots,z_g)\in W(\mathbb{C}).$$

Thus, Proposition 7.7 holds for Φ and V because, by [12, Theorem 1.8], it holds for Ψ and W. □

Proposition 7.8 *Let E be a field of characteristic 0, and K a function field of transcendence degree 1 over E. Let $\varphi\in K[t]$ be a polynomial of degree $m\geq 2$ in normal form. Assume that φ is not conjugate to t^m or D_m over the algebraic closure $\overline{K}$ of K. Then for all but finitely places v of the function field K, the reduction φ_v of φ at v is not conjugate to t^m or D_m over the algebraic closure $\overline{k}_v$ of the residue field k_v corresponding to the place v.*

Proof After replacing K by a finite extension, we may assume that K contains all $(m-1)$-st roots of unity. All coefficients of φ are v-adic integers at all but finitely many places v. For any such place, write k_v for the residue field and φ_v for the reduction of φ. If φ_v is conjugate to the reduction f_v of either $f=D_m$ or $f(t)=t^m$, write $\varphi_v(t)=\mu_v^{-1}\circ f_v\circ\mu_v$ for some linear polynomial $\mu_v(t)=At+B\in\overline{k}_v[t]$. Because φ_v and f_v are both in normal form, we must have $\mu_v(t)=\zeta_v t$, for some $(m-1)$-st root of unity $\zeta_v\in\overline{k}_v$. (Indeed, because $\operatorname{char} k_v=\operatorname{char} E=0$ and both φ_v and f_v have trivial t^{m-1} term, we must have $B=0$; and because both are monic, A must be an $(m-1)$-st root of unity.)

Thus, at any such place v, φ is congruent modulo v to one of the m polynomials $\zeta^{-1}D_m(\zeta t)$ or $\zeta^{-1}(\zeta t)^m=t^m$, where $\zeta\in K$ is an $(m-1)$-st root of unity. Since φ is not one of those m polynomials itself, there are only finitely many such v at which that occurs. □

Proposition 7.9 *Let E be a field, and K a function field of transcendence degree 1 over E. Let $f\in K[t]$ be an indecomposable polynomial of degree greater than one. Then for all but finitely many places v of K, the reduction of f modulo v is also an indecomposable polynomial over $\overline{k}_v$ of degree greater than one, where k_v is the residue field of K at v.*

Proof First we note that for all but finitely many places v of K, the coefficients of f are integral at v, and the leading coefficient of f is a unit at v. Thus, the reduction f_v of f modulo v is a polynomial of same degree as f.

We will show that for any given positive integers m and n (with $m,n\geq 2$) such that $mn=\deg(f)$, if f is not a composition of a polynomial of degree m with a polynomial of degree n, then for all but finitely many places v of K, the reduction of f modulo v cannot be written as a composition of two polynomials of degrees m and n, respectively, with coefficients in $\overline{k}_v$. Because there are finitely many pairs of positive integers (m,n) such that $mn=\deg(f)$, our desired conclusion follows.

Let m and n be positive integers such that $mn = \deg(f)$ (with $m, n \geq 2$). Then the nonexistence of polynomials

$$g(t) = \sum_{i=0}^{m} a_i t^i \quad \text{and} \quad h(t) = \sum_{j=0}^{n} b_j t^j$$

with coefficients in $\overline{K}$, such that $f = g \circ h$, where $f(t) = \sum_{\ell=0}^{\deg(f)} c_\ell t^\ell$, translates to the statement that the variety $X \subset \mathbb{A}^{m+n+2}$ given by the equations which must be satisfied by the a_i's and the b_j's has no $\overline{K}$-points. Furthermore, X is a variety defined over a subring R of K such that all but finitely many places of K are maximal ideals of R.

Suppose there is an infinite set $\mathcal{S}$ of places v of K at which f_v is actually a composition of two polynomials of degrees m and n, with coefficients in $\overline{k}_v$. Then the special fibre of X over v is nonempty over $\overline{k}_v$ for each $v \in \mathcal{S}$. Therefore, the equations defining X determine a nonempty locus over the ultraproduct $\mathcal{K}_{\mathcal{S},\mathcal{U}}$ of all the infinitely many fields $\overline{k}_v$ with respect to a non-principal ultrafilter $\mathcal{U}$ based on $\mathcal{S}$. However, K embeds into $\mathcal{K}_{\mathcal{S},\mathcal{U}}$ (see [17, p. 198–199]). Since X is defined over K and has a rational point over a field containing K, it must in fact have an algebraic point over K, giving a contradiction to the fact that $X(\overline{K})$ is empty. □

We are ready to prove Theorem 7.6.

Proof of Theorem 7.6 If φ is a linear polynomial, then the result follows from [5]. If φ is conjugate to t^m or D_m, then our conclusion follows from Proposition 7.7. We may therefore assume that φ is an indecomposable, nonlinear polynomial which is neither a conjugate of t^m, nor of D_m. Furthermore, after conjugating φ by a linear polynomial μ (and replacing (x_0, y_0) by $(\mu^{-1}(x_0), \mu^{-1}(y_0))$ and C by $(\mu^{-1}, \mu^{-1})(C))$, we may assume that φ is in normal form. Let $m = \deg\varphi$.

As before, we may assume that C is an irreducible curve, and that C does not project to a single point to any of the coordinates. For example, if $C = \mathbb{A}^1 \times \{y_1\}$, then y_1 is φ-periodic, and hence C is Φ-periodic. In particular, we may assume that neither x_0 nor y_0 is φ-preperiodic.

Let K be a finitely generated field over which C, φ, x_0 and y_0 are defined. Furthermore, at the expense of replacing K by a finite extension, we may assume that C is geometrically irreducible and that K contains all critical points of φ and all $(m-1)$-st roots of unity.

We will prove Theorem 7.6 by induction on $d := \operatorname{trdeg}_{\mathbb{Q}} K$. If $d = 0$, then K is a number field, and our conclusion follows from Theorem 5.1.

Assume $d \geq 1$. Then K may be viewed as the function field of a smooth, geometrically irreducible curve Z defined over a finitely generated field E; thus, $\operatorname{trdeg}_{\mathbb{Q}} E = d - 1$. Moreover, the curve C extends to a 1-dimensional scheme over Z (called $\mathfrak{C}$), all but finitely many of whose fibres $\mathfrak{C}_\gamma$ are irreducible curves.

We claim that there are infinitely many places γ of K for which all of the following statements hold. (By a place of K, we mean a valuation of the function field K/E, cf. Chapter 2 of [29].)

(a) The fibre $\mathfrak{C}_\gamma$ is an irreducible curve defined over the residue field $E(\gamma)$ of γ, of the same degree as C.

(b) All nonzero coefficients of φ are units at the place γ; in particular, φ has good reduction at γ, and so we write φ_γ and $\Phi_\gamma := (\varphi_\gamma, \varphi_\gamma)$ for the reductions of φ and Φ at γ.
(c) The critical points of φ_γ are reductions at γ of the critical points of φ.
(d) For each critical point z of φ (other than infinity), the reduction z_γ is not a periodic point for φ_γ.
(e) The map $\mathcal{O} \longrightarrow \mathcal{O}_\gamma$ from the Φ-orbit of (x_0, y_0) to the Φ_γ-orbit of $(x_{0,\gamma}, y_{0,\gamma})$, induced by reduction at γ, is injective.
(f) φ_γ is not conjugate to t^m or D_m. (Recall $m = \deg \varphi$.)
(g) φ_γ is a nonlinear, indecomposable polynomial.

Conditions (a)–(c) above are satisfied at all but finitely many places γ of K. The same is true of conditions (f)–(g), by Proposition 7.8 and Proposition 7.9. Condition (d) for preperiodic (but not periodic) critical points also holds at all but finitely many places; see the first paragraph of the proof of Lemma 4.3. Meanwhile, [14, Proposition 6.2] says that the reduction of any finite set of nonpreperiodic points remains nonpreperiodic at infinitely many places γ (in fact, at all γ on Z of sufficiently large Weil height). Thus, conditions (d)–(e) hold by applying [14, Proposition 6.2] to (x_0, y_0) and the nonpreperiodic critical points, proving the claim.

Let γ be one of the infinitely many places satisfying conditions (a)–(g) above. From condition (e), we deduce that $\mathfrak{C}_\gamma(E(\gamma)) \cap \mathcal{O}_\gamma$ is infinite. Conditions (c)–(d) guarantee that φ_γ has no periodic critical points (other than the exceptional point at infinity). Because $E(\gamma)$ is a finite extension of E, we get $\operatorname{trdeg}_{\mathbb{Q}} E(\gamma) = d-1$. By the inductive hypothesis, then, $\mathfrak{C}_\gamma$ is Φ_γ-periodic. By conditions (f)–(g) and Theorem 7.4, $\mathfrak{C}_\gamma$ is the zero set of an equation from one of the four forms (i)–(iv) in Theorem 7.4. In fact, if φ has type (a, b), then the degree d in Theorem 7.4 satisfies $d|b$ and $\gcd(d, a) = 1$, because condition (b) implies that φ_γ also has type (a, b). Thus, for one of the four forms (i)–(iv), there are infinitely many places γ satisfying (a)–(g) above such that the equation for $\mathfrak{C}_\gamma$ is of that form. By symmetry, it suffices to consider only forms (i) and (iii).

Case 1 Assume there are infinitely many γ satisfying (a)–(g) such that $\mathfrak{C}_\gamma$ is given by an equation $x = x(\gamma)$, for some φ_γ-periodic point $x(\gamma) \in E(\gamma)$. Then, since the degree of C is preserved by the reduction at γ, we see that the degree of C must be 1. Thus, C is defined by an equation of the form $ax + by + c = 0$. Since there are infinitely many γ such that the above equation reduces at γ to $x = x(\gamma)$, we must have $b = 0$; hence, the curve C must be given by an equation $x = x_1$ for some $x_1 \in K$, contradicting our assumption that C does not project to a point in any of the coordinates.

Case 2 Assume there are infinitely many γ satisfying (a)–(g) such that $\mathfrak{C}_\gamma$ is given by an equation $y = \zeta\varphi_\gamma^r(x)$, for some $r \geq 0$ and some d-th root of unity ζ, where $d \mid b$ and $\gcd(d, a) = 1$. Because there are only finitely many b-th roots of unity, we may assume ζ is the same for all of the infinitely many γ. Moreover, because $\mathfrak{C}_\gamma$ has the same degree as C, the integer r is the same for all such γ. Thus, there are infinitely many places γ for which the polynomial equation for C reduces modulo γ to $y - \zeta\varphi^r(x)$, and hence the two polynomials are the same. Thus, C is the zero set of the polynomial $y - \zeta\varphi^r(x)$. Because φ is of type (a, b), it follows that C is Φ-periodic. □

Arguing precisely as in the proof of Theorem 1.4, Theorem 1.5 follows as a consequence of Theorem 7.6.

Remark 7.10 In personal communications, Medvedev and Scanlon told us that, using the methods of [23], it is possible to prove the conclusion of Theorem 7.4 even for decomposable polynomials f that are not compositional powers of other polynomials. Using that stronger result in our proofs above, we could then extend Theorems 7.6 and 1.5 to any f that is not a compositional power of another polynomial. It would then be easy to extend those results to *all* polynomials $f \in \mathbb{C}[t]$ (with no periodic superattracting points other than exceptional points); indeed, if $f = g^k$ is a compositional power, then we may simply replace the action of f with the action of g.

Acknowledgments The authors would like to thank A. Medvedev, T. Scanlon, L. Szpiro, and M. Zieve for helpful conversations, and the referee for many useful suggestions. Research of R. B. was partially supported by NSF Grant DMS-0600878, that of D. G. by an NSERC grant, that of P. K. by grants from the Göran Gustafsson Foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council, and that of T. T. by NSA Grant 06G-067, NSF Grants 0801072 and 0854839.

8 Appendix by Umberto Zannier

As anticipated in the Introduction, in the present Appendix we shall prove a result similar to but stronger than Proposition 4.2 above. This appeared in a weaker form in a previous version of this paper (replacing the present Proposition 4.2) and was subsequently sharpened. For the purposes of the present paper such result has been later found not to be strictly necessary; however it is still relevant in the context, in that it relates the strategy of this paper to questions about integral points, indicating another possible approach to the present issues, which shall be discussed in detail elsewhere.

As above, we let K be a number field and, for a finite place v of K with residue field $K(v)$, we let $r_v : \mathbb{P}^1(K) \to \mathbb{P}^1(K(v))$ be the reduction map. For a finite set S of places of K (including the infinite ones) we let as usual $\mathcal{O}_S$ denote the ring of S-integers of K.

We shall meet derivatives of rational functions; we shall denote by $\varphi^{(h)}$ the h-th derivative of φ whereas φ^n shall denote as above the n-th iterate.

Theorem 8.1 *Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism defined over K, of degree $d \geq 2$ and not conjugate to a map of the shape $t \mapsto t^d$. Let $\alpha, \beta \in \mathbb{P}^1(K)$ be points not preperiodic for φ and suppose that there is an irreducible curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ containing infinitely many points $(\varphi^k(\alpha), \varphi^k(\beta))$.*

Then there are infinitely many finite places v of K such that φ has good reduction at v and such that for some integer $n \geq 1$ the points $\varphi^n(\alpha), \varphi^n(\beta)$ are in the same residue class modulo v, i.e. $r_v(\varphi^n(\alpha)) = r_v(\varphi^n(\beta))$.

Further, if we assume that φ is conjugate to a polynomial, the conclusion holds also on dropping the assumption of the existence of the curve C.

Proof In a first part we show that either the conclusion holds or φ is totally branched above some point, and actually it is conjugate to a polynomial. Then we shall consider the polynomial case. For clarity, we subdivide the proof in several steps.

1. Let us suppose that the conclusion is not true so there exists a finite set S of places such that for all $v \notin S$ and all $n > n_0$, we have $r_v(\varphi^n(\alpha)) \neq r_v(\varphi^n(\beta))$, i.e. $\varphi^n(\alpha) - \varphi^n(\beta)$ has a numerator not divisible by v, hence $(\varphi^n(\alpha) - \varphi^n(\beta))^{-1} \in \mathcal{O}_S$. (If one of $\varphi^n(\alpha), \varphi^n(\beta) = \infty$, then the condition implies that the other cannot be ∞ and the thing again holds.)
Let $\lambda \in \mathrm{PGL}_2(\bar{\mathbb{Q}}) = \mathrm{Aut}(\mathbb{P}^1)$ be any fixed homography. Then, by enlarging K and S we may assume that λ is defined over K and has good reduction outside S, so it induces an automorphism of $\mathbb{P}^1(K(v))$. Hence the same holds if we replace φ^n with $\lambda \circ \varphi^n$; namely, $(\lambda(\varphi^n(\alpha)) - \lambda(\varphi^n(\beta)))^{-1} \in \mathcal{O}_S$. This also allows us to replace φ by $\lambda \circ \varphi \circ \lambda^{-1}$ and α, β with $\lambda(\alpha), \lambda(\beta)$ respectively.

2. Let u, v be the projections from the curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ to the factors (none is constant by the assumptions that α, β are not preperiodic). For $n \in \mathbb{N}$ and a $\lambda \in \mathrm{PGL}_2$ put

$$\psi_n = \psi_{n,\lambda} := (\lambda(\varphi^n(u)) - \lambda(\varphi^n(v)))^{-1}.$$

This is a rational function on C; it is well defined because if $\varphi^n(u) = \varphi^n(v)$ then $\varphi^N(\alpha) = \varphi^N(\beta)$ for infinitely many N, contrary to **1**.
By **1.**, ψ_n takes S-integer values at infinitely many rational points $(\varphi^k(\alpha), \varphi^k(\beta))$ on C.

3. By Siegel's theorem [30] (see [19, Theorem 8.5.2] for the exact form used here) on integral points on curves we conclude that the union Σ of all zeros of all the functions $\lambda(\varphi^n(u)) - \lambda(\varphi^n(v))$ (for varying λ and n) satisfies $|\Sigma| \leq 2$, and moreover we conclude that C is a rational curve (over some number field).

4. To simplify some of the coming calculations we now choose λ with the property that none among $\lambda(\varphi^n(u)), \lambda(\varphi^n(v))$, any $n \in \mathbb{N}$, has a pole at any point of Σ. It suffices to choose $\lambda(x) = 1/(x - a)$ where a is different from all the values $\varphi^n(u(P)), \varphi^n(v(P))$, for $P \in \Sigma$. For instance, any algebraic number a outside a number field of definition for φ, u, v, Σ shall do.
Then, we may replace φ by $\lambda \circ \varphi \circ \lambda^{-1}$, and replace u, v by $\lambda(u), \lambda(v)$, and suppose directly that $\varphi^n(u), \varphi^n(v)$ have no pole in Σ. The previous conclusions continue to hold, whence in particular the functions $\varphi^n(u) - \varphi^n(v)$ have zeros in Σ.
With these normalizations, we put $u_n := \varphi^n(u)$, $v_n := \varphi^n(v)$, $\delta_n := v_n - u_n$, so δ_n has zeros in Σ whereas u_n, v_n have no pole in Σ.
Also, we choose any point $P_0 \in \Sigma$ and we put $\omega(f) := \mathrm{ord}_{P_0}(f - f(P_0))$, for a rational function $f \in \bar{\mathbb{Q}}(C)$. We use the usual convention that $1/f$ stands for $f - \infty$ when f has a pole at P_0, so $\omega(f) > 0$ always.

5. Suppose $\delta_r(P_0) = 0$. Then $u_r(P_0) = v_r(P_0)$ (recall that u_r, v_r have no pole in Σ) whence for all $n \geq r$ we have $u_n(P_0) = v_n(P_0)$, i.e. $\delta_n(P_0) = 0$ (recall that in the present normalization no u_n has a pole at P_0). We want to estimate some multiplicities.
Fix $n \geq r$ and write $\mu := u_n(P_0)$; this μ is not a pole of φ, for otherwise P_0 would be a pole of φ^{n+1}; then write $\varphi(t) = \varphi(\mu) + (t - \mu)^m \varphi_1(t)$, where φ_1 is regular and does not vanish at μ. We have $m = m(\mu) > 0$; note that μ and m depend on n (not only on P_0). We have the Taylor expansion

$$\delta_{n+1} = \varphi(v_n) - \varphi(u_n) = \varphi(u_n + \delta_n) - \varphi(u_n) = \delta_n \varphi'(u_n) + \delta_n^2 \frac{\varphi''(u_n)}{2} + \cdots .$$

The terms $\delta_n^h \varphi^{(h)}(u_n)/h!$ are rational functions on C whose orders at P_0 tends to infinity, so we may consider this expansion in the topology of local series at P_0. Observe that $\operatorname{ord}_{P_0} \varphi^{(h)}(u_n) = (m-h)\omega(u_n)$ for $1 \leq h \leq m$. Hence

$$\omega(\delta_n^h \varphi^{(h)}(u_n)) = h\omega(\delta_n) + (m-h)\omega(u_n), \quad 1 \leq h \leq m.$$

Also, it is immediately checked that $\omega(u_{n+1}) = m\omega(u_n)$.

6. If $\omega(\delta_n) > \omega(u_n)$ then by the last displayed formula at **5.** we find that the minimum order in the Taylor expansion at **5.** is attained strictly at the first term (i.e. for $h = 1$), whence $\omega(\delta_{n+1}) = \omega(\delta_n) + (m-1)\omega(u_n)$ and, by the last equality at **5.**,

$$\omega(\delta_{n+1}) - \omega(u_{n+1}) = \omega(\delta_n) - \omega(u_n).$$

We also deduce that $\omega(u_{n+1}) < \omega(\delta_{n+1})$, so we fall in this same case, with $n+1$ in place of n.

7. If $\omega(\delta_n) < \omega(u_n)$ then similarly to **6.** we find that $\omega(\delta_{n+1}) = m\omega(\delta_n)$; from **5.** we have $\omega(u_{n+1}) = m\omega(u_n)$, so $\omega(\delta_{n+1}) < \omega(u_{n+1})$.

8. Similarly, if $\omega(\delta_n) = \omega(u_n)$ we see from the Taylor expansion that certainly $\omega(\delta_{n+1}) \geq m\omega(\delta_n) = m\omega(u_n) = \omega(u_{n+1})$.

9. So, if $\omega(\delta_s) > \omega(u_s)$ for some s we are in case **6.** for all $n \geq s$. Otherwise $\omega(\delta_n) \leq \omega(u_n)$ for all n.

10. In all cases we easily see from the above that $\omega(\delta_n) - \omega(u_n) \leq O(1)$ as $n \to \infty$, whence, by iterating the last equality of **5.** and recalling the definition of ω, we find in particular that

$$\omega(\delta_n) \ll m_0(P_0)^n,$$

where $m_0(P_0)$ is the maximum ramification of φ at some point in $\{u_n(P_0) : n \in \mathbb{N}\}$.

11. Note now that any common pole of u_n and v_n is a zero of $(1/v_n) - (1/u_n)$. Hence by **3.** (using this time $\lambda(x) = 1/x$) we conclude that such a pole lies in Σ. But in the present normalization (see **4**) no element of Σ is a pole of u_n; hence there are no common poles at all of u_n and v_n. In particular, there is no pole cancellation in $v_n - u_n$, whence $\deg(\delta_n) \geq \deg(u_n) + \deg(v_n)$. Also, putting $d := \deg(\varphi)$, we have $\deg(u_n) = d^n \deg(u)$, $\deg(v_n) = d^n \deg(v)$, so

$$\deg(\delta_n) \gg d^n.$$

12. Putting $m_0 := \max_{P_0 \in \Sigma} m_0(P_0)$, by **10.** we have

$$\max_{P_0 \in \Sigma} \operatorname{ord}_{P_0} \delta_n \ll m_0^n.$$

> Comparing with **11.** and using that the degree is the number of zeros with multiplicity, we find $\deg(\delta_n) \ll |\Sigma| \cdot m_0^n$, whence $m_0 \geq d$, so actually $m_0 = d$. In particular, φ is totally branched over some finite point. But the deductions from **3.** onwards hold also by replacing φ by φ^r (any fixed integer r), so any φ^r is totally branched above a finite point $P = P_r$. Then $\varphi^{-r}(P)$ consists of a single point and φ is totally branched above $\varphi^{-(r-1)}(P)$. But φ can be totally branched above at most two points, and if it is such, it is conjugate to a cyclic polynomial, against the assumptions of the Theorem. Thus we can assume that φ is totally branched above exactly a single point. Then this P_r must be a fixed point of φ.

By conjugating φ in PGL_2 we may thus assume that φ has ∞ as a totally ramified fixed point. This means that φ is conjugate to a polynomial. All the conclusions of **3.** continue to hold (on changing suitably u, v according to the conjugation).

The polynomial case

The various steps in our argument will be denoted now by **Pn** for various positive integers n in order to distinguish them from the previous steps in our proof.

P1. Before continuing our deductions, let us start by noting that *if we assume from the beginning that φ is a polynomial, then either the first conclusion of the Theorem is true or anyway infinitely many $(\varphi^k(\alpha), \varphi^k(\beta))$ lie on a curve*. Hence in the polynomial case we can dispense with the assumptions that infinitely many $(\varphi^k(\alpha), \varphi^k(\beta))$ lie on a curve. After the coming arguments, this shall eventually justify the final assertion of the Theorem.

To justify this claim, suppose that the first conclusion of the Theorem is not true. Note that for large enough S the numbers $\varphi^n(\alpha) - \varphi^n(\beta)$ are S-integers, for all $n \in \mathbb{N}$: in fact, since φ is a polynomial, it suffices that α, β and the coefficients of φ are S-integers. Then, as in **1.** above we find that $\varphi^n(\alpha) - \varphi^n(\beta)$ are actually S-units for all $n \in \mathbb{N}$.

Now suppose by contradiction that the points $(\varphi^k(\alpha), \varphi^k(\beta))$, $k \in \mathbb{N}$, are Zariski-dense in $\mathbb{A}^2$, and denote now by x, y coordinates on $\mathbb{A}^2$. Then the rational functions $x - y$, $\varphi(x) - \varphi(y)$, $\varphi^2(x) - \varphi^2(y)$ assume S-unit values on a Zariski-dense set (i.e. the set $\{(\varphi^k(\alpha), \varphi^k(\beta)) : k \in \mathbb{N}\}$). Then by Laurent's theorem [20] (see also [8, Theorem 7.4.7]) on the structure of S-unit points on subvarieties of multiplicative tori the closure in $\mathbb{G}_m^3$ of the image of $\mathbb{A}^2$ by these functions must be a translate of a torus in $\mathbb{G}_m^3$. Since the image has anyway dimension ≤ 2, we have thus an identical equation

$$(x - y)^a(\varphi(x) - \varphi(y))^b(\varphi^2(x) - \varphi^2(y))^c = c_0,$$

for integers a, b, c not all zero and a nonzero constant c_0. However this is easily checked to be impossible for $d \geq 2$ (it suffices to note that the zero divisor of $\varphi(x) - \varphi(y)$ has at least a component not containing the line $x = y$). This contradiction proves the claim.

Let us now go on by proving the conclusion of the Theorem, assuming that φ is a polynomial (and that infinitely many $(\varphi^k(\alpha), \varphi^k(\beta))$, $k \in \mathbb{N}$, lie on the curve C).

P2. As in **P1.** we find that $\varphi^n(\alpha), \varphi^n(\beta)$ are S-units. Hence, again by Siegel's theorem, we conclude as in **3.** that all the maps $\delta_n := \varphi^n(u) - \varphi^n(v)$ have zeros AND poles in

Σ. (Note however that now that we are assuming that φ is a polynomial, we shall not change anymore normalization as in **4.** above.)

Recall also that by Siegel's theorem our curve must be rational, and we may take it equal to $\mathbb{P}^1$ and we may take $\Sigma = \{0, \infty\}$.

We contend that the poles of u_n and of v_n are in Σ: in fact, a pole of u_n is either a pole of δ_n or a pole of v_n; in this last case it is a zero of $(1/u_n) - (1/v_n)$, so in any case it is in Σ. (This also follows directly from Siegel's theorem: u_n, v_n take infinitely many S-integer values on $C(K)$.)

With these normalizations, we may also write $\delta_n = \gamma t^{g_n}$ with integer g_n, whereas u_n, v_n are Laurent polynomials in t.

P3. Suppose first that u_1 has precisely two poles. Then $u_n = \varphi^n(u_1)$ has also two poles.

We then write $u_n = \alpha t^{a_n} + \cdots + \beta / t^{b_n}$, where a_n, b_n are the pole orders, so > 0. On replacing t by $1/t$ if necessary, we may assume $g_n \geq 0$ for a given n.

Write as in **5.** the Taylor expansion (now it has only finitely many terms)

$$\delta_{n+1} = \varphi(v_n) - \varphi(u_n) = \varphi(u_n + \delta_n) - \varphi(u_n) = \delta_n \varphi'(u_n) + \delta_n^2 \frac{\varphi''(u_n)}{2} + \cdots .$$

and note that δ_{n+1} contains a term t^A with $A = g_n - (d-1)b_n$ (look at $\delta_n \varphi'(u_n)$ in the Taylor expansion). We conclude that

$$g_{n+1} = g_n - (d-1)b_n.$$

P4. If $g_n > a_n$ then we must have $g_{n+1} = dg_n$ (look now at terms of highest degree in the Taylor series or observe that $\varphi(u_n + \delta_n)$ has order dg_n at ∞), a contradiction.

If $g_n < a_n$, then (look again at highest degree terms) we have $g_{n+1} = g_n + (d-1) a_n > g_n$, a contradiction.

Then $g_n = a_n$, and moreover there must be cancellation in the highest terms in the Taylor series (because $g_{n+1} < g_n$ by **P3**). Now, if $g_{n+1} \geq 0$, we may apply the same argument and deduce $g_{n+1} = a_{n+1} = da_n = dg_n$, a contradiction.

Hence $g_{n+1} < 0$. But then the argument applies after changing t into $1/t$, i.e. exchanging a_{n+1}, b_{n+1}. This gives $(d-1)b_n - g_n = b_{n+1} = db_n$, which is also impossible.

We conclude that u_n cannot have two poles, and therefore we may assume it is a polynomial.

P5. Write $a_n = \deg u_n$, $\beta_n = u_n(0)$. In this doubly polynomial case we easily see as above that:

if $g_n \neq a_n$ then $g_{n+1} = g_n + (d-1)a_n \neq a_{n+1}$, so we deduce that $g_n - a_n$ is constant.

The same holds if $g_n = a_n$, except if some cancellation occurs. But this cancellation produces $g_{n+1} < a_{n+1}$ and we fall in the previous case.

Hence eventually we have that $g_n - a_n$ is constant in all cases. Note that $a_n = d^n a_0$.

P6. Using once more the Taylor series in the form $\delta_n \varphi'(u_n) = \delta_{n+1} - \delta_n^2 \frac{\varphi''(u_n)}{2} - \cdots$, we deduce that $\operatorname{ord}_0 \varphi'(u_n) \geq \min(g_n, g_{n+1} - g_n)$, so $\varphi'(u_n)$ eventually vanishes at 0. Then β_n is a zero of φ', say of multiplicity μ_n. Put also $\omega_n = \operatorname{ord}_0(u_n - \beta_n) > 0$. We have

$$\mathrm{ord}_0(\delta_n^h \varphi^{(h)}(u_n)) = hg_n + (\mu_n + 1 - h)\omega_n, \quad 1 \leq h \leq \mu_n + 1,$$

and $\mathrm{ord}_0(\delta_n^h \varphi^{(h)}(u_n)) \geq hg_n$ for all $h > 0$.

P7. We want to show that $\mu_n = d - 1 = \deg \varphi'$.

Suppose that $\omega_n < g_n$. Then by **P6.**, the minimum order

$$\mathrm{ord}_0(\delta_n^h \varphi^{(h)}(u_n)),$$

for varying $h \geq 1$, is attained uniquely for $h = 1$ and hence (by the Taylor series again) must be g_{n+1}. In other words, $g_n + \mu_n \omega_n = g_{n+1}$ ($\geq$ in place of $=$ suffices here) whence (by **P5.**) $\mu_n \omega_n \geq (d-1)a_n$, which in turn implies $\mu_n g_n > (d-1)a_n$, whence $\mu_n \geq d - 1$, as required.

Hence assume $\omega_n \geq g_n$ for all large n. Write $u_n = \beta_n + t^{\omega_n}\rho_n$. Note that ρ_n does not vanish at 0 and has bounded degree because $a_n = \deg u_n$ and $\omega_n \geq g_n \geq a_n - O(1)$. Now, $u_{n+1} = \varphi(u_n)$, hence

$$\beta_{n+1} + t^{\omega_{n+1}}\rho_{n+1} = \varphi(\beta_n) + t^{\omega_n}\rho_n\varphi'(\beta_n) + (t^{\omega_n}\rho_n)^2 \frac{\varphi''(\beta_n)}{2} + \cdots .$$

Taking into account that $\omega_{n+1} = g_{n+1} + O(1)$ we deduce $\omega_{n+1} = d\omega_n + O(1)$, whence we find $\varphi(\beta_n) = \beta_{n+1}$ and $\varphi^{(h)}(\beta_n) = 0$ for $1 \leq h \leq d - 1$, as required.

All of this also implies $\beta_{n+1} = \beta_n$, since β_n is unique with such a property.

P8. The opening assertion of **P7.** and the closing one together say that φ is conjugate to a power t^d, against the assumptions, which concludes the argument. □

References

1. Amerik, E., Bogomolov, F., Rovinsky, M.: Remarks on endomorphisms and rational points, pp. 22 preprint, available at arxiv.org/abs/1001.1150
2. Amerik, E.: Existence of non-preperiodic algebraic points for a rational self-map of infinite order, pp. 6, preprint, available at arxiv.org/abs/1007.1635
3. Beardon, A.F.: Symmetries of Julia sets. Bull. Lond. Math. Soc. **22**(6), 576–582 (1990)
4. Beardon, A.F.: Iteration of rational functions. In: Complex analytic dynamical systems. Graduate Texts in Mathematics, vol. 132. Springer, New York (1991)
5. Bell, J.P.: A generalised Skolem–Mahler–Lech theorem for affine varieties. J. Lond. Math. Soc. (2) **73**(2), 367–379 (2006)
6. Bell, J.P., Ghioca, D., Tucker, T.J.: The dynamical Mordell-Lang problem for étale maps. Am. J. Math. **132**(6), 1655–1675 (2010)
7. Benedetto, R., Ghioca, D., Kurlberg, P., Tucker, T.J.: A gap principle for dynamics. Compos. Math. **146**, 1056–1072 (2010)
8. Bombieri, E., Gubler, W.: Heights in diophantine geometry. In: New Mathematical Monographs, vol. 4. Cambridge University Press, Cambridge (2006)
9. Denis, L.: Géométrie et suites récurrentes. Bull. Soc. Math. France **122**(1), 13–27 (1994)
10. Evertse, J.-H., Schlickewei, H.P., Schmidt, W.M.: Linear equations in variables which lie in a multiplicative group. Ann. Math. (2) **155**(3), 807–836 (2002)

11. Faltings, G.: The general case of S. Lang's conjecture. In: Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., no. 15, Academic Press, San Diego, CA, pp. 175–182 (1994)
12. Ghioca, D., Tucker, T.J.: Periodic points, linearizing maps, and the dynamical Mordell-Lang problem. J. Number Theory **129**, 1392–1403 (2009)
13. Ghioca, D., Tucker, T.J., Zhang, S.: Towards a Dynamical Manin-Mumford conjecture. Internat. Math. Res. Notices (to appear)
14. Ghioca, D., Tucker, T.J., Zieve, M.E.: Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture. Invent. Math. **171**, 463–483 (2008)
15. Ghioca, D., Tucker, T.J., Zieve, M.E.: The Mordell–Lang question for endomorphisms of semiabelian varieties (submitted)
16. Ghioca, D., Tucker, T.J., Zieve, M.E.: Complex polynomials having orbits with infinite intersection (submitted)
17. Hrushovski, E.: Proof of Manin's theorem by reduction to positive characteristic. In: Model theory and algebraic geometry, Lecture Notes in Math., vol. 1696, pp. 197–205. Springer, Berlin (1998)
18. Jones, R.: The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc. (2) **78**(2), 523–544 (2008)
19. Lang, S.: Fundamentals of Diophantine Geometry. Springer, New York (1983)
20. Laurent, M.: Equations diophantiennes exponentielles. Invent. Math. **78**, 299–327 (1984)
21. Lech, C.: A note on recurring series. Ark. Mat. **2**, 417–421 (1953)
22. Mahler, K.: Eine arithmetische Eigenshaft der Taylor-Koeffizienten rationaler Funktionen. Proc. Kon. Nederlandsche Akad. V. Wetenschappen **38**, 50–60 (1935)
23. Medvedev, A., Scanlon, T.: Polynomial dynamics, pp. 67 (submitted). Available on http://arxiv.org/abs/0901.2352
24. Morton, P., Silverman, J.H.: Rational periodic points of rational functions. Internat. Math. Res. Notices (2), 97–110 (1994)
25. Raynaud, M.: Courbes sur une variété abélienne et points de torsion. Invent. Math. **71**(1), 207–233 (1983)
26. Raynaud, M.: Sous-variétés d'une variété abélienne et points de torsion, Arithmetic and geometry, vol. I, Progr. Math., vol. 35, pp. 327–352. Birkhäuser, Boston, MA, (1983)
27. Rivera-Letelier, J.: Dynamique des fonctions rationnelles sur des corps locaux, Astérisque **287**, 147–230 (Geometric methods in dynamics. II) (2003)
28. Robert, A.M.: A course in p-adic analysis. In: Graduate Texts in Mathematics, vol. 198. Springer, New York (2000)
29. Serre, J.-P.: Lectures on the Mordell-Weil theorem, 3rd edn. In: Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig (1997) (Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre)
30. Siegel, C.L.: Über einige Anwendungen Diophantischer Approximationen. Abh. Preuss. Akad. Wiss. Phys. Math. Kl., pp. 41–69 (1929) [Reprinted as pp. 209–266 of his Gesammelte Abhandlungen I. Springer, Berlin (1966)]
31. Silverman, J.H.: Integer points, Diophantine approximation, and iteration of rational maps. Duke Math. J. **71**(3), 793–829 (1993)
32. Skolem, T.: Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen, C. r. 8 congr. scand. à Stockholm, pp. 163–188 (1934)
33. Ullmo, E.: Positivité et discrétion des points algébriques des courbes. Ann. Math. (2) **147**(1), 167–179 (1998)
34. Vojta, P.: Integral points on subvarieties of semiabelian varieties. I. Invent. Math. **126**(1), 133–181 (1996)
35. Zhang, S.: Equidistribution of small points on abelian varieties. Ann. Math. (2) **147**(1), 159–165 (1998)
36. Zhang, S.: Distributions in algebraic dynamics. In: Survey in Differential Geometry, vol. 10, pp. 381–430. International Press, Boston (2006)