A gap principle for dynamics

Robert L. Benedetto, Dragos Ghioca, Pär Kurlberg and Thomas J. Tucker

Abstract

Let $f_1, \dots, f_g \in \mathbb{C}(z)$ be rational functions, let $\Phi = (f_1, \dots, f_g)$ denote their coordinate-wise action on $(\mathbb{P}^1)^g$, let $V \subset (\mathbb{P}^1)^g$ be a proper subvariety, and let $P = (x_1, \dots, x_g) \in (\mathbb{P}^1)^g(\mathbb{C})$ be a nonpreperiodic point for Φ. We show that if $\mathcal{S} = \{n \geqslant 0 : \Phi^n(P) \in V(\mathbb{C})\}$ does not contain any infinite arithmetic progressions, then $\mathcal{S}$ must be a very sparse set of integers. In particular, for any k and any sufficiently large N, the number of $n \leqslant N$ such that $\Phi^n(P) \in V(\mathbb{C})$ is less than $\log^k N$, where $\log^k$ denotes the k-th iterate of the log function. This result can be interpreted as an analog of the gap principle of Davenport-Roth and Mumford.

1. Introduction

The Mordell-Lang conjecture proved by Faltings [Fal94] and Vojta [Voj96] implies that if V is a subvariety of a semiabelian variety G defined over $\mathbb{C}$ such that V contains no translate of a positive-dimensional algebraic subgroup of G, then $V(\mathbb{C})$ contains at most finitely many points of any given finitely generated subgroup Γ of $G(\mathbb{C})$. A reformulation of this result says that if no translate of V contains a positive-dimensional subvariety W which is fixed by the multiplication-by-n-map (for any positive integer $n \geqslant 2$), then $V(\mathbb{C}) \cap \Gamma$ is finite (see [Abr94, Lemma 3]).

In [GT09], Ghioca and Tucker proposed a dynamical analogue of the Mordell-Lang conjecture (see also [Den94] and [Bel06]).

Conjecture 1.1. *Let X be a quasiprojective variety defined over $\mathbb{C}$, let $V \subset X$ be any subvariety, let $\Phi : X \longrightarrow X$ be any endomorphism, and let $P \in X(\mathbb{C})$. For any integer $m \geqslant 0$, denote by Φ^m the m^{th} iterate $\Phi \circ \cdots \circ \Phi$. Then $\{n \geqslant 0 : \Phi^n(P) \in V(\mathbb{C})\}$ is a union of at most finitely many arithmetic progressions and at most finitely many other integers.*

A special case of the above conjecture is our Conjecture 1.3. Before stating it, we need the following definition.

Definition 1.2. *Let X be a quasiprojective variety, let $\Phi : X \longrightarrow X$ be an endomorphism, let P be a point on X, and let $V \subset X$ be a subvariety. The* orbit *of P under Φ is $\mathcal{O}_\Phi(P) = \{\Phi^n(P) : n \geqslant 0\}$. We say V is* periodic *under Φ if there is a positive integer $N \geqslant 1$ such that $\Phi^N(V) \subseteq V$.*

We will often omit the phrase "under Φ" if the meaning is clear from context. We say that P is *preperiodic* if $\mathcal{O}_\Phi(P)$ is finite.

Conjecture 1.3. *Let X be a quasiprojective variety defined over $\mathbb{C}$, let $V \subset X$ be a subvariety, let Φ be an endomorphism of X, and let $P \in X(\mathbb{C})$. If $V(\mathbb{C}) \cap \mathcal{O}_\Phi(P)$ is an infinite set, then V contains a positive-dimensional subvariety that is periodic under Φ.*

A proof of Conjecture 1.1 would also solve Conjecture 1.3 in the affirmative. Indeed, assuming Conjecture 1.1, we see that if $V(\mathbb{C}) \cap \mathcal{O}_\Phi(P)$ is infinite, then V contains $\mathcal{O}_{\Phi^N}(\Phi^\ell(P))$ for some

2000 Mathematics Subject Classification Primary: 37P55. Secondary: 14G25, 37F10.
Keywords: p-adic dynamics, Mordell-Lang conjecture

positive integers N and ℓ. Thus, V also contains the Zariski closure W of $\mathcal{O}_{\Phi^N}(\Phi^\ell(P))$, which must have positive dimension since $\mathcal{O}_{\Phi^N}(\Phi^\ell(P))$ is infinite; clearly $\Phi^N(W) \subset W$, and hence W is periodic.

In this paper we consider the case that $X = (\mathbb{P}^1)^g$ and Φ is of the form $\Phi(z_1, \dots, z_g) = (f_1(z_1), \dots, f_g(z_g))$, and we prove a weak form of Conjecture 1.3: either the conclusion of Conjecture 1.3 holds, or the set $\{n \geqslant 0 : \Phi^n(P) \in V(\mathbb{C})\}$ is *very thin*.

Theorem 1.4. *Let $f_1, \dots, f_g \in \mathbb{C}(z)$ be rational functions, and let $\Phi = (f_1, \dots, f_g)$ denote their coordinatewise action on $(\mathbb{P}^1)^g$. Let $P = (x_1, \dots, x_g) \in (\mathbb{P}^1)^g(\mathbb{C})$, and let $V \subset (\mathbb{P}^1)^g$ be a proper subvariety such that $\Phi^n(P) \in V$ for infinitely many $n \in \mathbb{N}$. Then there exist positive integers $N, \ell \geqslant 1$ and a real number $C > 1$ such that one of the following two statements holds:*

(i) $\Phi^{\ell+mN}(P) \in V$ for all nonnegative integers m.

(ii) For any sufficiently large integers $n > m \geqslant 0$ such that $n \equiv m \pmod{N}$ and $\Phi^m(P), \Phi^n(P) \in V$, we have $n - m > C^m$.

Theorem 1.4 says that unless V contains a positive-dimensional periodic subvariety, the integers n such that $\Phi^n(P) \in V$ grow *very rapidly*. To describe this growth more explicitly we first recall Knuth's "up-arrow" notation. Given $C > 1$, define $C \uparrow\uparrow m$ for integers $m \geqslant 1$ as follows: $C \uparrow\uparrow 1 := C$; and for $m \geqslant 2$, set $C \uparrow\uparrow m := C^{C \uparrow\uparrow (m-1)}$. It follows from Theorem 1.4 that there is a real number T such that if n_i is the i^{th} integer in a given congruence class mod N for which $\Phi^{n_i}(P) \in V$, then $n_i > C \uparrow\uparrow (i - T)$ for all $i > T$, where C and N are the constants in Theorem 1.4. The growth condition might also be formulated without restricting to congruence classes: if n_i is the i^{th} integer such that $\Phi^{n_i}(P) \in V$, then $n_i > C \uparrow\uparrow \lfloor (i - T)/N \rfloor$ for $i > T$. In particular, n_i grows much faster than $\exp^k(i)$ for any $k \geqslant 1$, where $\exp^k$ denotes the k^{th} iterate of the exponential function.

We may also rephrase Theorem 1.4 in terms of extremely *slow* growth of the counting function for the number of indices n such that $\Phi^n(P) \in V$. To do so, we set the following notation. Given $Y, C > 1$, define $L_C(Y)$ to be the smallest integer m such that $(C \uparrow\uparrow m) > Y$. In particular, note that for any k, $L_C(Y)$ grows slower than the k-fold iterated logarithm.

Corollary 1.5. *Let P, Φ, and V be as in Theorem 1.4. Set $\mathcal{S} = \{n \geqslant 0 : \Phi^n(P) \in V\}$. Then either $\mathcal{S}$ contains some infinite arithmetic progression, or there are constants $N, C > 1$ such that*

$$|\{n \in \mathcal{S} : n \leqslant M\}| \leqslant N \cdot L_C(M) + O_{V,\Phi,P}(1).$$

Denis [Den94] has treated the question of the distribution of the set $\mathcal{S}$ when V does not contain a periodic subvariety. He showed, for any morphism Φ of varieties over a field of characteristic 0, that $\mathcal{S}$ cannot be "very dense of order 2" (see [Den94, Définition 2]). Theorem 1.5 shows that $\mathcal{S}$ satisfies a much stronger nondensity condition in the case that the morphism is a product of self-maps of the projective line.

When our points and maps are defined over a number field K, we may phrase this discussion in terms of (logarithmic) Weil heights; see [Sil07, Ch. 3] for background on heights. If P is not preperiodic, then the Weil height $h(\Phi^n(P))$ grows *at least* as $\deg_{\min}(\Phi)^n$, where $\deg_{\min}(\Phi) := \min_j \deg(f_j)$. Thus, we obtain:

Corollary 1.6. *Let P, Φ, and V be as in Theorem 1.4, and let n_i denote the i^{th} integer n such that $\Phi^n(P) \in V$. Assume that P and Φ are defined over some number field K, that $\deg_{\min}(\Phi) \geqslant 2$, that P is not preperiodic for Φ, and that the set $\mathcal{S} = \{n \geqslant 0 : \Phi^n(P) \in V\}$ does not contain any infinite arithmetic progressions. Then there are constants $T, N \geqslant 1$ and $C > 1$ such that $h(\Phi^{n_i}(P))$ grows faster than $C \uparrow\uparrow \lfloor (i - T)/N \rfloor$; in particular, faster than $\exp^k(i)$ for any $k \geqslant 1$.*

This growth is much more rapid than that of the "gap principles" of Mumford [Mum65] and Davenport-Roth [DR55]. If $\mathcal{C}$ is a curve of genus greater than 1, Mumford showed that there are

constants $a, b > 0$ such that if we order the rational points of $\mathcal{C}$ according to Weil height, then the i^{th} point has Weil height at least e^{a+bi}. In his proof, he embedded points of $\mathcal{C}$ into $\mathbb{R}^d$; *Mumford's gap principle* roughly states that there is a constant $C > 1$ such that if $v_1, v_2 \in \mathbb{R}^d$ are the images of two points on the curve lying in a small sector, then either $|v_1| > C \cdot |v_2|$ or $|v_2| > C \cdot |v_1|$. Similarly, in our Theorem 1.4, two indices n_1, n_2 lying in the same congruence class modulo N can be considered analogous to two vectors v_1, v_2 lying in a small sector. By this analogy, given that Faltings [Fal83] later proved that the curve $\mathcal{C}$ has only finitely many rational points, Theorem 1.4 can be viewed as evidence that Conjecture 1.3 is true, at least for coordinatewise maps on $(\mathbb{P}^1)^g$.

In fact, in Theorem 4.1, we will show that the pair of constants (N, C) in the conclusion of Theorem 1.4 may be replaced by the pair $(eN, C^{e-\epsilon})$, for any positive integer e and any positive real number $\epsilon > 0$. Hence, by the same analogy to Mumford's gap principle, we prove that "the smaller the angles" between two indices, "the larger the gap" between them. Further, if V is a curve defined over a number field K, we give a different way of forcing C to be large while controlling the size of N— in Theorem 6.1 we show that for any $\epsilon > 0$, we can take $C > p - \epsilon$ and $N = O(p^{2[K:\mathbb{Q}]})$ for an infinite sequence of primes p.

Other partial results towards Conjecture 1.1 may be found in [Bel06, GT09, GTZ08, BGKT, BGT]. In addition, [GTZ] discusses a generalization of Conjecture 1.1 for orbits of points under the action of a commutative, finitely generated semigroup of endomorphisms of X, which is itself a generalization of the classical Mordell-Lang conjecture. Conjecture 1.1 also fits into Zhang's far-reaching system of dynamical conjectures (see [Zha06]). Zhang's conjectures include dynamical analogues of the Manin-Mumford and Bogomolov conjectures for abelian varieties (now theorems of [Ray83a, Ray83b], [Ull98] and [Zha98]).

Our proof of Theorem 1.4 uses p-adic dynamics. First we find a suitable prime number p such that V, Φ, and P are defined over $\mathbb{Q}_p$, and Φ has good reduction modulo p. Then, using a one-variable result of Rivera-Letelier [RL03], we carefully choose a positive integer N, and for each $\ell = 0, \ldots, N-1$, we construct finitely many multivariable p-adic power series $G_{H,\ell}(z_0, z_1, \ldots, z_m)$ such that for n sufficiently large, we have $\Phi^{\ell+nN}(P) \in V$ if and only if $G_{H,\ell}(n, p^n, p^{2^n}, \ldots, p^{m^n}) = 0$ for all H. We then show that either $G_{H,\ell}$ is identically zero for all H (which implies conclusion (i) of Theorem 1.4), or the integers n with $\Phi^{\ell+nN}(P) \in V(\mathbb{C})$ grow as in conclusion (ii).

For each prime number p, we also construct an example (see Proposition 7.1) of a power series $f \in \mathbb{Z}_p[[z]]$ such that for an infinite increasing sequence $\{n_k\}_{k \geqslant 1} \subset \mathbb{N}$ we have $f(p^{n_k}) = n_k$, and moreover $n_{k+1} < n_k + p^{2n_k}$ for each $k \geqslant 1$. This example shows that Theorem 1.4 cannot be improved merely by sharpening our p-adic methods; some new technique would be required for a full proof of Conjecture 1.3.

The outline of the paper is as follows. In Section 2 we present some Lemmas from p-adic dynamics, and in Section 3 we state and prove a technical Lemma on the rapid growth of integer zeros of certain p-adic functions. In Section 4 we prove Theorem 1.4, in Section 5 we prove Corollary 1.5, and in Section 6 we prove Theorem 6.1. Finally, in Section 7 we prove Proposition 7.1, which shows that our Theorem 1.4 cannot be improved through purely p-adic analytic methods.

Acknowledgements: The authors are very grateful to the referee for a careful reading of the paper and for many comments and suggestions that improved the exposition.

R.B. gratefully acknowledges the support of NSF Grant DMS-0600878. Research of D.G. was partially supported by a grant from the NSERC. P.K. was partially supported by grants from the Göran Gustafsson Foundation, the Knut and Alice Wallenberg foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council. T.T. was partially supported by NSA Grant 06G-067 and NSF Grant DMS-0801072.

2. Background on p-adic dynamics

Fix a prime p. As usual, $\mathbb{Z}_p$ will denote the ring of p-adic integers, $\mathbb{Q}_p$ will denote the field of p-adic rationals, and $\mathbb{C}_p$ will denote the completion of an algebraic closure of $\mathbb{Q}_p$. Given a point $y \in \mathbb{C}_p$ and a real number $r > 0$, write

$$D(y,r) = \{x \in \mathbb{C}_p : |x-y|_p < r\}, \quad \overline{D}(y,r) = \{x \in \mathbb{C}_p : |x-y|_p \leqslant r\}$$

for the open and closed disks, respectively, of radius r about y in $\mathbb{C}_p$.

Write $[y] \subseteq \mathbb{P}^1(\mathbb{C}_p)$ for the residue class of a point $y \in \mathbb{P}^1(\mathbb{C}_p)$. That is, $[y] = D(y,1)$ if $|y| \leqslant 1$, or else $[y] = \mathbb{P}^1(\mathbb{C}_p) \setminus \overline{D}(0,1)$ if $|y| > 1$.

The action of a p-adic power series $f \in \mathbb{Z}_p[[z]]$ on $D(0,1)$ is either attracting (i.e., f contracts distances) or quasiperiodic (i.e., f is distance-preserving), depending on its linear coefficient. Rivera-Letelier gives a more precise description of this dichotomy in [RL03, Sections 3.1 and 3.2]. The following two Lemmas essentially reproduce his Propositions 3.3 and 3.16, but we also verify that the power series he defines also have coefficients in $\mathbb{Q}_p$, not just in $\mathbb{C}_p$.

Lemma 2.1. *Let $f(z) = a_0 + a_1 z + a_2 z^2 + \cdots \in \mathbb{Z}_p[[z]]$ be a nonconstant power series with $|a_0|_p, |a_1|_p < 1$. Then there is a point $y \in p\mathbb{Z}_p$ such that $f(y) = y$, and $\lim_{n\to\infty} f^n(z) = y$ for all $z \in D(0,1)$. Write $\lambda = f'(y)$; then $|\lambda|_p < 1$, and:*

(i) *(Attracting). If $\lambda \neq 0$, then there is a radius $0 < r < 1$ and a power series $u \in \mathbb{Q}_p[[z]]$ mapping $\overline{D}(0,r)$ bijectively onto $\overline{D}(y,r)$ with $u(0) = y$, such that for all $z \in D(y,r)$ and $n \geqslant 0$,*

$$f^n(z) = u(\lambda^n u^{-1}(z)).$$

(ii) *(Superattracting). If $\lambda = 0$, then write f as*

$$f(z) = y + c_m(z-y)^m + c_{m+1}(z-y)^{m+1} + \cdots \in \mathbb{Z}_p[[z-y]]$$

with $m \geqslant 2$ and $c_m \neq 0$. If c_m has an $(m-1)$-st root in $\mathbb{Z}_p$, then there are radii $0 < r, s < 1$ and a power series $u \in \mathbb{Q}_p[[z]]$ mapping $\overline{D}(0,s)$ bijectively onto $\overline{D}(y,r)$ with $u(0) = y$, such that for all $z \in D(y,r)$ and $n \geqslant 0$,

$$f^n(z) = u\Big((u^{-1}(z))^{m^n}\Big).$$

Proof. Applying the Weierstrass Preparation Theorem to $f(z) - z$ (or equivalently, by inspection of the Newton polygon), f has a $\mathbb{Q}_p$-rational fixed point $y \in D(0,1)$; that is, $y \in p\mathbb{Z}_p$. Clearly $\lambda = f'(y)$ is also in $p\mathbb{Z}_p$. Replacing $f(z)$ by $f(z+y) - y$ (and, ultimately, replacing $u(z)$ by $u(z) + y$), we may assume hereafter that $y = 0$. By [RL03, Proposition 3.2(i)], $\lim_{n\to\infty} f^n(z) = 0$ for all $z \in D(0,1)$.

If $\lambda \neq 0$, then Rivera-Letelier defines $u^{-1}(z) := \lim_{n\to\infty} \lambda^{-n} f^n(z)$ and proves in [RL03, Proposition 3.3(i)] that it has an inverse $u(z)$ under composition that satisfies the desired properties for some radius $0 < r < 1$. Note that $f \in \mathbb{Q}_p[[z]]$, and hence $\lambda^{-n} f^n \in \mathbb{Q}_p[[z]]$ for all $n \geqslant 1$. Thus, $u^{-1} \in \mathbb{Q}_p[[z]]$, and therefore $u \in \mathbb{Q}_p[[z]]$ as well.

If $\lambda = 0$, then choose $\gamma \in \mathbb{Z}_p \smallsetminus \{0\}$ with $\gamma^{m-1} = c_m$, according to the hypotheses. Define $\tilde{f}(z) := \gamma f(\gamma^{-1} z)$, so that $\tilde{f}(z) = z^m(1 + g(z))$, with $g \in z\mathbb{Q}_p[[z]]$. Rivera-Letelier defines

$$h(z) := \sum_{n \geqslant 0} m^{-n-1} \log\Big(1 + g(\tilde{f}^n(z))\Big) \in z\mathbb{Q}_p[[z]]$$

in [RL03, Proposition 3.3(ii)], where $\log(1+z) = z - z^2/2 + z^3/3 - \cdots$. He then sets $\tilde{u}^{-1}(z) := z \exp(h(z))$, where $\exp(z) = 1 + z + z^2/2! + \cdots$, and shows that the inverse $\tilde{u}$ of $\tilde{u}^{-1}$ has all the desired properties for $\tilde{f}$; note also that $\tilde{u} \in \mathbb{Q}_p[[z]]$, because $\log(1+\cdot)$, $\exp$, g, $\tilde{f} \in \mathbb{Q}_p[[z]]$. Hence, $u(z) = \gamma^{-1}\tilde{u}(z) \in \mathbb{Q}_p[[z]]$ has the desired properties for f, mapping some disk $\overline{D}(0,s)$ bijectively

onto some disk $\overline{D}(y,r) \subseteq D(0,1)$. Finally, the radius s must be less than 1, or else $u(1) \neq y$ will be fixed by f, contradicting the fact that $\lim_{n\to\infty} f^n(u(1)) = y$. □

LEMMA 2.2. *Let $f(z) = a_0 + a_1 z + a_2 z^2 + \cdots \in \mathbb{Z}_p[[z]]$ be a nonconstant power series with $|a_0|_p < 1$ but $|a_1|_p = 1$. Then for any nonperiodic $x \in p\mathbb{Z}_p$, there are: an integer $k \geqslant 1$, radii $0 < r < 1$ and $s \geqslant |k|_p$, and a power series $u \in \mathbb{Q}_p[[z]]$ mapping $\overline{D}(0,s)$ bijectively onto $\overline{D}(x,r)$ with $u(0) = x$, such that for all $z \in \overline{D}(x,r)$ and $n \geqslant 0$,*

$$f^{nk}(z) = u(nk + u^{-1}(z)).$$

Proof. Because $f \in \mathbb{Z}_p[[z]]$ with $|c_1|_p = 1$ and $|c_0|_p < 1$, f maps $D(0,1)$ bijectively onto itself. Therefore, by [RL03, Corollaire 3.12], f is quasiperiodic, which means in particular that for some $0 < r < 1$ and for some positive integer k, the function

$$f_*(z) := \lim_{|n|_p \to 0} \frac{f^{nk}(z) - z}{nk}$$

converges uniformly on $\overline{D}(x,r)$ to a power series in $\mathbb{C}_p[[z-x]]$. In fact, $f_* \in \mathbb{Q}_p[[z-x]]$, because $(f^{nk}(z) - z)/(nk) \in \mathbb{Q}_p[[z-x]]$ for every n.

Since x is not periodic, $f_*(x) \neq 0$, by [RL03, Proposition 3.16(1)]. Define $u^{-1} \in \mathbb{Q}_p[[z-x]]$ to be the antiderivative of $1/f_*$ with $u^{-1}(x) = 0$. Because $(u^{-1})'(x) \neq 0$, we may decrease r so that u^{-1} is one-to-one on $\overline{D}(x,r)$. Also replace k by a multiple of itself so that $f^k(x) \in \overline{D}(0,r)$, and write $\overline{D}(0,s) := u^{-1}(\overline{D}(x,r))$. The proof of [RL03, Proposition 3.16(2)] shows that the inverse u of u^{-1}, which must also have coefficients in $\mathbb{Q}_p$, satisfies the desired properties. □

Remark 2.3. In fact, the integer k in Lemma 2.2 is at most p, at least in the case that $p > 3$; see Proposition 6.4.

Finally, we will also use the following basic result on p-adic analysis.

LEMMA 2.4. *Let $g \in \mathbb{Q}_p[[t]]$ be a nontrivial power series converging on $\overline{D}(0,1)$. Then there exists $s \in (0,1]$ such that for all $\alpha \in \overline{D}(0,1)$, there is at most one point in $\overline{D}(\alpha,s)$ at which g vanishes.*

Proof. By the Weierstrass Preparation Theorem, because g is nontrivial and converges on the closed unit disk, it can have only finitely many zeros $\{\alpha_i\}_{1\leqslant i\leqslant r}$ in $\overline{D}(0,1)$. If $r = 0$, we may set $s = 1$; otherwise, we may set $s = \frac{1}{p}\min_{1\leqslant i<j\leqslant r} |\alpha_i - \alpha_j|_p$. □

3. A growth lemma

We will also need a technical lemma about the growth of certain solutions of multivariate p-adic power series. Before stating it, we set some notation. First, we fix $m \geqslant 1$, and with $\mathbb{N} = \{0,1,2,\ldots\}$ denoting the natural numbers, we order $\mathbb{N}^m$ by lexicographic ordering reading right-to-left. That is, $(b_1,\ldots,b_m) \prec (b'_1,\ldots,b'_m)$ if either $b_m < b'_m$, or $b_m = b'_m$ but $b_{m-1} < b'_{m-1}$, or $b_m = b'_m$ and $b_{m-1} = b'_{m-1}$ but $b_{m-2} < b'_{m-2}$, etc. Note that this order $\prec$ gives a well-ordering of $\mathbb{N}^m$.

Given a power series $G \in \mathbb{Q}_p[[z_0, z_1, \ldots, z_m]]$, we may write G uniquely as

$$G(z_0, z_1, \ldots, z_m) = \sum_{w\in\mathbb{N}^m} g_w(z_0) z^w, \tag{3.1}$$

where $g_w \in \mathbb{Q}_p[[z_0]]$, and for $w = (a, b_2, \ldots, b_m) \in \mathbb{N}^m$, z^w denotes

$$z^w = z_1^a z_2^{b_2} z_3^{b_3} \cdots z_m^{b_m}.$$

Armed with this notation, we can now state our Lemma.

Lemma 3.1. *Let $G(z_0, z_1, z_2, \ldots, z_m) \in \mathbb{Q}_p[[z_0, z_1, z_2, \ldots, z_m]]$ be a nontrivial power series in $m+1 \geqslant 1$ variables. Write $G = \sum_w g_w(z_0) z^w$ as in equation (3.1), and let $v \in \mathbb{N}^m$ be the minimal index with respect to $\prec$ such that $g_v \neq 0$. Assume that g_v converges on $\overline{D}(0,1)$, and let s be a positive real number such that for all $\alpha \in \mathbb{Z}_p$, g_v does not vanish at more than one point of the disk $\overline{D}(\alpha, s)$, as in Lemma 2.4. Assume also that there exists $B > 0$ such that for each $w \succ v$, all coefficients of g_w have absolute value at most $p^{B|w|}$.*

Then there exists $C > 1$ with the following property: If $\alpha \in \overline{D}(0,1)$, and if $\{n_i\}_{i \geqslant 1}$ is a strictly increasing sequence of positive integers such that for each $i \geqslant 1$,

(a) $|n_i - \alpha|_p \leqslant s$, *and*
(b) $G(n_i, p^{n_i}, p^{2n_i}, p^{3n_i}, ..., p^{m^{n_i}}) = 0$,

then $n_{i+1} - n_i > C^{n_i}$ for all sufficiently large i.

Proof. If $g_w = 0$ for all $w \neq v$, then $G = g_v(z_0) z^v$. By hypothesis (b), then, the one-variable nonzero power series $g_v(z_0)$ vanishes at all points of the sequence $\{n_i\}_{i \geqslant 1}$, a contradiction; hence, no such sequence exists. (In particular, if $m = 0$, then G is a nontrivial power series in the one variable z_0, and therefore G vanishes at only finitely many points n_i.) Thus, we may assume that g_w is nonzero for some $w \succ v$.

Next, for any m-tuple $w = (a, b_2, \ldots, b_m) \in \mathbb{N}^m$ and $n \geqslant 0$, set $|w| := a + b_2 + \cdots + b_m$, and define the function $f_w : \mathbb{N} \to \mathbb{N}$ by

$$f_w(n) = an + \sum_{j=2}^{m} b_j j^n. \tag{3.2}$$

For any $w, w' \in \mathbb{N}^m$, note that $w \prec w'$ if and only if $f_w(n)$ grows more slowly than $f_{w'}(n)$ as $n \to \infty$.

Claim 3.2. *For any $A > 0$, there is an integer $M = M(v, A) \geqslant 0$ such that for each $w \succ v$ and $n \geqslant M$,*

$$f_w(n) - f_v(n) \geqslant n + A(|w| - |v| - 1).$$

Proof of Claim 3.2.. Write $v = (a, b_2, ..., b_m)$, and choose $M \geqslant A$ large enough so that $j^M \geqslant (a+1)M + \sum_{k=2}^{j-1} b_k k^M$ for all $j = 2, \ldots, m$. Write $w = (a', b_2', .., b_m')$. Then

$$f_w(n) - f_v(n) = (a' - a)n + (b_2' - b_2)2^n + ... + (b_m' - b_m)m^n.$$

We consider two cases:

Case 1. If $b_k' = b_k$ for each $k = 2, .., m$, then $a' > a$, and therefore

$$f_w(n) - f_v(n) - n = (a' - a - 1)n \geqslant (a' - a - 1)A = A(|w| - |v| - 1)$$

for $n \geqslant M$, because $M \geqslant A$.

Case 2. Otherwise, there exists $k = 2, .., m$ such that $b_k' > b_k$. Let j be the largest such k, so that $b_k' = b_k$ for $k > j$. Then

$$\begin{aligned} f_w(n) - f_v(n) - A|w| + A|v| &= (a' - a)(n - A) + \sum_{k=2}^{j-1} (b_k' - b_k)(k^n - A) + (b_j' - b_j)(j^n - A) \\ &\geqslant -an - \sum_{k=2}^{j-1} b_k k^n + j^n - A \geqslant n - A, \end{aligned}$$

where the first inequality is because $n \geqslant A$ and $b_j' - b_j \geqslant 1$, and the second is because $n \geqslant M$. The proof of Claim 3.2 is now complete. □

By hypothesis (b), for any i such that $n_i \geqslant M(v,B)$, we have

$$|g_v(n_i)|_p = \left| \sum_{w \succ v} g_w(n_i) p^{f_w(n_i)-f_v(n_i)} \right|_p \leqslant p^{-n_i+B|v|+B}, \tag{3.3}$$

where the inequality is by Claim 3.2, the fact that $|n_i|_p \leqslant 1$, and the fact that the absolute values of all coefficients of g_w are at most $p^{B|w|}$. Let $\beta \in \overline{D}(\alpha,s) \cap \mathbb{Z}_p$ be a limit point of the sequence $\{n_i\}_{i \geqslant 1}$. Then by inequality (3.3), we have $g_v(\beta) = 0$. Thus, g_v can be written as

$$g_v(z) = \sum_{i \geqslant \delta} c_i (z-\beta)^i,$$

where $\delta \geqslant 1$ and $c_\delta \neq 0$. In fact, we must have $|c_\delta|_p s^\delta > |c_i|_p s^i$ for all $i > \delta$; otherwise, inspection of the Newton polygon shows that g_v would have a zero besides β in $\overline{D}(\alpha,s)$. Thus, for i sufficiently large (i.e., such that $n_i \geqslant M(v,B)$), we have

$$|c_\delta (n_i - \beta)^\delta|_p = |g_v(n_i)|_p \leqslant p^{-n_i+O(1)},$$

by hypothesis (a) and inequality (3.3), and hence

$$|n_i - \beta|_p \leqslant |c_\delta|_p^{-1/\delta} p^{-n_i/\delta + O(1)}. \tag{3.4}$$

It follows that

$$n_{i+1} \equiv n_i \mod p^{\lfloor n_i/\delta - O(1) \rfloor}. \tag{3.5}$$

Hence, if we choose C such that $1 < C < p^{1/\delta}$, we have $n_{i+1} - n_i > C^{n_i}$ for i sufficiently large, as desired. □

Remark 3.3. Lemma 3.1 holds also if G is defined over a finite extension K of $\mathbb{Q}_p$; the only significant change is that the constant C will depend also on the ramification index e of $K/\mathbb{Q}_p$.

4. Proof of Theorem 1.4

Proof. If any x_j (without loss, x_g) is preperiodic under f_j, choose m such that $x_g' := f_g^m(x_g)$ is periodic under f_g, and consider the action of $\Phi' := (f_1, \ldots, f_{g-1})$ on $(\mathbb{P}^1)^{g-1}$, with $V' := V \cap \{z_g = x_g'\}$ viewed as a subvariety of $(\mathbb{P}^1)^{g-1}$. By this reduction we may assume, without loss of generality, that no x_j is preperiodic.

Step (i). Our first goal is to find an appropriate prime p so that we may work over $\mathbb{Z}_p$.

Choose homogeneous coordinates for each $\mathbb{P}^1$, so that we may write each f_j as $f_j([a:b]) = [\phi_j(a,b) : \psi_j(a,b)]$ for homogeneous relatively prime polynomials $\phi_j, \psi_j \in \mathbb{C}[a,b]$; write P in these coordinates as well. Let $\mathcal{V}$ be a finite set of polynomials (in g pairs of homogeneous variables) generating the vanishing ideal of the variety V. Let R_1 be the subring of $\mathbb{C}$ generated by the coordinates of P, the coordinates of all critical points of each f_j, the coefficients of each polynomial $H \in \mathcal{V}$, the coefficients of each ϕ_j and ψ_j, and the reciprocals

$$1/\operatorname{Res}(\phi_1,\psi_1), \ldots, 1/\operatorname{Res}(\phi_g,\psi_g)$$

of the resultants $\operatorname{Res}(\phi_1,\psi_1), \ldots, \operatorname{Res}(\phi_g,\psi_g)$.

Each superattracting periodic point Q of any f_j of period κ_j has a critical point in its cycle; in particular, there are only finitely many such points, and they are all defined over R_1. (Note that in contrast to the attracting case, our upcoming choice of a prime p will not affect whether a periodic point Q is superattracting.) For each such point, then, we may choose an R_1-rational local coordinate $x_{j,Q}$ at Q, and write $f_j^{\kappa_j}$ as

$$f_j^{\kappa_j}(x_{j,Q}) = c_{j,Q} x_{j,Q}^{m_{j,Q}} + O(x_{j,Q}^{m_{j,Q}+1}), \tag{4.1}$$

where $m_{j,Q} \geqslant 2$ and $c_{j,Q} \neq 0$.

Let R_2 be the subring of $\mathbb{C}$ generated by R_1 and all the $(m_{j,Q}-1)$-st roots of $c_{j,Q}$, for all superattracting points Q of f_j, where $c_{j,Q}$ and $m_{j,Q}$ are as in (4.1).

Clearly, R_2 is a finitely generated $\mathbb{Z}$-algebra. By [Bel06, Lemma 3.1] (see also [Lec53]), we can embed R_2 into $\mathbb{Z}_p$ for some prime p. Thus, we may consider P, Φ, and $\mathcal{V}$ to be defined over $\mathbb{Z}_p$. Because the resultants $\mathrm{Res}(\phi_j, \psi_j)$ are all mapped to units in $\mathbb{Z}_p$, each map f_j has good reduction, i.e., reducing f_j modulo p gives an endomorphism of $\mathbb{P}^1$ defined over $\mathbb{F}_p$. The $(m_{j,Q}-1)$-st roots of $c_{j,Q}$ will be needed in Step (ii), to deal with superattracting points.

Step (ii). Next, we will apply Lemmas 2.1 and 2.2 to produce certain power series $u_j(z)$, points $\mu_j \in \mathbb{Q}_p$ in the domain of u_j, and various preliminary quantities.

Write $P := (x_1, \ldots, x_g) \in (\mathbb{P}^1)^g(\mathbb{Z}_p)$. There are only $p+1$ residue classes in $\mathbb{P}^1(\mathbb{Z}_p)$; hence, for each $j = 1, \ldots, g$, there are integers $k_{j,0} \geqslant 1$ and $\ell_{j,0} \geqslant 0$ such that $f_j^{k_{j,0}}$ maps the residue class $[f_j^{\ell_{j,0}}(x_j)]$ into itself. By a $PGL(2, \mathbb{Z}_p)$-change of coordinates at each j, we may assume that $f_j^{\ell_{j,0}}(x_j) \in p\mathbb{Z}_p$, and therefore $f_j^{k_{j,0}}$ may be written as a nonconstant power series in $\mathbb{Z}_p[[z]]$ mapping $\overline{D}(0,1)$ to itself.

If $|(f_j^{k_{j,0}})'(f_j^{\ell_{j,0}}(x_j))|_p < 1$ (i.e., the attracting or superattracting case, in the language of Section 2), we may apply Lemma 2.1. (In the superattracting case we are using the fact that the corresponding coefficient $c_{j,Q}$ has an $(m_{j,Q}-1)$-st root in $\mathbb{Q}_p$. Although the new local coordinate $\tilde{x}_{j,Q}$ at the superattracting point may differ from the local coordinate $x_{j,Q}$ of Step (i), both are defined over $\mathbb{Q}_p$. Thus, there is some $\gamma_{j,Q} \in \mathbb{Q}_p^\times$ such that $x_{j,Q} = \gamma_{j,Q}\tilde{x}_{j,Q} + O(\tilde{x}_{j,Q}^2)$, and the expansion $c_{j,Q}x_{j,Q}^{m_{j,Q}} + O(x_{j,Q}^{m_{j,Q}+1})$ from (4.1) becomes $\gamma_{j,Q}^{m_{j,Q}-1}c_{j,Q}\tilde{x}_{j,Q}^{m_{j,Q}} + O(\tilde{x}_{j,Q}^{m_{j,Q}+1})$. Hence, the integer $m_{j,Q}$ is preserved, and the lead coefficient still has all its $(m_{j,Q}-1)$-st roots in $\mathbb{Q}_p$. Of course, those roots are in fact in $\mathbb{Z}_p$, because our choice of coordinates forced $f_j^{k_{j,0}} \in \mathbb{Z}_p[[z]]$.)

Lemma 2.1 yields that there is a point $y_j \in D(0,1)$ fixed by $f_j^{k_{j,0}}$, along with radii r_j and s_j (where $s_j := r_j$ in the non-superattracting case), and an associated power series $u_j \in \mathbb{Q}_p[[z]]$. Set $k_{j,1} = k_{j,0}$ and $\ell_{j,1} = \ell_{j,0} + n_j k_{j,1}$ for a suitable integer $n_j \geqslant 0$ so that $f_j^{\ell_{j,1}}(x_j) \in \overline{D}(y_j, r_j)$. Define $\lambda_{j,1} := (f_j^{k_{j,1}})'(y_j)$ to be the multiplier of the point y_j, so that $|\lambda_{j,1}|_p < 1$. Define $\mu_j := u_j^{-1}(f_j^{\ell_{j,1}}(x_j))$; note that $\mu_j \in p\mathbb{Z}_p$, because $s_j < 1$. In addition, $\mu_j \neq 0$, because u_j is bijective and $u_j(0) = y_j$ is fixed by f_j, while $u_j(\mu_j) = f_j^{\ell_{j,1}}(x_j)$ is not.

If $|(f_j^{k_{j,0}})'(f_j^{\ell_{j,0}}(x_j))|_p = 1$ (i.e., the quasiperiodic case, in the language of Section 2), apply Lemma 2.2 to $f_j^{k_{j,0}}$ and the point $f_j^{\ell_{j,0}}(x_j)$ to obtain radii r_j and s_j and a power series u_j. Define $\mu_j := u_j^{-1}(f_j^{\ell_{j,0}}(x_j))$, and set $\ell_{j,1} = \ell_{j,0}$ and $k_{j,3} = n_j k_{j,0}$, for a suitable integer $n_j \geqslant 1$ so that $f_j^{k_{j,3}+\ell_{j,1}}(x_j) \in \overline{D}(f_j^{\ell_{j,1}}(x_j), r_j)$. (The existence of such an integer n_j follows easily from Lemma 2.2. Meanwhile, the jump from a subscript of 0 to 3 is because certain complications, to be addressed in Steps (iii) and (iv), do not arise in the quasiperiodic case.) Note that $f_j^{\ell_{j,1}+nk_{j,3}}(x_j)$ may be expressed as a power series in the integer $n \geqslant 0$; specifically, $f_j^{\ell_{j,1}+nk_{j,3}}(x_j) = u_j(nk_{j,3} + \mu_j)$.

Step (iii). In this step, we consider only the case that $0 < |\lambda_{j,1}|_p < 1$ (i.e., attracting but not superattracting). We will express certain functions of n as power series in n and p^n.

Write $\lambda_{j,1} = \alpha_j p^{e_{j,1}}$, where $e_{j,1} \geqslant 1$ and $\alpha_j \in \mathbb{Z}_p^\times$. If α_j is a root of unity, we can choose an integer $M_{j,1} \geqslant 1$ such that $\alpha_j^{M_{j,1}} = 1$. If α_j is not a root of unity, it is well known that there is an integer $M_{j,1} \geqslant 1$ such that $\alpha_j^{nM_{j,1}}$ can be written as a power series in n with coefficients in $\mathbb{Z}_p$. (For example, apply Lemma 2.2 to the function $z \mapsto \alpha_j z$ and the point p. In fact, by Theorem 6.2, we can choose $M_{j,1}$ to be the smallest positive integer such that $|\alpha_j^{M_{j,1}} - 1|_p < 1$, so that $M_{j,1} | (p-1)$.)

Either way, set

$$k_{j,3} := M_{j,1}k_{j,1}, \quad \lambda_{j,2} := \lambda_{j,1}^{M_{j,1}}, \quad \text{and} \quad e_{j,2} := M_{j,1}e_{j,1}.$$

(The subscript again jumps to 3 because of the complications of Step (iv).) Thus, we can write

$$\lambda_{j,2}^n = (p^n)^{e_{j,2}} g_{j,1}(n) \qquad \text{for all integers } n \geqslant 0, \tag{4.2}$$

for some power series $g_{j,1}(z) \in \mathbb{Z}_p[[z]]$.

Step (iv). In this step, we consider only the superattracting case, that $\lambda_{j,1} = 0$, and we will express certain functions of n as power series in n, p^n, and $p^{m_{j,2}^n}$, where $m_{j,2} \geqslant 2$ is a certain integer.

Write the integer $m_j := m_{j,Q} \geqslant 2$ (for the unique superattracting point Q of f_j in $D(0,1)$, as in Lemma 2.1(ii) and equation (4.1)) as $m_j = a_j p^{b_j}$, for integers $a_j \geqslant 1$ and $b_j \geqslant 0$, with $p \nmid a_j$. Then as in Step (iii), we can find a positive integer $M_{j,1}$ such that $a_j^{nM_{j,1}}$ can be written as a power series in n with coefficients in $\mathbb{Z}_p$. Set

$$k_{j,2} := M_{j,1}k_{j,1} \quad \text{and} \quad m_{j,1} := m_j^{M_{j,1}}.$$

Then $m_{j,1}^n$ can be written as a power series in n and p^n, with coefficients in $\mathbb{Z}_p$.

In addition, recall that $\mu_j = u_j^{-1}(f^{\ell_{j,1}}(x_j))$ satisfies $0 < |\mu_j|_p < 1$; thus, we can write $\mu_j = \beta_j p^{e_j}$, where $e_j \geqslant 1$ and $\beta_j \in \mathbb{Z}_p^\times$. If β_j is a root of unity with, say, $\beta_j^{M_{j,2}} = 1$ for some positive integer $M_{j,2}$, choose a positive integer $M_{j,3}$ so that $M_{j,2} | \big(m_{j,1}^{2M_{j,3}} - m_{j,1}^{M_{j,3}}\big)$. Set

$$k_{j,3} := M_{j,3}k_{j,2} \quad \text{and} \quad m_{j,2} := m_{j,1}^{M_{j,3}},$$

and note that $\beta_j^{m_{j,2}^n}$ is constant in n.

On the other hand, if β_j is not a root of unity, then as in Step (iii), there is an integer $1 \leqslant M'_{j,2} \leqslant p-1$ such that $\beta_j^{nM'_{j,2}}$ can be written as a power series in n over $\mathbb{Z}_p$. As above, choose a positive integer $M'_{j,3}$ such that $M'_{j,2} | \big(m_{j,1}^{2M'_{j,3}} - m_{j,1}^{M'_{j,3}}\big)$, and set

$$k_{j,3} := M'_{j,3}k_{j,2} \quad \text{and} \quad m_{j,2} := m_{j,1}^{M'_{j,3}}.$$

Then $m_{j,2}^n \equiv m_{j,2} \pmod{M'_{j,2}}$ for all $n \in \mathbb{N}$, and therefore

$$\beta_j^{m_{j,2}^n} = \beta_j^{m_{j,2}} \cdot \beta_j^{m_{j,2}^n - m_{j,2}} = \beta_j^{m_{j,2}} \cdot \Big(\beta_j^{M'_{j,2}}\Big)^{(m_{j,2}^n - m_{j,2})/M'_{j,2}}$$

can be written as a power series in $(m_{j,2}^n - m_{j,2})/M'_{j,2}$ with coefficients in $\mathbb{Z}_p$. Using the fact that $p \nmid M'_{j,2}$, and expressing $m_{j,2}^n = (m_{j,1}^n)^{M'_{j,3}}$ as a power series in n and p^n with coefficients in $\mathbb{Z}_p$, we conclude that $\beta_j^{m_{j,2}^n}$ can in fact be written as a power series in n and p^n, with coefficients in $\mathbb{Z}_p$.

Thus, whether or not β_j is a root of unity, we can write

$$\mu_j^{m_{j,2}^n} = (p^{m_{j,2}^n})^{e_j} g_{j,1}(n, p^n) \qquad \text{for all integers } n \geqslant 0, \tag{4.3}$$

for some power series $g_{j,1}(z_0, z_1) \in \mathbb{Z}_p[[z_0, z_1]]$.

Step (v). Let $k := \operatorname{lcm}(k_{1,3}, \dots, k_{g,3}) \geqslant 1$; this will essentially be our value of N in the statement of Theorem 1.4 except for one more change in Step (vii). In the attracting case, we set

$$\lambda_{j,3} := \lambda_{j,2}^{k/k_{j,3}}, \quad e_{j,3} := \frac{k}{k_{j,3}} e_{j,2}, \quad \text{and} \quad g_{j,2}(z) := \big(g_{j,1}(z)\big)^{k/k_{j,3}} \in \mathbb{Z}_p[[z]];$$

and in the superattracting case, we set

$$m_{j,3} := m_{j,2}^{k/k_{j,3}} \quad \text{and} \quad g_{j,2}(z_0, z_1) := g_{j,1}\Big(\frac{k}{k_{j,3}} z_0, z_1^{k/k_{j,3}}\Big) \in \mathbb{Z}_p[[z_0, z_1]].$$

With this new notation, it follows from Steps (ii)–(iv) that for any integer $n \geqslant 0$,

(1) $f_j^{\ell_{j,1}+nk}(x_j) = u_j(nk + \mu_j)$, if $f^{\ell_{j,1}}(x_j)$ lies in a quasiperiodic residue class;

(2) $f_j^{\ell_{j,1}+nk}(x_j) = u_j\big(\lambda_{j,3}^n \mu_j\big) = u_j\big((p^n)^{e_{j,3}} g_{j,2}(n)\mu_j\big)$, if $f^{\ell_{j,1}}(x_j)$ lies in an attracting residue class; and

(3) $f_j^{\ell_{j,1}+nk}(x_j) = u_j\big(\mu_j^{m_{j,3}^n}\big) = u_j\Big(\big(p^{m_{j,3}^n}\big)^{e_j} g_{j,2}(n, p^n)\Big)$, if $f^{\ell_{j,1}}(x_j)$ lies in an superattracting residue class,

where $\mu_j = u_j^{-1}(f^{\ell_{j,1}}(x_j))$ as in Step (ii). In particular, in all three cases, we have expressed $f_j^{\ell_{j,1}+nk}(x_j)$ as a power series in n, p^n, and, if needed, $p^{m_{j,3}^n}$.

Let $L = \max\{\ell_{1,1}, \ldots, \ell_{g,1}\}$. For each $\ell = L, \ldots, L + k - 1$ and each $j = 1, \ldots, g$, choose a linear fractional transformation $\eta_{j,\ell} \in PGL(2, \mathbb{Z}_p)$ so that $\eta_{j,\ell} \circ f_j^{\ell}(x_j) \in D(0, 1)$. Then $\eta_{j,\ell} \circ f_j^{\ell-\ell_{j,1}}(D(0, 1)) \subseteq D(0, 1)$, because f_j has good reduction. Finally, define $E_{j,\ell} = \eta_{j,\ell} \circ f_j^{\ell-\ell_{j,1}} \circ u_j$, so that $E_{j,\ell} \in \mathbb{Q}_p[[z]]$ maps $\overline{D}(0, s_j)$ into $D(0, 1)$.

Step (vi). In this step, we will write down power series $F_{j,\ell}$ for $f_j^{\ell+nk}$ in terms of n, p^n, and p^{m^n}. We will also produce bounds $B_{j,\ell}$ to be used in applying Lemma 3.1. For each $j = 1, \ldots, g$, we consider the three cases that $f_j^{\ell}(x_j)$ lies in a quasiperiodic, attracting (but not superattracting), or superattracting residue class for the function f_j^k.

In the quasiperiodic case, for each $\ell = L, \ldots, L + k - 1$, define the power series

$$F_{j,\ell}(z_0) = E_{j,\ell}(kz_0 + \mu_j) \in \mathbb{Q}_p[[z_0]],$$

so that $F_{j,\ell}(n) = \eta_{j,\ell} \circ f_j^{\ell+nk}(x_j)$ for all $n \geqslant 0$. All coefficients of $F_{j,\ell}$ have absolute value at most $1 = p^0$, because $|k|_p, |\mu_j|_p \leqslant s_j$ and $E_{j,\ell}$ maps $\overline{D}(0, s_j)$ into $D(0, 1)$. Hence, we set our bound $B_{j,\ell}$ to be $B_{j,\ell} := 0$.

Second, in the attracting (but not superattracting) case, for each $\ell = L, \ldots, L + k - 1$, define the power series

$$F_{j,\ell}(z_0, z_1) = E_{j,\ell}\big(z_1^{e_{j,3}} g_{j,2}(z_0)\mu_j\big) \in \mathbb{Q}_p[[z_0, z_1]],$$

where $E_{j,\ell}$ and $g_{j,2}$ are as in Step (v), so that $F_{j,\ell}(n, p^n) = \eta_{j,\ell} \circ f_j^{\ell+nk}(x_j)$ for all $n \geqslant 0$.

Still in the attracting (but not superattracting) case, because $E_{j,\ell}$ maps $\overline{D}(0, s_j)$ into $D(0, 1)$, there is some $B_{j,\ell} > 0$ such that for every $i \geqslant 0$, the coefficient of z^i in $E_{j,\ell}(z)$ has absolute value at most $p^{iB_{j,\ell}}$. Recalling also that $g_{j,2} \in \mathbb{Z}_p[[z]]$ and $|\mu_j|_p < 1$, it follows that if we write $F_{j,\ell}(z_0, z_1) = \sum_{i=0}^{\infty} h_i(z_0) z_1^i$ (where $h_i \in \mathbb{Q}_p[[z]]$), then for each $i \geqslant 0$, all coefficients of h_i have absolute value at most $p^{iB_{j,\ell}}$.

Third, in the superattracting case, for each $\ell = L, \ldots, L + k - 1$, define the power series

$$F_{j,\ell}(z_0, z_1, z_{m_{j,3}}) = E_{j,\ell}\big(g_{j,2}(z_0, z_1) z_{m_{j,3}}^{e_j}\big) \in \mathbb{Q}_p[[z_0, z_1, z_{m_{j,3}}]],$$

where $E_{j,\ell}$ and $g_{j,2}$ are as in Step (v), so that $F_{j,\ell}(n, p^n, p^{m_{j,3}^n}) = \eta_{j,\ell} \circ f_j^{\ell+nk}(x_j)$ for all $n \geqslant 0$.

Still in the superattracting case, because $E_{j,\ell}$ maps $\overline{D}(0, s_j)$ into $D(0, 1)$, there is some $B_{j,\ell} > 0$ such that for every $i \geqslant 0$, the coefficient of z^i in $E_{j,\ell}(z)$ has absolute value at most $p^{iB_{j,\ell}}$. Hence, if we write $F_{j,\ell}(z_0, z_1, z_{m_{j,3}}) = \sum_{i_1,i_2 \geqslant 0} h_{i_1,i_2}(z_0) z_1^{i_1} z_{m_{j,3}}^{i_2}$ (where $h_{i_1,i_2} \in \mathbb{Q}_p[[z]]$), then as before, since $g_{j,2} \in \mathbb{Z}_p[[z_0, z_1]]$, all coefficients of h_{i_1,i_2} have absolute value at most $p^{i_2 B_{j,\ell}} \leqslant p^{B_{j,\ell}(i_1+i_2)}$.

Finally, set $B := \max\{B_{j,\ell} : 1 \leqslant j \leqslant g \text{ and } L \leqslant \ell \leqslant L + k - 1\}$.

Step (vii). Let $m := \max\big\{1, \max_j\{m_{j,3}\}\big\}$, where the inner maximum is taken over all $j \in \{1, \ldots, g\}$ for which $f_j^{\ell_j}(x_j)$ is in a superattracting residue class for f_j^k. For each $\ell = L, \ldots, L+k-1$, let $\mathcal{V}_\ell \subseteq \mathbb{Z}_p[t_1, \ldots, t_g]$ be the finite set of polynomials $\mathcal{V}$ generating the vanishing ideal of V from

step (i), but now dehomogenized with respect to the coordinates determined by $(\eta_{1,\ell}, \ldots, \eta_{g,\ell})$. For each polynomial $H \in \mathcal{V}_\ell$, define

$$G_{H,\ell}(z_0, \ldots, z_m) = H(F_{1,\ell}, F_{2,\ell}, \ldots, F_{g,\ell}) \in \mathbb{Q}_p[[z_0, z_1, \ldots, z_m]].$$

Then by construction, $G_{H,\ell}(n, p^n, p^{2^n}, \ldots, p^{m^n})$ is defined for all integers $n \geqslant 0$, and is zero precisely at those n for which $\Phi^{\ell+nk}(P) \in V$.

For each nontrivial $G_{H,\ell}$, write

$$G_{H,\ell}(z_0, p^n, p^{2^n}, \ldots, p^{m^n}) = \sum_{w \in \mathbb{N}^m} g_w(z_0) p^{f_w(n)}$$

and select $v \in \mathbb{N}^m$ as in the statement of Lemma 3.1. By our choice of the bound B in Step (vi), and because all coefficients of H lie in $\mathbb{Z}_p$, all coefficients of g_w have absolute value at most $p^{B|w|}$, for every $w \in \mathbb{N}^m$. Since $G_{H,\ell}(n, p^n, p^{2^n}, \ldots, p^{m^n})$ is defined at every $n \geqslant 0$, g_v must converge on $\overline{D}(0,1)$; therefore, we may choose a radius $0 < s_{H,l} \leqslant 1$ for g_v as in Lemma 2.4.

Let s be the minimum of all the $s_{H,\ell}$ across all such pairs (H, ℓ). The set $\mathbb{Z}_p$ may be covered by the disks $D(0,s)$, $D(1,s)$, …, $D(p^M - 1, s)$, for some integer $M \geqslant 0$. Let $N := p^M k$.

Apply Lemma 3.1 (with the bound B from Step (vi) and radius s from the previous paragraph) to every nontrivial $G_{H,\ell}$, and let $C_0 > 1$ be the minimum of the resulting constants. Choose any $\epsilon > 0$, and let $C := C_0^{p^M - \epsilon} > 1$.

Step (viii). Unless conclusion (ii) of Theorem 1.4 holds for these values of C and N, there is some $\ell \in \{L, \ldots, L + N - 1\}$, and there are infinitely many pairs (n, n') of positive integers such that

(i) $\Phi^{\ell+nN}(P), \Phi^{\ell+n'N}(P) \in V$, and

(ii) $0 < n' - n \leqslant C^n$.

For any fixed $n \geqslant 1$, there are only finitely many choices of n' for which condition (ii) above holds; thus, there are pairs (n, n') with n arbitrarily large satisfying these two conditions.

Write $\ell = \ell_1 + \alpha k$ for integers $L \leqslant \ell_1 < L + k$ and $0 \leqslant \alpha < p^M$. For each pair (n, n') above, set $n_1 = np^M + \alpha$ and $n_1' = n'p^M + \alpha$. Then there are infinitely many pairs (n_1, n_1') such that

(1) $\Phi^{\ell_1+n_1k}(P), \Phi^{\ell_1+n_1'k}(P) \in V$,

(2) $n_1 \equiv n_1' \equiv \alpha \pmod{p^M}$, and

(3) $0 < (n_1' - n_1)/p^M \leqslant C^{(n_1-\alpha)/p^M}$.

Recalling that $C = C_0^{p^M - \epsilon} > 1$ and $\alpha \geqslant 0$, condition (3) becomes

(3') $0 < n_1' - n_1 \leqslant p^M C_0^{(n_1-\alpha)(1-\epsilon p^{-M})} \leqslant C_0^{n_1}$,

for n_1 sufficiently large (more precisely, for $n_1 \geqslant \frac{Mp^M \log p}{\epsilon \log C_0}$). However, conditions (1), (2) and (3') coupled with Lemma 3.1 yield that G_{H,ℓ_1} must be trivial for all $H \in \mathcal{V}_{\ell_1}$. Hence, $\Phi^{\ell_1+nk}(P) \in V$ for all $n \geqslant 0$. □

In the final step of the proof, we produced the constants N and C that appeared in the statement of Theorem 1.4. In fact, as the following result shows, for any integer $e \geqslant 1$, we can increase C to $C^{e-\epsilon}$, at the expense of increasing N to eN.

THEOREM 4.1. *If the proof of Theorem 1.4 yields constants $C > 1$ and $N \geqslant 1$ satisfying its conclusion, then for any integer $e > 1$ and for any $\epsilon > 0$, the conclusion of Theorem 1.4 holds when replacing the pair (C, N) by $(C^{e-\epsilon}, eN)$.*

Proof. In steps (v) and (vii) of the proof of Theorem 1.4, we had produced positive integers k, L, and M, and a real constant $C_0 > 1$. We then set $N = p^M k$ and $C = C_0^{p^M - \epsilon}$. Instead, we now set $N := ep^M k$ and $C := C_0^{ep^M - \epsilon}$, as promised in the statement of Theorem 4.1.

Step (viii) of the proof of Theorem 1.4 still applies even when we change all appearances of p^M to ep^M. More precisely, we have $0 \leqslant \alpha < ep^M$ when we write $\ell = \ell_1 + \alpha k$, and we write $n_1 = nep^M + \alpha$ and $n_1' = n'ep^M + \alpha$. The $\pmod{p^M}$ in condition (2) becomes $\pmod{ep^M}$, which of course still implies congruence modulo p^M. The change from p^M to ep^M ultimately leaves condition (3') as $0 < n_1' - n_1 \leqslant C_0^{n_1}$, though now only for $n_1 \geqslant \frac{ep^M \log(ep^M)}{\epsilon \log C_0}$). Thus, conditions (1), (2), and (3') remain the same as before, allowing exactly the same application of Lemma 3.1. The rest of the proof then goes through verbatim. □

5. Proof of Corollary 1.5

Proof. Assume that $\mathcal{S} = \{n \geqslant 0 : \Phi^n(P) \in V\}$ does not contain any infinite arithmetic progressions. Hence the second conclusion of Theorem 1.4 holds, and thus, taking T sufficiently large, we find that if $\ell \in \{T+1, T+2, \ldots, T+N\}$ and $\Phi^{\ell+mN}(P), \Phi^{\ell+nN}(P)$ *both* lie in V, for some $n > m \geqslant 0$, then $n - m > C^m$. Let $A = T + N + NC$, and for each $\ell \in \{T+1, \ldots, T+N\}$, let

$$\mathcal{S}_\ell := \{n > C : \ell + nN \in \mathcal{S}\}.$$

For all $i \geqslant 1$, let $n_{\ell,i}$ be the i^{th} smallest integer in $\mathcal{S}_\ell$, or $n_{\ell,i} = \infty$ if $|\mathcal{S}_\ell| < i$. Then $n_{\ell,1} > C = C \uparrow\uparrow 1$, and $n_{\ell,i+1} > n_{\ell,i} + C^{n_{\ell,i}} > C^{n_{\ell,i}} > C \uparrow\uparrow (i+1)$ for all $i \geqslant 1$. Hence, $L_C(n_{\ell,i}) \geqslant i$, and therefore $L_C(M) \geqslant i$ for all $M \geqslant n_{\ell,i}$. Summing across all ℓ, we have

$$|\{n \in \mathcal{S} : n \leqslant M\}| \leqslant |\{n \in \mathcal{S} : n \leqslant A\}| + \sum_{\ell=T+1}^{T+N} |\{n \in \mathcal{S}_\ell : n \leqslant M\}| \leqslant A + N \cdot L_C(M). \qquad \square$$

6. Curves

If V is a curve and everything is defined over a number field, we can, using a different method, obtain slightly more information about the relationship between C, N, and the prime p (albeit for a sparse sequence of primes.) Further, given a little more information about the applicable primes p, it may be possible to improve the following method to a proof of Conjecture 1.1 in this special case of curves over number fields.

Theorem 6.1. *Let P, Φ, and V be as in Theorem 1.4. Assume further that V is an irreducible* curve *that is not periodic, and that V, P, and Φ are all defined over a number field K. Then for any $\epsilon > 0$, there are infinitely many primes p and associated constants $C = C(p) > p - \epsilon$ and $N = N(p) = O(p^{2[K:\mathbb{Q}]})$ with the following property: For any integers $n > m \geqslant 0$ and $\ell \in \{1, 2, \ldots, N\}$, if m is sufficiently large and if both $\Phi^{\ell+mN}(P), \Phi^{\ell+nN}(P) \in V$, then $n - m > C^m$.*

The proof of Theorem 6.1 is simpler than the proof of Theorem 1.4, but it requires an additional ingredient that is only available over number fields, namely, the existence of a suitable indifferent cycle in at least one of the variables (which one obtains over number fields by [Sil93, Theorem 2.2] or [BGKT, Lemma 4.1]). Because of the counterexample presented in Proposition 7.1, it seems likely that a proof of Conjecture 1.1 would also have to involve extra information beyond what is used in the proof of Theorem 1.4. Thus, although Theorem 6.1 only applies to curves, it may well be that the techniques used to prove it are better adapted to a general proof of Conjecture 1.1.

To prove Theorem 6.1 we will need a sharper version of Lemma 2.2, giving an upper bound on k. We first recall the following special case of [BGT, Theorem 3.3].

THEOREM 6.2. *Let $p > 3$ be prime, let $K_p/\mathbb{Q}_p$ be a finite unramified extension, and let $\mathcal{O}_p$ denote the ring of integers in K_p. Let $g(z) = a_0 + a_1 z + a_2 z^2 + \cdots \in \mathcal{O}_p[[z]]$ be a power series with $|a_0|_p, |a_1 - 1|_p < 1$ and for each $i \geqslant 2$, $|a_i|_p \leqslant p^{1-i}$. Then for any $z_0 \in \mathcal{O}_p$, there is a power series $u \in \mathcal{O}_p[[z]]$ mapping $\overline{D}(0,1)$ into itself such that $u(0) = z_0$, and $u(z+1) = g(u(z))$.*

Remark 6.3. In [BGT], the theorem is only stated for $K_p = \mathbb{Q}_p$, but the proof goes through essentially unchanged for any finite unramified extension of $\mathbb{Q}_p$.

We can now give an explicit bound on k. However, we give up any claims on the size of the image of u. In fact, if z_0 is a periodic point, the map u is constant. (On the other hand, if z_0 is not periodic, then the derivative of u is nonvanishing at zero, and hence u is a local bijection.)

PROPOSITION 6.4. *Let $p > 3$ be prime, let K_p and $\mathcal{O}_p$ be as in Theorem 6.2, let $h(z) \in \mathcal{O}_p[[z]]$ be a power series, and let $z_0 \in \mathcal{O}_p$. Suppose that $|h(z_0) - z_0|_p < 1$ and $|h'(z_0)|_p = 1$. Then there is an integer $1 \leqslant k \leqslant p^{[K_p:\mathbb{Q}_p]}$ and a power series $u \in \mathcal{O}_p[[z]]$ mapping $\overline{D}(0,1)$ into $\overline{D}(0,1)$ such that $u(0) = z_0$ and $h^k(u(z)) = u(z+1)$. In particular,*

$$h^{nk}(z_0) = u(n) \qquad \text{for all } n \geqslant 0.$$

Proof. Let $q = p^{[K_p:\mathbb{Q}_p]}$ denote the cardinality of the residue field of $\mathcal{O}_p$. Conjugating by a translation we may assume that $z_0 = 0$. Let

$$g(z) := h(pz)/p = b_0 + b_1 z + b_2 z^2 + \cdots \in \mathcal{O}_p[[z]]$$

We find that $|b_0|_p \leqslant 1, |b_1|_p = 1$, and $|b_i|_p \leqslant p^{1-i}$ for each $i \geqslant 2$. By considering the iterates of the map $z \mapsto b_0 + b_1 z$, we have $g^k(z) \equiv z \pmod{p}$ for some $1 \leqslant k \leqslant q$. Hence, $g^k(z) = a_0 + a_1 z + a_2 z^2 + \cdots$ satisfies the hypotheses of Theorem 6.2, giving a power series $\tilde{u} \in \mathcal{O}_p[[z]]$ mapping $\overline{D}(0,1)$ into itself, with $\tilde{u}(0) = 0$ and $\tilde{u}(z+1) = g^k(\tilde{u}(z))$. It follows that $u(z) = p\tilde{u}(z)$ has the desired properties. □

Now we are ready to prove Theorem 6.1.

Proof of Theorem 6.1. For simplicity we assume that $X = \mathbb{P}^1 \times \mathbb{P}^1$, and that $V \subset X$ is an irreducible curve; the argument is easily modified to include the general case. If x_i is preperiodic under f_i for either $i = 1$ or $i = 2$, the result is trivial. If both f_1 and f_2 are of degree one, V can be shown to be be periodic, either by the Skolem-Mahler-Lech theorem, by [BGKT, Theorem 3.4], or by [BGT, Theorem 1.3]. Thus, possibly after permuting indices, we may assume that the degree of f_1 is greater than 1. Define $\pi_1 : V \to \mathbb{P}^1(K)$ by $(z_1, z_2) \to z_1$. By taking a periodic cycle $D = \{d_1, \ldots, d_a\}$ of f_1 of sufficiently large cardinality a, defined over some number field L, we may assume that D is not superattracting (i.e., no d_i is a critical point of f_1), that all points $(\alpha_1, \alpha_2) \in \pi_1^{-1}(D) \cap V$ are smooth points on V, and finally, that for (z_1, z_2) near (α_1, α_2),

$$z_1 - \alpha_1 = \gamma_\alpha \cdot (z_2 - \alpha_2) + O\left((z_2 - \alpha_2)^2\right), \tag{6.1}$$

for some $\gamma_\alpha \neq 0$. (Note that only finitely many points violate these conditions.) Since f_1 is not preperiodic, by [Sil93, Theorem 2.2] (or [BGKT, Lemma 4.1]), we can find infinitely many primes p such that $|f_1^n(x_1) - d_1|_p < 1$ for some n, where $|\cdot|_p$ denotes some extension of the p-adic absolute value on $\mathbb{Q}$ to L. We may of course assume that $L/\mathbb{Q}$ is unramified at p and that $|\gamma_\alpha|_p = |(f_1^a)'(d_1)|_p = 1$ for all sufficiently large p, as there are only finitely many p not fitting these conditions. In particular, the orbit of x_1 under f_1 ends up in a domain of quasiperiodicity.

If the orbit of x_2 under f_2 also has quasiperiodic behavior, then V is periodic by [BGKT, Theorem 3.4]. Otherwise, the orbit of x_2 ends up in an attracting or superattracting domain. The arguments in these two cases are very similar, and we shall only give details for the attracting case. Hence, assume that $f_2^n(x_2)$ tends to an attracting cycle $E = \{e_1, e_2, \ldots, e_b\}$, with multiplier λ_2 satisfying $0 < |\lambda_2|_p < 1$. Since λ_2 and E are defined over K_p, and $K_p/\mathbb{Q}_p$ is unramified, we have

$|\lambda|_p \leqslant 1/p$. Note that $b \leqslant p^{[K_p:\mathbb{Q}_p]} + 1 \leqslant p^{[K:\mathbb{Q}]} + 1$. Let $N = \operatorname{lcm}(a, b)$, so that $N \leqslant a \cdot (p^{[K:\mathbb{Q}]} + 1) = O(p^{[K:\mathbb{Q}]})$. Choose representatives $\{\alpha_{ij} : 1 \leqslant i \leqslant a,\ 1 \leqslant j \leqslant b\}$ for $\mathbb{Z}/N\mathbb{Z}$ such that

$$|f_1^{\alpha_{ij}+Nn}(x_1) - d_i|_p < 1, \quad |f_2^{\alpha_{ij}+Nn}(x_2) - e_j|_p < 1$$

for n sufficiently large. At the cost of increasing N by a factor bounded by $p^{[K:\mathbb{Q}]}$, by Proposition 6.4 and Lemma 2.1 there exist p-adic power series A_i, B_j, such that

$$f_1^{\alpha_{ij}+Nn}(x_1) - d_i = A_i(n), \quad f_2^{\alpha_{ij}+Nn}(x_2) - e_j = B_j(\lambda_2^n) \tag{6.2}$$

for n sufficiently large. If $n > m$ and $\phi^{mN+\alpha_{ij}}(P), \phi^{nN+\alpha_{ij}}(P) \in V$, then (6.1) and (6.2) yield that

$$|A_i(n) - A_i(m)|_p = O(|\lambda_2|_p^m),$$

since we had $|\gamma_\alpha|_p = 1$ in (6.1). Hence $n \equiv m \pmod{p^{m-O_p(1)}}$, where the $O_p(1)$ depends on the derivative of A_i. Thus, if we take $C < p$, we find that $n \geqslant m + C^m$ for m sufficiently large. □

7. An analytic counterexample

It is natural to ask if an even more rapid growth condition than the one in Theorem 1.4 should hold when V is not periodic. However, as the following shows, Lemma 3.1 is essentially sharp.

Proposition 7.1. *For any prime $p \geqslant 2$ and for any positive integer n_1, there is an increasing sequence $\{n_j\}_{j\geqslant 2}$ of positive integers and a power series $f(z) \in \mathbb{Z}_p[[z]]$ such that*

$$f(p^{n_j}) = n_j \quad \text{and} \quad n_j + p^{n_j} \leqslant n_{j+1} \leqslant n_j + p^{n_1+\cdots+n_j}$$

for all $j \geqslant 1$. Moreover, $n_1 + \cdots + n_{j-1} \leqslant n_j$, and hence $n_{j+1} \leqslant n_j + p^{2n_j}$.

Remark 7.2. Setting $G(z_0, z_1) = z_1 - f(z_0)$, we find that Lemma 3.1 cannot be substantially improved; specifically, the constant C is at most p^2 for this example. Furthermore, the bound of p^2 can be improved to something much closer to p because, by a simple inductive argument, one can show that for every $j \geqslant 1$, we have

$$n_1 + \cdots + n_j \leqslant \frac{n_{j+1}}{n_1},$$

from which $n_{j+1} \leqslant n_j + p^{n_j \cdot \left(1+\frac{1}{n_1}\right)}$ follows. Letting n_1 be arbitrarily large we obtain that for every $\epsilon > 0$ there exists an increasing sequence $\{n_j\}_{j\geqslant 1}$ satisfying the hypothesis of Proposition 7.1, and for which

$$n_j + p^{n_j} \leqslant n_{j+1} \leqslant n_j + p^{(1+\epsilon)\cdot n_j}.$$

Proof of Proposition 7.1. We will inductively construct the sequence $\{n_j : j \geqslant 2\}$ of positive integers and a sequence $\{f_j(z) : j \geqslant 1\}$ of polynomials $f_j \in \mathbb{Z}_p[z]$, with $\deg(f_j) = j - 1$. The power series f will be $f = \lim_{j\to\infty} f_j$.

Let f_1 be the constant polynomial n_1. Then, for each $j \geqslant 1$, suppose we are already given $f_1, \ldots, f_j$ and $n_1, \ldots, n_j$ such that $f_k(p^{n_i}) = n_i$ for each i, k with $1 \leqslant i \leqslant k \leqslant j$. Choose n_{j+1} to be the unique integer such that

$$n_j + 1 \leqslant n_{j+1} \leqslant n_j + p^{n_1+\cdots+n_j}$$

and

$$|n_{j+1} - f_j(0)|_p \leqslant |p|_p^{n_1+\cdots+n_j}. \tag{7.1}$$

Note that because $f_j \in \mathbb{Z}_p[z]$ and $f_j(p^{n_j}) = n_j$, we have

$$|f_j(0) - n_j|_p = |f_j(0) - f_j(p^{n_j})|_p \leqslant |p|_p^{n_j},$$

and therefore $|n_{j+1}-n_j|_p \leqslant |p|_p^{n_j}$, implying that $n_{j+1} \geqslant n_j + p^{n_j}$ and that $n_{j+1} \geqslant n_1+n_2+\cdots+n_j$, as claimed in the Proposition.

Define $g_j(z) := (z-p^{n_1})(z-p^{n_2})\cdots(z-p^{n_j})$, and set

$$c_j := \frac{n_{j+1} - f_j(p^{n_{j+1}})}{g_j(p^{n_{j+1}})} \in \mathbb{Q}_p,$$

and

$$f_{j+1}(z) := f_j(z) + c_j g_j(z) \in \mathbb{Q}_p[z].$$

We claim that $|c_j|_p \leqslant 1$. Indeed, we have

$$|f_j(0) - f_j(p^{n_{j+1}})|_p \leqslant |p|_p^{n_{j+1}}, \tag{7.2}$$

because $f_j \in \mathbb{Z}_p[[z]]$. Therefore,

$$\begin{aligned} |n_{j+1} - f_j(p^{n_{j+1}})|_p &\leqslant \max\{|n_{j+1} - f_j(0)|_p, |f_j(0) - f_j(p^{n_{j+1}})|_p\} \\ &\leqslant \max\{|p|_p^{n_1+\cdots+n_j}, |p|_p^{n_{j+1}}\} \\ &= |p|_p^{n_1+\cdots+n_j} = |g_j(p^{n_{j+1}})|_p, \end{aligned}$$

where the second inequality is by (7.1) and (7.2). It follows immediately that $|c_j|_p \leqslant 1$, as claimed.

Clearly, $f_{j+1}(p^{n_i}) = n_i$ for all $i = 1, \ldots, j+1$. Because $c_j \in \mathbb{Z}_p$, we obtain that $f_{j+1} \in \mathbb{Z}_p[z]$, completing the induction. In fact, because (for any fixed $m \geqslant 0$) the size of the z^m-coefficient of g_j goes to zero as $j \to \infty$, it follows that $\lim_{j\to\infty} f_j$ converges coefficient-wise to some power series $f \in \mathbb{Z}_p[[z]]$. Because every f_j also lies in $\mathbb{Z}_p[[z]]$, it follows that the convergence $f_j \to f$ is uniform on $p\mathbb{Z}_p$. Hence, $f(p^{n_i}) = n_i$ for all $i \geqslant 1$, as desired. □

References

Abr94 D. Abramovich, *Subvarieties of semiabelian varieties*, Compositio Math. **90** (1994), no. 1, 37–52.

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

BGKT R. L. Benedetto, D. Ghioca, P. Kurlberg, and T. J. Tucker, *The dynamical Mordell-Lang conjecture* (with an Appendix by Umberto Zannier), submitted for publication, available online at `http://arxiv.org/abs/0712.2344`.

BGT J. P. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell-Lang problem for étale maps*, to appear in Amer. J. Math., available online at `http://arxiv.org/abs/0808.3266`.

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

DR55 H. Davenport and K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 160–167.

Fal83 G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

Fal94 ———, *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.

GTZ D. Ghioca, T. J. Tucker, and M. Zieve, *Linear relations between polynomial orbits*, submitted for publication, available at `http://arxiv.org/abs/0807.3576`, 27 pages.

GTZ08 ———, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math. **171** (2008), no. 2, 463–483.

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

Mum65 D. Mumford, *A remark on Mordell's conjecture*, Amer. J. Math. **87** (1965), 1007–1016.

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.

Sil93 J. H. Silverman, *Integer points, Diophantine approximation, and iteration of rational maps*, Duke Math. J. **71** (1993), no. 3, 793–829.

Sil07 ———, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007. MR MR2316407 (2008c:11002)

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

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.

Robert L. Benedetto rlb@math.amherst.edu
Department of Mathematics, Amherst College, Amherst, MA 01002, USA

Dragos Ghioca dragos.ghioca@uleth.ca
Department of Mathematics & Computer Science, University of Lethbridge, 4401 University Drive, Lethbridge, AB T1K 3M4, Canada

Pär Kurlberg kurlberg@math.kth.se
Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden

Thomas J. Tucker ttucker@math.rochester.edu
Department of Mathematics, Hylan Building, University of Rochester, Rochester, NY 14627, USA