Math. Ann. (2013) 355:637–660
DOI 10.1007/s00208-012-0799-8

Mathematische Annalen

Periods of rational maps modulo primes

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

Received: 26 July 2011 / Revised: 1 February 2012 / Published online: 8 March 2012

Abstract Let K be a number field, let $\varphi \in K(t)$ be a rational map of degree at least 2, and let $\alpha, \beta \in K$. We show that if α is not in the forward orbit of β, then there is a positive proportion of primes $\mathfrak{p}$ of K such that $\alpha \bmod \mathfrak{p}$ is not in the forward orbit of $\beta \bmod \mathfrak{p}$. Moreover, we show that a similar result holds for several maps and several points. We also present heuristic and numerical evidence that a higher dimensional analog of this result is unlikely to be true if we replace α by a hypersurface, such as the ramification locus of a morphism $\varphi : \mathbb{P}^n \to \mathbb{P}^n$.

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

B. Hutz
Ph.D. Program in Mathematics, Graduate Center of CUNY,
365 Fifth Avenue, New York, NY 10016-4309, USA
e-mail: bhutz@gc.cuny.edu

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

T. Scanlon
Mathematics Department, University of California Berkeley,
Evans Hall, Berkeley, CA 94720-3840, USA
e-mail: scanlon@math.berkeley.edu

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

1 Introduction

Let K be a number field, and let $\varphi : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ be a rational map of degree at least 2. For any integer $m \geq 0$, write $\varphi^m = \varphi \circ \varphi \circ \cdots \circ \varphi$ for the mth iterate of φ under composition. The *forward orbit* of a point $\alpha \in \mathbb{P}^1(K)$ under φ is the set $\{\varphi^m(\alpha) : m \geq 0\}$. Similarly, the *backward orbit* of α is the set $\{\beta \in \mathbb{P}^1(\overline{K}) : \varphi^m(\beta) = \alpha \text{ for some } m \geq 0\}$. We say α is *φ-periodic* if $\varphi^m(\alpha) = \alpha$ for some $m \geq 1$; the smallest such m is called the (*exact*) *period* of α. More generally, we say α is *φ-preperiodic* if its forward orbit is finite; if the backward orbit of α is finite, we say α is *exceptional* for φ.

Given two points $\alpha, \beta \in \mathbb{P}^1(K)$ such that β is not φ-preperiodic and α is not in the forward orbit of β under φ, one might ask how many primes $\mathfrak{p}$ of K there are such that α *is* in the forward orbit of β under φ modulo $\mathfrak{p}$. It follows from [4, Lemma 4.1] that there are infinitely many such $\mathfrak{p}$ unless α is exceptional for φ. The same techniques (essentially, an application of [19, Theorem 2.2]) can be used to show that there are infinitely many $\mathfrak{p}$ such that α is *not* in the forward orbit of β modulo $\mathfrak{p}$.

Odoni [15], Jones [13], and others have shown that the set $\mathcal{S}$ of primes $\mathfrak{p}$ such that α is in the forward orbit of β modulo $\mathfrak{p}$ has density zero in some cases. However, there are cases when $\mathcal{S}$ has positive density. For example, if $K = \mathbb{Q}$ and $\varphi(x) = x^3 + 1$, then $\alpha = 0$ is in the forward orbit of $\beta = 1$ modulo any prime congruent to 2 mod 3. More generally, one may expect such examples for *exceptional maps*; for more details, see [9].

The following is a simplified version of the main result of this paper.

Theorem 1 *Let K be a number field, and let $\varphi_1, \ldots, \varphi_g : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ be rational maps of degree at least 2. Let $\mathcal{A}_1, \ldots, \mathcal{A}_g$ be finite subsets of $\mathbb{P}^1(K)$ such that for each $i = 1, \ldots, g$, every point in $\mathcal{A}_i$ is φ_i-preperiodic. Let $\mathcal{T}_1, \ldots, \mathcal{T}_g$ be finite subsets of $\mathbb{P}^1(K)$ such that no $\mathcal{T}_i$ contains any φ_i-preperiodic points. Then there is a positive integer M and a set of primes $\mathcal{P}$ of K having positive density such that for any $i = 1, \ldots, g$, any $\gamma \in \mathcal{T}_i$, any $\alpha \in \mathcal{A}_i$, any $\mathfrak{p} \in \mathcal{P}$, and any $m \geq M$,*

$$\varphi_i^m(\gamma) \not\equiv \alpha \pmod{\mathfrak{p}}.$$

Theorem 1 is a special case of our main result, Theorem 5, which features a weaker hypothesis: one of the sets $\mathcal{A}_i$ is allowed to contain a single non-preperiodic point. We will prove Theorem 5, and hence also Theorem 1, in Sect. 3. The technique is to find a prime $\mathfrak{p}$ at which, for each $i = 1, \ldots, g$, the expression $\varphi_i^M(x) - \alpha$ does not have a root modulo $\mathfrak{p}$ for any $\alpha \in \mathcal{A}_i$. One then applies the Chebotarev density theorem to obtain a positive density set of primes with the desired property.

Theorem 5 has a number of applications to arithmetic dynamics and to elliptic curves. We present two such corollaries here. The first involves the notion of good reduction of a rational function; see Definition 1.

Corollary 2 *Let K be a number field, let $\varphi : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ be a rational function of degree at least 2, and let $\alpha \in \mathbb{P}^1(K)$ be a non-periodic point of φ. Then there is a positive density set of primes $\mathfrak{p}$ of K at which φ has good reduction $\varphi_\mathfrak{p}$ and such that the reduction of α modulo $\mathfrak{p}$ is not $\varphi_\mathfrak{p}$-periodic.*

To state our second corollary, we fix some notation. If $\mathfrak{p}$ is a prime of a number field K, E is an elliptic curve defined over K of good reduction at $\mathfrak{p}$, and $Q \in E(K)$ is a K-rational point on E, then $k_\mathfrak{p} = \mathfrak{o}_K/\mathfrak{p}$ is the residue field at $\mathfrak{p}$, $E_\mathfrak{p}$ is the reduction of E modulo $\mathfrak{p}$, and $Q_\mathfrak{p} \in E_\mathfrak{p}(k_\mathfrak{p})$ is the reduction of Q modulo $\mathfrak{p}$.

Corollary 3 *Let K be a number field, let E be an elliptic curve defined over K, let $Q \in E(K)$ be a non-torsion point, let q be a prime number, and let n be a positive integer. Then there is a positive density set of primes $\mathfrak{p}$ of K at which E has good reduction and such that the order of $Q_\mathfrak{p}$ in the finite group $E_\mathfrak{p}(k_\mathfrak{p})$ is divisible by q^n.*

Corollary 3 is in fact a weak version of a theorem of Pink, who showed the following result in [16, Corollary 4.3]: given an abelian variety A over a number field K, a point $Q \in A(K)$ such that $\mathbb{Z} \cdot Q$ is Zariski dense in A, and any prime power q^n, there is a positive density set of primes $\mathfrak{p}$ of K such that the q-primary part of the order of $Q_\mathfrak{p} \in A_\mathfrak{p}(k_\mathfrak{p})$ equals q^n.

This project originated in the summer of 2009, when four of the authors (R.B., D.G., P.K., and T.T.) were working to extend their results from [4] to other cases of the dynamical Mordell–Lang conjecture. At that time, T.S. suggested the general strategy for such an extension. The details for the proposed strategy turned out to be more complicated than originally thought, and thus later, with the help of B.H., particularly with respect to the computations in Sect. 5, the project was finalized.

The outline of the paper is as follows. After some background in Sect. 2, we state and prove Theorem 5 in Sect. 3. In Sect. 4, we prove the two above corollaries, and we present other applications of Theorem 5 to some recent problems in arithmetic dynamics. In Sect. 5 we present evidence that a result like Theorem 5 is unlikely to hold in higher dimensions. We conclude by posing some related questions in Sect. 6.

2 Notation and terminology

Let K be a number field with algebraic closure $\overline{K}$ and ring $\mathfrak{o}_K$ of algebraic integers. Fix an isomorphism π from $\mathbb{P}^1_K$ to the generic fibre of $\mathbb{P}^1_{\mathfrak{o}_K}$. By standard abuse of language, we call a nonzero prime $\mathfrak{p}$ of $\mathfrak{o}_K$ simply a *prime of* K, and we denote the corresponding residue field $k_\mathfrak{p} := \mathfrak{o}_K/\mathfrak{p}$. For each prime $\mathfrak{p}$ of K, and for each $x \in \mathbb{P}^1(K)$, we denote by $r_\mathfrak{p}(x)$ the intersection of the Zariski closure of $\pi(x)$ with the fibre above $\mathfrak{p}$ of $\mathbb{P}^1_{\mathfrak{o}_K}$; intuitively, $r_\mathfrak{p}(x)$ is x modulo $\mathfrak{p}$. The resulting map $r_\mathfrak{p} : \mathbb{P}^1(K) \longrightarrow \mathbb{P}^1(k_\mathfrak{p})$ is the *reduction map* at $\mathfrak{p}$. Again by standard abuse of language, we say that $\alpha \in \mathbb{P}^1(K)$ is *congruent* to $\beta \in \mathbb{P}^1(K)$ modulo $\mathfrak{p}$, and we write $\alpha \equiv \beta \pmod{\mathfrak{p}}$, if $r_\mathfrak{p}(\alpha) = r_\mathfrak{p}(\beta)$.

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 $\varphi([X, Y]) = [F(X, Y) : G(X, Y)]$; note that F and G are uniquely defined up to a nonzero constant multiple. (In affine coordinates, $\varphi(t) = F(t, 1)/G(t, 1) \in K(t)$ is a rational function in one variable.) We can then define the following notion of good reduction of φ, first introduced by Morton and Silverman [14].

Definition 1 Let K be a number field, let $\mathfrak{p}$ be a prime of K, and let $\mathfrak{o}_\mathfrak{p} \subseteq K$ be the corresponding local ring of integers. 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 $F, G \in \mathfrak{o}_\mathfrak{p}[X, Y]$ are relatively prime homogeneous polynomials of the same degree such that at least one coefficient of F or G is a unit in $\mathfrak{o}_\mathfrak{p}$. Let $\varphi_\mathfrak{p} := [F_\mathfrak{p}, G_\mathfrak{p}]$, where $F_\mathfrak{p}, G_\mathfrak{p} \in k_\mathfrak{p}[X, Y]$ are the reductions of F and G modulo $\mathfrak{p}$. We say that φ has *good reduction* at $\mathfrak{p}$ if $\varphi_\mathfrak{p} : \mathbb{P}^1(k_\mathfrak{p}) \longrightarrow \mathbb{P}^1(k_\mathfrak{p})$ is a morphism of the same degree as φ.

Intuitively, the map $\varphi_\mathfrak{p} : \mathbb{P}^1(k_\mathfrak{p}) \to \mathbb{P}^1(k_\mathfrak{p})$ in Definition 1 is the reduction of φ modulo $\mathfrak{p}$. If $\varphi \in K[t]$ is a polynomial, there is an elementary criterion for good reduction: φ has good reduction at $\mathfrak{p}$ if and only if all coefficients of φ are $\mathfrak{p}$-adic integers, and its leading coefficient is a $\mathfrak{p}$-adic unit.

We will use the following definition in Sect. 4.

Definition 2 Let K be a field, let $\varphi \in K(t)$ be a rational function, and let $z \in \mathbb{P}^1(\overline{K})$ be φ-periodic of period $n \geq 1$. Then $\lambda := (\varphi^n)'(z)$ is called the *multiplier* of z. If $\mathfrak{p}$ is a prime of K with associated absolute value $|\cdot|_\mathfrak{p}$, and if $|\lambda|_\mathfrak{p} < 1$, then z is said to be *attracting* with respect to the prime $\mathfrak{p}$.

In Sects. 5 and 6 we will consider morphisms of higher-dimensional spaces. Therefore we note that the multiplier λ in Definition 2 is the unique number λ such that the induced map $d(\varphi^n) : T_z\mathbb{P}^1 \longrightarrow T_z\mathbb{P}^1$ on the tangent space at z is multiplication by the 1×1 matrix $[\lambda]$.

Multipliers are invariant under coordinate change. More precisely, if z is a φ-periodic point and $\varphi = \mu^{-1} \circ \psi \circ \mu$, then $\mu(z)$ is a ψ-periodic point, and by the chain rule, it has the same multiplier as z does. 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 $\varphi^\mu(z)$ is the same as that of 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.

We conclude this section by recalling the statement of the Chebotarev Density Theorem; for more details, see, for example [21].

Theorem 4 *Let L/K be a Galois extension of number fields, and let $G := \mathrm{Gal}(L/K)$. Let $C \subset G$ be closed under conjugation, and define*

$$\Pi_C(x, L/K) := \#\{\mathfrak{p} : N(\mathfrak{p}) \leq x,\ \mathfrak{p} \text{ is unramified in } L/K, \text{ and } \sigma_\mathfrak{p} \subseteq C\},$$

where $N(\mathfrak{p})$ is the $(K/\mathbb{Q})$-norm of the prime ideal $\mathfrak{p}$ of K, and $\sigma_\mathfrak{p}$ is the Frobenius conjugacy class corresponding to $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$. Then

$$\lim_{x\to\infty} \frac{\Pi_C(x, L/K)}{\Pi_G(x, L/K)} = \frac{|C|}{|G|}.$$

3 Proof of main result

We now state and prove our promised generalization of Theorem 1.

Theorem 5 *Let K be a number field, and let $\varphi_1, \ldots, \varphi_g : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ be rational maps of degree at least 2. Let $\mathcal{A}_1, \ldots, \mathcal{A}_g$ be finite subsets of $\mathbb{P}^1(K)$ such that at most one set $\mathcal{A}_i$ contains a point that is not φ_i-preperiodic, and such that there is at most one such point in that set $\mathcal{A}_i$. Let $\mathcal{T}_1, \ldots, \mathcal{T}_g$ be finite subsets of $\mathbb{P}^1(K)$ such that no $\mathcal{T}_i$ contains any φ_i-preperiodic points. Then there is a positive integer M and a set of primes $\mathcal{P}$ of K having positive density such that for any $i = 1, \ldots, g$, any $\gamma \in \mathcal{T}_i$, any $\alpha \in \mathcal{A}_i$, any $\mathfrak{p} \in \mathcal{P}$, and any $m \geq M$,*

$$\varphi_i^m(\gamma) \not\equiv \alpha \pmod{\mathfrak{p}}.$$

We will need the following standard ramification lemma over $\mathfrak{p}$-adic fields; it says, roughly, that if the field of definition of a point in $\varphi^{-m}(\alpha)$ ramifies at $\tilde{\mathfrak{p}}$, then that point must be a ramification point of φ^m modulo $\tilde{\mathfrak{p}}$.

Lemma 1 *Let K be a number field, let $\tilde{\mathfrak{p}}$ be a prime of $\mathfrak{o}_{\overline{K}}$, and let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a rational function defined over K and of good reduction at $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_K$ such that $2 \leq \deg \varphi < \operatorname{char} k_{\mathfrak{p}}$. Let $\alpha \in \mathbb{P}^1(K)$, let $m \geq 1$ be an integer, let $\beta \in \varphi^{-m}(\alpha) \subseteq \mathbb{P}^1(\overline{K})$, and let $\mathfrak{q} := \tilde{\mathfrak{p}} \cap \mathfrak{o}_{K(\beta)}$. If $\mathfrak{q}$ is ramified over $\mathfrak{p}$, then β is congruent modulo $\tilde{\mathfrak{p}}$ to a ramification point of φ^m.*

Proof By induction, it suffices to show the lemma in the case $m = 1$. Let $|\cdot|_{\tilde{\mathfrak{p}}}$ denote the $\tilde{\mathfrak{p}}$-adic absolute value on $\overline{K}$, and let $K_{\mathfrak{p}}$ be the completion of K with respect to $|\cdot|_{\tilde{\mathfrak{p}}}$. After a change of coordinates, we may assume that $\alpha = 0$ and that $|\beta|_{\tilde{\mathfrak{p}}} \leq 1$.

Writing $\varphi = f/g$, where $f, g \in K[t]$ are relatively prime polynomials, we have $f(\beta) = 0$. Since $\mathfrak{q}$ is ramified over $\mathfrak{p}$, f must have at least one other root congruent to β modulo $\tilde{\mathfrak{p}}$. Thus, the reduction $f_{\mathfrak{p}}$ of f has a multiple root at β. However, $g_{\mathfrak{p}}(\beta) \neq 0$, since φ has good reduction. Therefore, the reduction $\varphi_{\mathfrak{p}}$ has a multiple root at β, and hence $\varphi'_{\mathfrak{p}}(\beta) = 0$. On the other hand, because $\deg \varphi < \operatorname{char} k_{\mathfrak{p}}$, there must be some $\gamma \in \mathfrak{o}_{\overline{K}}$ such that $\varphi'_{\mathfrak{p}}(\gamma) \neq 0$. It follows that there is a root of φ' congruent to β modulo $\tilde{\mathfrak{p}}$.

Next, we use the fact that our residue fields are finite to show that if α is not periodic modulo a large enough prime $\mathfrak{p}$, then for large m, there can be no roots of $\varphi^m(x) - \alpha$ modulo $\mathfrak{p}$. We also obtain some extra information about our fields of definition, which we will need in order to apply the Chebotarev density theorem in our proof of Theorem 5.

Lemma 2 *Let K be a number field, let $\tilde{\mathfrak{p}}$ be a prime of $\mathfrak{o}_{\overline{K}}$, and let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a rational function defined over K and of good reduction at $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_K$ such that $2 \leq \deg \varphi < \operatorname{char} k_{\mathfrak{p}}$. Suppose that $\alpha \in \mathbb{P}^1(K)$ is not periodic modulo $\mathfrak{p}$. Then there exists a finite extension E of K with the following property: for any finite extension L of E, there is an integer $M \in \mathbb{N}$ such that for all $m \geq M$ and all $\beta \in \mathbb{P}^1(\overline{K})$ with $\varphi^m(\beta) = \alpha$,*

(i) $\mathfrak{r}$ *does not ramify over* $\mathfrak{q}$, *and*
(ii) $[\mathfrak{o}_{L(\beta)}/\mathfrak{r} : \mathfrak{o}_L/\mathfrak{q}] > 1$,

where $\mathfrak{r} := \tilde{\mathfrak{p}} \cap \mathfrak{o}_{L(\beta)}$, and $\mathfrak{q} := \tilde{\mathfrak{p}} \cap \mathfrak{o}_L$.

Proof For any $\gamma \in \mathfrak{o}_{\overline{K}}$,

$$\text{there is at most one } j \geq 0 \text{ such that } \varphi^j(\gamma) \equiv \alpha \pmod{\tilde{\mathfrak{p}}}, \tag{1}$$

since α is not periodic modulo $\mathfrak{p}$. In particular, for each ramification point $\gamma \in \mathbb{P}^1(\overline{K})$ of φ, there are only finitely many integers $n \geq 0$ and points $z \in \mathbb{P}^1(\overline{K})$ such that $\varphi^n(z) = \alpha$ and $z \equiv \gamma \pmod{\tilde{\mathfrak{p}}}$. Let E be the finite extension of K formed by adjoining all such points z.

Given any finite extension L of E, let $\mathfrak{q} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_L$. Since $\mathbb{P}^1(\mathfrak{o}_L/\mathfrak{q})$ is finite, (1) implies that for all sufficiently large M, the equation $\varphi^M(x) = \alpha$ has no solutions in $\mathbb{P}^1(\mathfrak{o}_L/\mathfrak{q})$. Fix any such M; note that M must be larger than any of the integers n in the previous paragraph. Hence, given $m \geq M$ and $\beta \in \mathbb{P}^1(\overline{K})$ such that $\varphi^m(\beta) = \alpha$, we must have $[\mathfrak{o}_{L(\beta)}/\mathfrak{r} : \mathfrak{o}_L/\mathfrak{q}] > 1$, where $\mathfrak{r} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_{L(\beta)}$, proving conclusion (ii). Furthermore, if β is a root of $\varphi^m(x) - \alpha$, then there are two possibilities: either (1) β is not congruent modulo $\tilde{\mathfrak{p}}$ to a ramification point of φ^m, or (2) $\varphi^j(\beta) = z$ for some $j \geq 0$ and some point $z \in \mathbb{P}^1(L)$ from the previous paragraph. In case (1), $\mathfrak{r}$ is unramified over $\mathfrak{q}$ by Lemma 1. In case (2), choosing a minimal such $j \geq 0$, and applying Lemma 1 with z in the role of α and j in the role of m, $\mathfrak{r}$ is again unramified over $\mathfrak{q}$. Thus, in either case, conclusion (i) holds.

We now apply Lemma 2 to a set $\mathcal{A}$ of points.

Proposition 1 *Let K be a number field, let $\tilde{\mathfrak{p}}$ be a prime of $\mathfrak{o}_{\overline{K}}$, and let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a rational function defined over K and of good reduction at $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_K$ such that $2 \leq \deg \varphi < \operatorname{char} k_{\mathfrak{p}}$. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ be a finite subset of $\mathbb{P}^1(K)$ such that for each $\alpha_i \in \mathcal{A}$,*

- *if α_i is not periodic, then α_i is not periodic modulo $\mathfrak{p}$; and*
- *if α_i is periodic, then $\varphi(\alpha_i) = \alpha_i$ (i.e., α_i is fixed by φ) and the ramification index of φ at α_i is the same modulo $\mathfrak{p}$ as over K.*

Then there is a finite extension E of K with the following property: for any finite extension L of E, there is an integer $M \in \mathbb{N}$ such that for all $m \geq M$ and all $\beta \in \mathbb{P}^1(\overline{K})$ with $\varphi^m(\beta) \in \mathcal{A}$ but $\varphi^t(\beta) \notin \mathcal{A}$ for all $t < m$,

(i) *$\mathfrak{r}$ does not ramify over $\mathfrak{q}$, and*
(ii) *$[\mathfrak{o}_{L(\beta)}/\mathfrak{r} : \mathfrak{o}_L/\mathfrak{q}] > 1$,*

where $\mathfrak{r} := \tilde{\mathfrak{p}} \cap \mathfrak{o}_{L(\beta)}$ and $\mathfrak{q} := \tilde{\mathfrak{p}} \cap \mathfrak{o}_L$.

Proof For each $\alpha_i \in \mathcal{A}$ that is not periodic, we apply Lemma 2 and obtain a field E_i with the property described in that Lemma. For each $\alpha_j \in \mathcal{A}$ that is periodic, we apply Lemma 2 to each point $\gamma_{jk} \in \varphi^{-1}(\alpha_j) \setminus \{\alpha_j\}$ and obtain a field E_{jk} with the corresponding property. To do so, of course, we must know that no γ_{jk} is periodic modulo $\tilde{\mathfrak{p}}$. To see that this is true, first note that $\gamma_{jk} \not\equiv \alpha_j \pmod{\tilde{\mathfrak{p}}}$; otherwise the ramification index of φ at α_j would be greater modulo $\mathfrak{p}$ than over K, contradicting our hypotheses. Since α_j is fixed and $\gamma_{jk} \not\equiv \alpha_j \pmod{\tilde{\mathfrak{p}}}$, it follows that γ_{jk} is not periodic modulo $\tilde{\mathfrak{p}}$, as desired.

Let E be the compositum of all the fields E_i and E_{jk}. Given any finite extension L of E, then by our choice of E_i and E_{jk}, there are integers M_i, $M_{jk} \in \mathbb{N}$ satisfying the conclusions of Lemma 2. Set

$$M := \max_{i,j,k}(M_i, M_{jk}) + 1.$$

Then for any $m \geq M$ and $\beta \in \mathbb{P}^1(\overline{K})$ such that $\varphi^m(\beta) \in \mathcal{A}$ but $\varphi^t(\beta) \notin \mathcal{A}$ for all $0 \leq t < m$, we have $\varphi^{m-1}(\beta) \notin \mathcal{A}$. Hence, $\varphi^{m-1}(\beta)$ is either some γ_{jk} or is in $\varphi^{-1}(\alpha_i)$ for some nonperiodic α_i; that is, β is an element either of some $\varphi^{-(m-1)}(\gamma_{jk})$ or of $\varphi^{-m}(\alpha_i)$ for some nonperiodic α_i. Thus, by the conclusions of Lemma 2, β satisfies conditions (i) and (ii), as desired.

We will now apply Proposition 1 to several maps $\varphi_1, \ldots, \varphi_g$ at once to obtain a proof of Theorem 5.

Proof (*Proof of Theorem 5*) We note first that it suffices to prove our result for a finite extension of K. Indeed, if L/K is a finite extension and $\mathfrak{q} \cap \mathfrak{o}_K = \mathfrak{r}$ for a prime $\mathfrak{q} \subseteq \mathfrak{o}_L$, then $\varphi_i^m(\gamma)$ is congruent to α modulo $\mathfrak{q}$ if and only if $\varphi_i^m(\gamma)$ is congruent to α modulo $\mathfrak{r}$. Moreover, given a positive density set of primes $\mathcal{Q}$ of L, the set $\mathcal{P} = \{\mathfrak{q} \cap \mathfrak{o}_K : \mathfrak{q} \in \mathcal{Q}\}$ also has positive density as a set of primes of K.

We may assume, for all $i = 1, \ldots, g$, that every φ_i-preperiodic point $\alpha \in \mathcal{A}_i$ is in fact fixed by φ_i. Indeed, for each such i and α, choose integers $j_\alpha \geq 0$ and $\ell_\alpha \geq 1$ such that $\varphi_i^{j_\alpha}(\alpha) = \varphi_i^{j_\alpha + \ell_\alpha}(\alpha)$. Set $j := \max_\alpha\{j_\alpha\}$, and replace each $\alpha \in \mathcal{A}_i$ by $\varphi_i^j(\alpha)$. Similarly, set $\ell := \operatorname{lcm}_\alpha\{\ell_\alpha\}$, and enlarge each $\mathcal{T}_i = \{\gamma_{i1}, \ldots, \gamma_{is_i}\}$ to include $\varphi_i^b(\gamma_{ic})$ for all $b = 1, \ldots, \ell - 1$ and $c = 1, \ldots, s_i$. Finally, replace each φ_i by φ_i^ℓ, so that for the new data, all the φ_i-preperiodic points in $\alpha \in \mathcal{A}_i$ are fixed by φ_i. If the Theorem holds for the new data, then it holds for the original data, since for any $m \geq M$ and any prime $\mathfrak{p}$ at which every φ_i has good reduction, $\varphi_i^m(\gamma_{ij}) \equiv \alpha \pmod{\mathfrak{p}}$ implies $(\varphi_i^\ell)^a(\varphi_i^b(\gamma_{ij})) \equiv \varphi_i^j(\alpha) \pmod{\mathfrak{p}}$, writing $m + j$ as $a\ell + b$ with $a \geq 0$ and $0 \leq b < \ell$.

We fix the following notation for the remainder of the proof. If there is any index i such that $\mathcal{A}_i$ contains a nonperiodic point, we may assume that this happens for $i = 1$, and we denote the nonperiodic point by α'. By hypothesis, all points in $\mathcal{A}_1 \smallsetminus \{\alpha'\}$ are φ_1-preperiodic, and we denote them by α_{1j}; similarly, for each $i \geq 2$, all points in $\mathcal{A}_i$ are φ_i-preperiodic, and we denote them by α_{ij}. By the previous paragraph, we may assume that φ_i fixes α_{ij} for all i, j.

Note that there are only finitely many primes $\mathfrak{p}$ of bad reduction for any φ_i, finitely many for which $\operatorname{char} k_\mathfrak{p} \leq \max_i\{\deg \varphi_i\}$, and finitely many such that the ramification index of φ_i at some $\alpha_{ij} \in \mathcal{A}_i$ is greater modulo $\mathfrak{p}$ than over K. On the other hand, by [4, Lemma 4.3], there are infinitely many primes $\mathfrak{p}$ of K such that α' is not φ_1-periodic modulo $\mathfrak{p}$. Hence, we may choose such a prime $\mathfrak{p}$, and then a prime $\tilde{\mathfrak{p}}$ of $\mathfrak{o}_{\overline{K}}$ for which $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_K$, that simultaneously satisfy, for each $i = 1, \ldots, g$, the hypotheses of Proposition 1 for φ_i and $\mathcal{A}_i$.

Applying Proposition 1, for each $i = 1, \ldots, g$ we obtain finite extensions E_i of K satisfying the conclusions of that result. Let L be the compositum of the fields

$E_1, \ldots, E_g$, and let $\mathfrak{q} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_L$. Then for all $i = 1, \ldots, g$, all sufficiently large M, and all $\beta \in \overline{K}$ such that $\varphi_i^M(\beta) \in \mathcal{A}_i$ but $\varphi_i^t(\beta) \notin \mathcal{A}_i$ for $0 \le t < M$, we have

(i) $\mathfrak{r}$ does not ramify over $\mathfrak{q}$, and
(ii) $[\mathfrak{o}_{L(\beta)}/\mathfrak{r} : \mathfrak{o}_L/\mathfrak{q}] > 1$,

where $\mathfrak{r} = \tilde{\mathfrak{p}} \cap \mathfrak{o}_{L(\beta)}$. As noted at the start of this proof, it suffices to prove the Theorem for the field L.

Fix such a sufficiently large integer M, and let F/L be the finite extension obtained by adjoining all points $\beta \in \mathbb{P}^1(\overline{L})$ such that for some $i = 1, \ldots, g$ we have $\varphi_i^M(\beta) \in \mathcal{A}_i$ but $\varphi_i^t(\beta) \notin \mathcal{A}_i$ for all $0 \le t < M$. Note that F/L is a Galois extension, since each $\mathcal{A}_i$ and each φ_i is defined over L. Moreover, by property (i) above, F/L is unramified over $\mathfrak{q}$. By property (ii), then, the Frobenius element of $\mathfrak{q}$ belongs to a conjugacy class of $\mathrm{Gal}(F/L)$ whose members do not fix any of the points β. By the Chebotarev density theorem (Theorem 4), then, there is a positive density set of primes $\mathcal{S}$ of L whose Frobenius conjugacy classes in $\mathrm{Gal}(F/L)$ do not fix any of the points β.

Fix any prime $\mathfrak{r} \in \mathcal{S}$. We make the following claim.

Claim Let $m \ge 0$, let $1 \le i \le g$, and let $z \in \mathbb{P}^1(L)$ be a point such that $\varphi_i^m(z)$ is congruent modulo $\mathfrak{r}$ to an element of $\mathcal{A}_i$. Then there is some $0 \le t < M$ such that $\varphi_i^t(z)$ is congruent modulo $\mathfrak{r}$ to an element of $\mathcal{A}_i$.

To prove the claim, note first that the conclusion is vacuous if $m < M$; thus, we may assume that $m \ge M$. In fact, given any index i and point z as in the claim, we may assume that m is the minimal integer $m \ge M$ satisfying the hypothesis, namely that $\varphi_i^m(z) = \varphi_i^M(\varphi_i^{m-M}(z))$ is congruent modulo $\mathfrak{r}$ to an element of $\mathcal{A}_i$. However, by the defining property of the set of primes $\mathcal{S}$, there cannot be any points $w \in \mathbb{P}^1(L)$ such that $\varphi_i^M(w)$ is congruent modulo $\mathfrak{r}$ to an element of $\mathcal{A}_i$ but $\varphi_i^t(w) \notin \mathcal{A}_i$ for all $0 \le t < M$. Choosing $w = \varphi_i^{m-M}(z) \in \mathbb{P}^1(L)$, then, there must be some $0 \le t < M$ such that $\varphi_i^t(\varphi_i^{m-M}(z))$ is congruent modulo $\mathfrak{r}$ to an element of $\mathcal{A}_i$. Thus, $\varphi_i^{m-M+t}(z)$ is congruent modulo $\mathfrak{r}$ to an element of $\mathcal{A}_i$; but $0 \le m - M + t < m$, contradicting the minimality of m and proving Claim 3.

Let $\mathcal{U}$ be the subset of $\mathcal{S}$ consisting of primes $\mathfrak{r} \in \mathcal{S}$ such that one or more of the following holds:

(i) $\varphi_i^t(\gamma) \equiv \alpha_{ij} \pmod{\mathfrak{r}}$ for some $i = 1, \ldots, g$, some $\gamma \in \mathcal{T}_i$, some φ_i-periodic $\alpha_{ij} \in \mathcal{A}_i$, and some $0 \le t < M$; or
(ii) $\varphi_1^t(\alpha') \equiv \alpha \pmod{\mathfrak{r}}$ for some $\alpha \in \mathcal{A}_1$ and some $1 \le t \le M$.

Note, for each φ_i-periodic $\alpha_{ij} \in \mathcal{A}_i$, we cannot have $\varphi_i^r(\gamma) = \alpha_{ij}$ for any $r \ge 0$ and any $\gamma \in \mathcal{T}_i$, since the elements of $\mathcal{T}_i$ are not φ_i-preperiodic. (However, it *is* possible that $\varphi_1^r(\gamma) = \alpha'$ for some r and some $\gamma \in \mathcal{T}_1$.) Thus, $\mathcal{U}$ is a finite subset of $\mathcal{S}$, and hence $\mathcal{S}' := \mathcal{S} \setminus \mathcal{U}$ has positive density. We will now show that the Theorem holds for the field L, the integer M, and this set of primes $\mathcal{S}'$.

Suppose there exist a prime $\mathfrak{r} \in \mathcal{S}'$, an index $1 \le i \le g$, points $\alpha \in \mathcal{A}_i$ and $\gamma \in \mathcal{T}_i$, and an integer $m \ge M$ such that $\varphi_i^m(\gamma) \equiv \alpha \pmod{\mathfrak{r}}$. By Claim 3, there is an integer $0 \le t < M$ and a point $\tilde{\alpha} \in \mathcal{A}_i$ such that $\varphi_i^t(\gamma) \equiv \tilde{\alpha} \pmod{\mathfrak{r}}$. By property (i) above, then, we must have $i = 1$ and $\tilde{\alpha} = \alpha'$. Moreover, since $\varphi_1^{m-t-1}(\varphi_1(\alpha')) \equiv \alpha \pmod{\mathfrak{r}}$,

and since $m - t - 1 \geq 0$, Claim 3 tells us that there is some $0 \leq k < M$ such that $\varphi_1^{k+1}(\alpha')$ is congruent modulo $\mathfrak{r}$ to an element of $\mathcal{A}_1$, contradicting property (ii) above, and hence proving the Theorem.

4 Applications

4.1 Proofs of the Corollaries

We are now prepared to prove the Corollaries of Theorem 5 stated in Sect. 1.

Proof (*Proof of Corollary 2*) We begin by noting that φ has good reduction at all but finitely many primes $\mathfrak{p}$ of K.

If α is φ-preperiodic but not φ-periodic, then for all but finitely many primes $\mathfrak{p}$ of K, the reductions modulo $\mathfrak{p}$ of the finitely many points in the forward orbit of α are all distinct. Hence $\alpha_\mathfrak{p}$ is $\varphi_\mathfrak{p}$-preperiodic but not $\varphi_\mathfrak{p}$-periodic. Thus, we may assume that α is not φ-preperiodic.

Applying Theorem 5 with $g = 1$, $\varphi_1 = \varphi$, and $\mathcal{T}_1 = \mathcal{A}_1 = \{\alpha\}$, there is a positive density set of primes $\mathfrak{p}$ of K for which

$$\varphi^m(\alpha) \not\equiv \alpha \pmod{\mathfrak{p}}$$

for *all* sufficiently large m. Hence, $\alpha_\mathfrak{p}$ is not $\varphi_\mathfrak{p}$-periodic.

Proof (*Proof of Corollary 3*) We begin by noting that E has good reduction at all but finitely many primes $\mathfrak{p}$ of K. (For more details on elliptic curves, see [18].) Write E in Weierstrass form, and let $x : E \to \mathbb{P}^1$ be the morphism that takes a point P to the x-coordinate of P. Let $[q] : E \to E$ denote the multiplication-by-q map, and let $\varphi \in K(x)$ be the associated Lattès map; that is, φ satisfies the identity $x \circ [q] = \varphi \circ x$.

Since Q is not torsion, the point $[q^{n-1}]Q \in E(K)$ is also not torsion, and therefore its x-coordinate $\alpha := x([q^{n-1}]Q) \in \mathbb{P}^1(K)$ is not φ-preperiodic. Hence, by Corollary 2, there is a positive density set of primes $\mathfrak{p}$ of K such that the reduction $\alpha_\mathfrak{p}$ is not $\varphi_\mathfrak{p}$-periodic. Equivalently, $[q^{m+n-1}](Q_\mathfrak{p}) \neq [q^{n-1}]Q_\mathfrak{p}$ for all $m \geq 1$. However, if the q-primary part of the order of $Q_\mathfrak{p}$ were at most q^{n-1}, then there *would* be some $m \geq 1$ such that $[q^{n-1+m}](Q_\mathfrak{p}) = [q^{n-1}]Q_\mathfrak{p}$. Thus, q^n must divide the order of $Q_\mathfrak{p}$.

4.2 Dynamical Mordell–Lang problems

The following conjecture was proposed in [8,10].

Conjecture 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 $x \in X(\mathbb{C})$ be an arbitrary point. Then the set of integers $n \in \mathbb{N}$ such that $\Phi^n(x) \in V(\mathbb{C})$ is a union of finitely many arithmetic progressions $\{nk + \ell\}_{n\in\mathbb{N}}$, where $k, \ell \geq 0$ are nonnegative integers.*

Theorem 5 allows us to prove a few new cases of Conjecture 1 over number fields. First we need to state a result which will be crucial for our proof; this is [4, Theorem 3.4].

Proposition 2 *Let V be a subvariety of $\left(\mathbb{P}^1\right)^g$ 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 $\left(\mathbb{P}^1\right)^g$. 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.*

In [4, Theorem 1.4] it is proven that Conjecture 1 holds for curves V and for endomorphisms Φ of $X = (\mathbb{P}^1)^g$ of the form $(\varphi_1, \ldots, \varphi_g)$ as long as each critical point of each φ_i is not φ_i-preperiodic. Using Theorem 5 we prove the following result which goes in the opposite direction of [4, Theorem 1.4] since it holds for endomorphisms of $(\mathbb{P}^1)^g$ of the form $(\varphi_1, \ldots, \varphi_g)$ for which at most one φ_i has a critical point that is not φ_i-preperiodic (also our result holds for arbitrary subvarieties V as opposed to only curves as it is the case in [4, Theorem 1.4]).

Theorem 6 *Let K be a number field, let $V \subset \left(\mathbb{P}^1\right)^g$ be a subvariety defined over K, let $x = (x_1, \ldots, x_g) \in (\mathbb{P}^1)^g(K)$, and let $\Phi := (\varphi_1, \ldots, \varphi_g)$ act on $\left(\mathbb{P}^1\right)^g$ coordinatewise, where each $\varphi_i \in K(t)$ is a rational function of degree at least 2. Suppose that at most one φ_i has a critical point α that is not φ_i-preperiodic, and that all other critical points of that φ_i are preperiodic. Then the set of integers $n \in \mathbb{N}$ such that $\Phi^n(x) \in V(\overline{K})$ is a union of finitely many arithmetic progressions $\{nk + \ell\}_{n \in \mathbb{N}}$, where $k, \ell \geq 0$ are nonnegative integers.*

Proof If x_g is φ_g-preperiodic, we can absorb the first finitely many iterates that may lie on V into trivial arithmetic progressions $\{nk + \ell\}_{n \geq 0}$ with $k = 0$. Thus, we may assume that x_g is φ_g-periodic, of some period $j \geq 1$. By restricting our attention to progressions $\{nk + \ell\}_{n \geq 0}$ with $j | k$, then, it suffices to assume x_g is fixed by φ_g, and hence the dimension may be reduced to $g - 1$. By induction on g, then, we may assume that no x_i is φ_i-preperiodic.

By Theorem 5, there exist a constant M and a positive proportion of primes $\mathfrak{p}$ of K such that for each $i = 1, \ldots, g$, φ_i has good reduction at $\mathfrak{p}$, $\deg \varphi_i < \operatorname{char} k_\mathfrak{p}$, and $\varphi_i^m(x_i)$ is not congruent modulo $\mathfrak{p}$ to any critical point of φ_i for all $m \geq M$. Fix any such $\mathfrak{p}$, and note that the derivative of the reduction $(\varphi_{i,\mathfrak{p}})'$ is nontrivial, because φ_i has good reduction and $1 \leq \deg \varphi_i < \operatorname{char} k_\mathfrak{p}$. Thus, $\varphi_i'(\varphi_i^m(x_i))$, or its appropriate analogue if $\varphi_i^m(x_i)$ lies in the residue class at ∞, is a $\mathfrak{p}$-adic unit for all $m \geq M$. It follows that $\varphi_i^m(x_i) \not\equiv \gamma \pmod{\mathfrak{p}}$ for any attracting periodic point γ of φ_i; applying Proposition 2 completes our proof.

To state the following special case of Theorem 6, we recall that a rational function is said to be *post-critically finite* if all of its critical points are preperiodic.

Corollary 7 *Let K be a number field, let $V \subset \left(\mathbb{P}^1\right)^g$ be a subvariety defined over K, let $x = (x_1, \ldots, x_g) \in (\mathbb{P}^1)^g(K)$, and let $\Phi := (\varphi_1, \ldots, \varphi_g)$ act on $\left(\mathbb{P}^1\right)^g$*

coordinatewise, where each $\varphi_i \in K(t)$ is post-critically finite and of degree at least 2. Then the set of integers $n \in \mathbb{N}$ such that $\Phi^n(x) \in V(\overline{K})$ is a union of finitely many arithmetic progressions $\{nk + \ell\}_{n\in\mathbb{N}}$, where $k, \ell \geq 0$ are nonnegative integers.

In the case that $\varphi_i = f$ for all i for some quadratic polynomial f, we have the following result which generalizes both [4, Theorem 1.6] and [4, Theorem 1.7]. Note that [4, Theorem 1.6] is valid only for quadratic polynomials f for which their critical point is not preperiodic, while [4, Theorem 1.7] is valid only for quadratic polynomials $f \in \mathbb{Q}[x]$ and for starting point $x \in (\mathbb{P}^1)^g(\mathbb{Q})$.

Theorem 8 *Let K be a number field, let $V \subset \left(\mathbb{P}^1\right)^g$ be a subvariety defined over K, let $x = (x_1, \ldots, x_g) \in (\mathbb{P}^1)^g(K)$, let $f \in K[t]$ be a quadratic polynomial, and let $\Phi := (f, \ldots, f)$ act on $\left(\mathbb{P}^1\right)^g$ coordinatewise. Then the set of integers $n \in \mathbb{N}$ such that $\Phi^n(x) \in V(\overline{K})$ is a union of finitely many arithmetic progressions $\{nk + \ell\}_{n\in\mathbb{N}}$, where $k, \ell \geq 0$ are nonnegative integers.*

Proof As in the proof of Theorem 6, we may assume that none of $x_1, \ldots, x_g$ is preperiodic. Let $\mathcal{T} = \{x_1, \ldots, x_g\}$, and let $\mathcal{A} = \{\alpha', \infty\}$, where $\alpha' \in K$ is the unique finite critical point of f. Then the map f, with the finite sets $\mathcal{A}$ and $\mathcal{T}$, satisfies the hypotheses of Theorem 5, and the rest of the proof is exactly like that of Theorem 6.

We obtain a similar result when each f_i takes the form $x^2 + c_i$ for $c_i \in \mathbb{Z}$. Our result generalizes [4, Theorem 1.8] which is valid only for starting points x whose coordinates are in $\mathbb{Z}$.

Theorem 9 *Let K be a number field, let $V \subset \left(\mathbb{P}^1\right)^g$ be a subvariety defined over K, let $x = (x_1, \ldots, x_g) \in (\mathbb{P}^1)^g(K)$, let $f_i(z) = z^2 + c_i$ with $c_i \in \mathbb{Z}$ for $i = 1, \ldots, g$, and let $\Phi := (f_1, \ldots, f_g)$ act on $(\mathbb{P}^1)^g$ coordinatewise. Then the set of integers $n \in \mathbb{N}$ such that $\Phi^n(x) \in V(\mathbb{Q})$ is a union of finitely many arithmetic progressions $\{nk + \ell\}_{n\in\mathbb{N}}$, where $k, \ell \geq 0$ are nonnegative integers.*

Proof As before, we can assume that no x_i is f_i-preperiodic. By [13, Theorem 1.2], for each $i = 1, \ldots, g$ such that $c_i \neq 0, -1, -2$, the set $\mathcal{U}_i$ of primes $\mathfrak{p}$ for which 0 is not periodic modulo $\mathfrak{p}$ has density 1. (The results in [13] are stated for $x \in \mathbb{Z}$, but the same proof works for arbitrary $x \in K$.) Intersecting $\mathcal{U}_i$ over all such i gives a set of primes $\mathcal{S}_1$ of density 1.

For each $i = 1, \ldots, g$, define $\mathcal{A}_i = \{\infty\}$ if $c_i \neq 0, -1, -2$, and $\mathcal{A}_i = \{0, \infty\}$ if $c_i = 0, -1, -2$. Because 0 is f_i-preperiodic if c_i is 0, -1, or -2, and because ∞ is exceptional and fixed for any c_i, we may apply Theorem 5 and conclude that

$$\mathcal{S}_2 := \{\mathfrak{p} \,:\, f_i^m(x_i) \notin \mathcal{A}_i \text{ modulo } \mathfrak{p} \text{ for all } m \geq M\}$$

must have positive density, for some $M \geq 0$. Thus, the set $\mathcal{S} = \mathcal{S}_1 \cap \mathcal{S}_2$ has positive density; the rest of the proof is now like that of Theorem 6.

4.3 Newton's method at finite places

Consider a rational function $N(x)$ of the form $N(x) = x - \frac{f(x)}{f'(x)}$, where $f \in K[x]$ is a polynomial of degree at least 2. Given $\gamma \in K$, let $\mathcal{S}$ be the set of primes $\mathfrak{p}$ of K such that $\{N^m(x)\}_{m=1}^{\infty}$ converges $\mathfrak{p}$-adically to a root of f. In [7], Faber and Voloch conjecture that $\mathcal{S}$ has density 0; that is, Newton's method for approximating roots of a polynomial "fails" at almost all finite places of K. Although we cannot use our methods to prove this conjecture, we can prove the following result, which says that given a finite set of nonpreperiodic points and a finite set of rational functions $N_i(x)$ arising from Newton's method, the set of primes at which convergence fails has positive density. In fact, we prove that for large enough m, the iterate $N_i^m(x)$ is not even in the same residue class modulo $\mathfrak{p}$ as any of the roots of f_i.

Theorem 10 *Let $f_1, \ldots, f_g \in K[x]$ be polynomials of degree at least 2. Let $N_i(x) = x - \frac{f_i(x)}{f_i'(x)}$ for $i = 1, \ldots, g$, and let $\mathcal{T}_i$ be finite subsets of K such that no $\mathcal{T}_i$ contains any N_i-preperiodic points. Then there is a positive integer M and a positive density set of primes $\mathcal{P}$ of K such that for any $i = 1, \ldots, g$, any $\gamma \in \mathcal{T}_i$, any root α of $f_i(x)$, any $m \geq M$, and any $\mathfrak{p} \in \mathcal{P}$, we have*

$$N_i^m(\gamma) \not\equiv \alpha \pmod{\mathfrak{p}}.$$

Proof The result is immediate from Theorem 5, since each root of f_i is a fixed point of N_i.

5 Heuristics and higher dimensions

We embarked on this project hoping to prove the cyclic case of the Dynamical Mordell–Lang Conjecture for endomorphisms Φ of $\mathbb{P}^d$ by the strategy outlined in [4]. (For a more general variant of this conjecture, see [11,12].) More precisely, assuming Φ is defined over a number field K, we had hoped to prove that for each $\alpha \in \mathbb{P}^d(K)$, one can *always* find a prime $\mathfrak{p}$ of K such that for all sufficiently large n, $\Phi^n(\alpha)$ is not congruent modulo $\mathfrak{p}$ to a point on the ramification divisor of Φ. This is equivalent to saying that, modulo $\mathfrak{p}$, the intersection of the ramification divisor and the "periodic part" of the forward orbit is empty. (Since any point is preperiodic modulo $\mathfrak{p}$, it makes sense to divide a forward orbit into its tail and its periodic part.) When this condition is met, even at a single prime of suitably good reduction, one can apply the generalized Skolem-type techniques of [5] to prove the cyclic case of the Dynamical Mordell–Lang Conjecture for Φ and α.

Unfortunately, a random map model suggests that there may be no such prime when $d > 4$. Roughly, assuming $K = \mathbb{Q}$, the issue is that if $\bar{\Phi} : \mathbb{P}^d \longrightarrow \mathbb{P}^d$, then under certain assumptions of randomness, an argument akin to the birthday paradox suggests that the periodic part of the forward orbit of a point under $\bar{\Phi}$ should typically be of order $p^{d/2}$. Since the proportion of points in $\mathbb{P}^d(\mathbb{F}_p)$ that lie on the ramification divisor should be about $1/p$, this means that for $d \geq 3$ and p large, the chances are very high that the periodic part of a given forward orbit passes through the ramification divisor

over $\mathbb{F}_p$. In fact, a naïve argument would seem to indicate that this chance is so high when $d \geq 3$ that even taking the product over all p, one is left with a nonzero chance that the periodic part of the forward orbit of a given point passes through the ramification divisor modulo p for *all* p. To our surprise, however, a more thorough analysis shows that the likelihood of periods intersecting the ramification divisor modulo p is dominated by *very short* cycles, namely of length $< p \log p$ (rather than $p^{d/2}$, the expected length of a period modulo p.) This changes the dimension cutoff so that it is only when $d \geq 5$ that there is a nonzero chance that the periodic part of the forward orbit of a given point passes through the ramification divisor modulo p for all p.

In Sect. 5.1, we explain this random model in some detail and present evidence that it is accurate in at least some cases.

Remark 1 The idea of using random maps to model orbit lengths is not new—for (generic) quadratic polynomials in one variable it is at the heart of Pollard's rho method [17] for factoring integers. Under the random map assumption, Pollard's method factors an integer n in (roughly) time $p^{1/2}$, where p is the smallest prime divisor of n. As for the validity of the random model, unfortunately not much is known. In [3], Bach showed that for a randomly selected quadratic polynomial and starting point, the random map heuristic correctly predicts the probability of finding orbits of length about $\log p$. Further, in [20], Silverman considered general morphisms of $\mathbb{P}^n$ defined over a number field, and he showed that for any $\epsilon > 0$, a random starting point has $\gg (\log p)^{1-\epsilon}$ distinct elements in its orbit modulo p for a full density subset of the primes; see also [1]. Silverman [20] also conjectured that the period is greater than $p^{d/2-\epsilon}$ for a full density subset of the primes, and motivated by experimental data, he also made a more precise conjecture for quadratic polynomials in dimension 1.

5.1 A probabilistic model for orbits and cycles

Let X be a (large) finite set, and let $f : X \to X$ be a random map in the following sense: for each $x \in X$, select the image $f(x)$ by randomly selecting an element of X, with uniform distribution.

5.1.1 Cycle lengths

Fix a starting point $x_0 \in X$, and inductively define $x_{n+1} = f(x_n)$. Since X is finite, x_0 is necessarily preperiodic. Let τ be the collision time for the orbit $(x_0, x_1, \ldots)$, i.e., τ is the smallest positive integer such that $x_\tau = x_s$ for some $s < \tau$. For any integer $k \geq 0$, we have $x_j \notin \{x_0, x_1, \ldots, x_{j-1}\}$ for all $j \leq k$ if and only if $\tau > k$. Thus, the randomness assumption on f implies that

$$\text{Prob}(\tau > k) = \prod_{j=1}^{k} \Big(1 - \frac{j}{|X|}\Big) = \exp\Big[\sum_{j=1}^{k} \log\Big(1 - \frac{j}{|X|}\Big)\Big],$$

as in the birthday paradox. From the Taylor series expansion $\log(1-x) = -(x + x^2/2 + x^3/3 + \cdots)$, we deduce the inequality

$$\text{Prob}(\tau > k) \le \exp\left(-\frac{k(k+1)}{2|X|}\right), \tag{2}$$

and similarly we find that for $k = o(|X|^{2/3})$,

$$\text{Prob}(\tau > k) = \exp\left(-\frac{k^2}{2|X|}\right) \cdot (1 + o(1)), \tag{3}$$

since

$$\begin{aligned}\text{Prob}(\tau > k) &= \exp\left(-\frac{k(k+1)}{2|X|} + O(k^3/|X|^2)\right) \\ &= \exp\left(-\frac{k^2}{2|X|} + O(k/|X| + k^3/|X|^2)\right).\end{aligned} \tag{4}$$

In addition, if we let $\alpha(k) := \text{Prob}(\tau > k-1)$, then

$$\begin{aligned}\text{Prob}(\tau = k) &= \text{Prob}(\tau > k-1) - \text{Prob}(\tau > k) \\ &= \prod_{j=1}^{k-1}\left(1 - \frac{j}{|X|}\right) - \prod_{j=1}^{k}\left(1 - \frac{j}{|X|}\right) \\ &= \left[1 - \left(1 - \frac{k}{|X|}\right)\right] \cdot \prod_{j=1}^{k-1}\left(1 - \frac{j}{|X|}\right) = \frac{k}{|X|} \cdot \alpha(k).\end{aligned}$$

Define $\mathcal{C} := \{x_s = x_\tau, x_{s+1}, \ldots, x_{\tau-1}\}$ to be the periodic part of the orbit of x_0. Conditioning on $\tau = k$, the random map assumption implies that x_k is uniformly selected among $\{x_0, \ldots, x_{k-1}\}$, and hence

$$\text{Prob}\Big(|\mathcal{C}| = \ell \Big| \tau = k\Big) = \frac{1}{k} \quad \text{for any} \quad \ell \le k.$$

The cycle length probability may thus be written as

$$\begin{aligned}\text{Prob}(|\mathcal{C}| = \ell) &= \sum_{k \ge \ell} \text{Prob}(|\mathcal{C}| = \ell \big| \tau = k) \cdot \text{Prob}(\tau = k) \\ &= \sum_{k \ge \ell} \frac{1}{k} \cdot \text{Prob}(\tau = k) = \sum_{k \ge \ell} \frac{1}{k} \cdot \frac{k}{|X|} \cdot \alpha(k) = \frac{1}{|X|} \sum_{k \ge \ell} \alpha(k).\end{aligned} \tag{5}$$

Before stating the next Lemma we recall that the *Gaussian error function* erfc is defined as (cf. [2, Chapter 7])

$$\text{erfc}(s) := \frac{2}{\sqrt{\pi}} \int_s^\infty e^{-t^2}\, dt.$$

Lemma 3 *If $\ell = o(|X|^{2/3})$ then, as $|X| \to \infty$,*

$$\mathrm{Prob}(|\mathcal{C}| = \ell) = \sqrt{\frac{\pi}{2|X|}} \cdot \left(\mathrm{erfc}\left(\ell/\sqrt{2|X|}\right) + o(1)\right).$$

Proof By (5), we find that

$$\mathrm{Prob}(|\mathcal{C}| = \ell) = \frac{1}{|X|}\sum_{k=\ell}^{|X|}\alpha(k) = \frac{1}{|X|}\left(\sum_{k=1}^{|X|}\alpha(k) - \sum_{1\le k<\ell}\alpha(k)\right). \tag{6}$$

We begin by evaluating the first sum. Recalling that $\alpha(k) = \mathrm{Prob}(\tau > k-1)$, if $k = o(|X|^{2/3})$, then by (3), we have

$$\alpha(k) = \exp\big(-k^2/(2|X|)\big)\cdot\big(1+o(1)\big).$$

Moreover, by (2) the inequality

$$\alpha(k) \ll \exp\big(-k^2/(3|X|)\big)$$

holds for $k \ge 1$. Thus, setting $Q(T) := T^{2/3}/\log T$, we have

$$\begin{aligned}\sum_{k=1}^{|X|}\alpha(k) &= \sum_{1\le k\le Q(|X|)}\alpha(k) + \sum_{Q(|X|)<k\le|X|}\alpha(k)\\ &= \big(1+o(1)\big)\cdot\sum_{1\le k\le Q(|X|)} e^{-k^2/(2|X|)} + O\left(\int_{Q(|X|)-1}^{\infty} e^{-t^2/(3|X|)}\,dt\right).\end{aligned} \tag{7}$$

To show that the contribution from the integral is negligible, we note the inequality (valid for all $A, B > 0$)

$$\int_A^\infty e^{-t^2/B}\,dt = \sqrt{B}\int_{A/\sqrt{B}}^\infty e^{-s^2}\,ds \le \frac{B}{A}\int_{A/\sqrt{B}}^\infty s e^{-s^2}\,ds = \frac{B}{2A}e^{-A^2/B}.$$

Thus,

$$\begin{aligned}\int_{Q(|X|)-1}^{\infty} e^{-t^2/(3|X|)}\,dt &\le \frac{3|X|}{2Q(|X|)-2}\exp\left(-\frac{\big(Q(|X|)-1\big)^2}{3|X|}\right)\\ &\ll |X|^{1/3}\log|X|\exp\left(-\frac{|X|^{1/3}}{3(\log|X|)^2}\right) = o(1)\end{aligned} \tag{8}$$

as $|X| \to \infty$.

Meanwhile, note that for any $L \geq 1$,

$$\sum_{1 \leq k \leq L} e^{-k^2/(2|X|)} = \sqrt{2|X|} \cdot \left[\int_0^{\lfloor L \rfloor / \sqrt{2|X|}} e^{-t^2}\, dt + O\left(\frac{\lfloor L \rfloor}{2|X|}\right) \right]$$
$$= \sqrt{2|X|} \cdot \int_0^{L/\sqrt{2|X|}} e^{-t^2}\, dt + O\left(\frac{L}{\sqrt{2|X|}} + 1\right),$$

by interpreting the sum as a $1/\sqrt{2|X|}$-spaced Riemann sum approximation of an integral and noting that $|e^{-s^2} - e^{-t^2}| \leq |s - t|$ for all $s, t \in \mathbb{R}$. Thus, the sum in the right side of (7) is

$$\sum_{1 \leq k \leq Q(|X|)} e^{-k^2/(2|X|)} = \sqrt{2|X|} \cdot \int_0^{Q(|X|)/\sqrt{2|X|}} e^{-t^2}\, dt + O\left(\frac{Q(|X|)}{\sqrt{2|X|}} + 1\right)$$
$$= \sqrt{2|X|} \cdot \left(\int_0^{\infty} e^{-t^2}\, dt + o(1) \right),$$

and the second sum on the right side of (6) is

$$\sum_{1 \leq k < \ell} \alpha(k) = \big(1 + o(1)\big) \cdot \sum_{k=1}^{\ell-1} e^{-k^2/(2|X|)}$$
$$= \big(1 + o(1)\big) \cdot \left(\sqrt{2|X|} \int_0^{\ell/\sqrt{2|X|}} e^{-t^2}\, dt + O\left(\frac{\ell}{\sqrt{2|X|}} + 1\right) \right).$$

Combining Eqs. (6), (7), and (8) with the above Riemann sum estimates, and recalling that $\operatorname{erfc}(s) = \frac{2}{\sqrt{\pi}} \int_s^{\infty} e^{-t^2}\, dt$, we have

$$\operatorname{Prob}(|\mathcal{C}| = \ell) = \frac{\sqrt{2} \cdot \int_{\ell/\sqrt{2|X|}}^{\infty} e^{-t^2}\, dt + o(1)}{|X|^{1/2}}$$
$$= \sqrt{\frac{\pi}{2|X|}} \cdot \left(\operatorname{erfc}\left(\ell/\sqrt{2|X|}\right) + o(1) \right).$$

□

5.1.2 Cycles intersecting the ramification locus

We now specialize to polynomial maps: let $\phi : \mathbb{A}^d(\mathbb{Z}) \to \mathbb{A}^d(\mathbb{Z})$ be a polynomial map such that its Jacobian matrix $d\phi$ has non-constant determinant, and fix

a starting point $x_0 \in \mathbb{A}^d(\mathbb{Z})$. Given a prime p, let $X_p = \mathbb{A}^d(\mathbb{F}_p)$, and denote by $\phi_p : X_p \to X_p$ the reduction of ϕ modulo p. Further, let $\mathcal{C}_p$ denote the periodic part of the forward orbit of x_0 under ϕ_p, and let $\mathcal{R}_p$ denote the ramification locus of ϕ_p.

We say ϕ has *random map behavior* modulo p if the following two conditions hold:

- $|\mathcal{C}_p|$ has the same probability distribution as the cycle length of a random map on a set of size p^d.
- The probability of a collection of distinct points $y_1, \ldots, y_k \in \mathcal{C}_p$ all belonging to $\mathcal{R}_p$ is $1/p^k$.

By the Weil bounds, $|\mathcal{R}_p| = p^{d-1} \cdot (1+o(1))$, since $\mathcal{R}_p$ is a hypersurface (assumed irreducible for simplicity) defined by the vanishing of the determinant of the Jacobian of the map ϕ_p. Thus, the main thrust of the second assumption above is that the sets $\mathcal{C}_p$ and $\mathcal{R}_p$ are suitably independent.

Proposition 3 *Assume that the polynomial map $\phi : \mathbb{A}^d(\mathbb{Z}) \to \mathbb{A}^d(\mathbb{Z})$ has random map behavior modulo every sufficiently large prime p. If $d \geq 3$, then*

$$\text{Prob}(\mathcal{C}_p \cap \mathcal{R}_p = \emptyset) = \frac{\sqrt{\pi/2}}{p^{d/2-1}} \cdot (1 + o(1)) \quad \text{as } p \to \infty.$$

Proof Fix a large enough prime p. For simplicity of notation, we will write $\mathcal{C}$ and $\mathcal{R}$ instead of $\mathcal{C}_p$ and $\mathcal{R}_p$. Conditioning on the cycle length $|\mathcal{C}|$ being equal to ℓ, we find that $\text{Prob}\Big(\mathcal{C} \cap \mathcal{R} = \emptyset \Big| |\mathcal{C}| = \ell\Big) = (1 - 1/p)^\ell$, and hence

$$\text{Prob}(\mathcal{C} \cap \mathcal{R} = \emptyset) = \sum_{\ell=1}^{p^d} (1 - 1/p)^\ell \cdot \text{Prob}(|\mathcal{C}| = \ell).$$

We start by bounding the contribution from the large cycles. Since $(1 - 1/p)^\ell$ is a decreasing function of ℓ and $\sum_{\ell=1}^{p^d} \text{Prob}(|\mathcal{C}| = \ell) = 1$, we have

$$\sum_{\ell \geq dp \log p}^{p^d} \left(1 - \frac{1}{p}\right)^\ell \cdot \text{Prob}(|\mathcal{C}| = \ell) \leq \left(1 - \frac{1}{p}\right)^{dp \log p} \ll \exp(-d \log p) = p^{-d}.$$

To determine the contribution from the short cycles we argue as follows. By Lemma 3, for $\ell \leq dp \log p = o(p^{d/2})$, we have

$$\text{Prob}(|\mathcal{C}| = \ell) = \sqrt{\frac{\pi}{2p^d}} \cdot \left(\text{erfc}\left(\ell/\sqrt{2p^d}\right) + o(1)\right) = \sqrt{\frac{\pi}{2p^d}} \cdot (1 + o(1))$$

since $\text{erfc}(0) = 1$. Hence,

$$\sum_{\ell=1}^{dp\log p} \left(1 - \frac{1}{p}\right)^{\ell} \cdot \text{Prob}(|\mathcal{C}| = \ell) = \big(1 + o(1)\big) \cdot \sqrt{\frac{\pi}{2p^d}} \cdot \sum_{\ell=1}^{dp\log p} \sum_{1 \le \ell < dp\log p} \left(1 - \frac{1}{p}\right)^{\ell},$$

which, on summing the geometric series, equals

$$\big(1 + o(1)\big) \cdot \sqrt{\frac{\pi}{2p^d}} \cdot \frac{1 - O(p^{-d})}{1 - (1 - 1/p)} = (\sqrt{\pi/2} + o(1)) \cdot p^{1-d/2}.$$

□

Remark 2 For $d = 2$ a similar argument gives that as $p \to \infty$,

$$\begin{aligned}\text{Prob}(\mathcal{C}_p \cap \mathcal{R}_p = \emptyset) &= \big(1 + o(1)\big) \cdot \sum_{\ell \le p^2} (1 - 1/p)^{\ell} \sqrt{\pi/(2p^2)}\,\text{erfc}(\ell/\sqrt{2p^2}) \\ &= \big(1 + o(1)\big) \cdot \sqrt{\pi} \int_0^{\infty} e^{-\sqrt{2}t}\,\text{erfc}(t)\,dt \approx (1 + o(1)) \cdot 0.598.\end{aligned}$$

For $d = 1$ it is easy to see that $\text{Prob}(\mathcal{C}_p \cap \mathcal{R}_p = \emptyset) = 1 + o(1)$ as $p \to \infty$ as follows: since $|\mathcal{R}_p| = O(1)$,

$$\text{Prob}(\mathcal{C}_p \cap \mathcal{R}_p = \emptyset \,\big|\, |\mathcal{C}_p| < p^{1/2}\log p) > (1 - O(1/p))^{p^{1/2}\log p} = 1 + o(1)$$

and, by (2),

$$\begin{aligned}\text{Prob}(|\mathcal{C}_p| \ge p^{1/2}\log p) &\le \text{Prob}(\tau \ge p^{1/2}\log p) \\ &= \exp(-(\log p)^2/2)(1 + o(1)) = o(1).\end{aligned}$$

5.1.3 Global probabilities in higher dimensions

Since it is enough to find *one* prime p for which $\mathcal{C}_p \cap \mathcal{R}_p = \emptyset$, the "probability" that our approach fails—assuming good reduction of the map for all primes, as well as the random map model being applicable and that the "events" $\mathcal{C}_p \cap \mathcal{R}_p = \emptyset$ are independent for different p—in dimension $d \ge 3$ is, by Proposition 3, given by an Euler product of the form

$$\prod_p \left(1 - \frac{\sqrt{\pi/2} + o(1)}{p^{d/2-1}}\right) = \prod_p \left(1 - O(p^{1-d/2})\right).$$

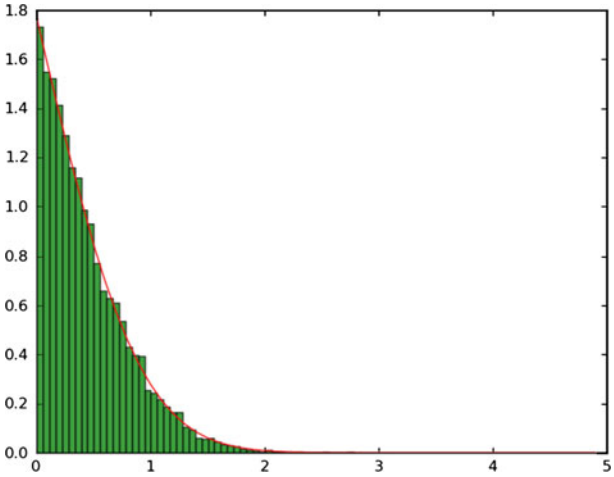

Fig. 1 Normalized cycle length statistics for $p < 100{,}000$

Since the product diverges to zero if $d = 3, 4$, we would in this case expect to find at least one (if not infinitely many) primes for which $\mathcal{C}_p \cap \mathcal{R}_p = \emptyset$. On the other hand, if $d \geq 5$ the product converges, and hence there is a non-vanishing probability that $\mathcal{C}_p \cap \mathcal{R}_p \neq \emptyset$ *for all* primes.

5.2 Numerical evidence for the random model

Letting $\tilde{c} := \frac{|C|}{\sqrt{2|X|}}$ denote the normalized cycle length, it is straightforward to deduce from Lemma 3 that the probability density function of $\tilde{c}$ is given by

$$g(s) = \sqrt{\pi} \cdot \operatorname{erfc}(s), \tag{9}$$

i.e., that

$$\operatorname{Prob}(\tilde{c} \leq t) = \int_0^t g(s)\, ds.$$

In this section, we shall compare observed cycle lengths with this prediction in dimensions one and three.

5.2.1 Cycle lengths in dimension $d = 1$

Consider the map $x \to f(x)$, where $f(x) = x^2 + x + 2$, with starting point $x_0 = 1$. For each prime $p < 100{,}000$, we computed the normalized cycle length $\tilde{c}_p := |\mathcal{C}_p|/\sqrt{2p}$. A histogram plot of $\{\tilde{c}_p\}_{p<N}$ for the resulting data appears in Fig. 1, along with the probability density function $g(t) = \sqrt{\pi} \cdot \operatorname{erfc}(t)$ from (9).

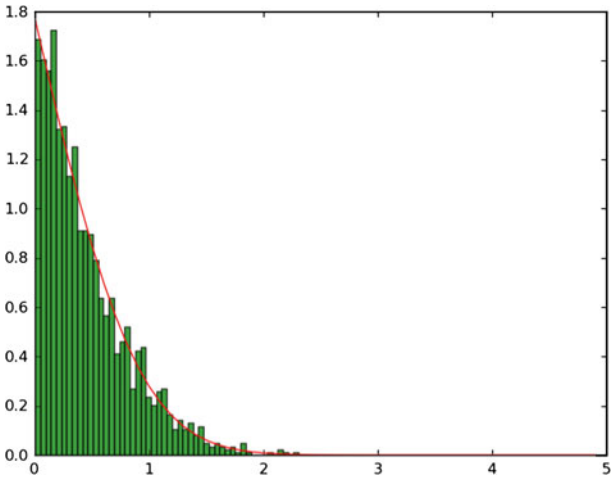

Fig. 2 Normalized cycle length statistics for $p < 21{,}000$

5.2.2 Cycle lengths in dimension $d = 3$

Next, consider the map

$$(x_1, x_2, x_3) \to (f_1(x_1, x_2, x_3),\ f_2(x_1, x_2, x_3),\ f_3(x_1, x_2, x_3)),$$

where

$$\begin{aligned} f_1(x_1, x_2, x_3) &= x_1^2 + 2x_1x_2 - 3x_1x_3 + 4x_2^2 + 5x_2x_3 + 6x_3^2 + 7x_1 \\ &\quad +8x_2 + 9x_3 + 11, \\ f_2(x_1, x_2, x_3) &= 2x_1^2 + 3x_1x_2 + 4x_1x_3 + 5x_2^2 + 6x_2x_3 + 10x_3^2 + 1x_1 \\ &\quad +8x_2 + 3x_3 + 7, \\ f_3(x_1, x_2, x_3) &= 3x_1^2 + 4x_1x_2 + 5x_1x_3 + 6x_2^2 + 17x_2x_3 + 11x_3^2 + 2x_1 \\ &\quad +8x_2 + 5x_3 + 121. \end{aligned}$$

With starting point $x_0 = (1, 2, 3)$, we proceed as we did in dimension one, except that now the normalized cycle length is $\tilde{c}_p := |\mathcal{C}_p|/\sqrt{2p^3}$, and we consider only $p < 21{,}000$. The resulting histogram and expected probability density function appear in Fig. 2.

5.2.3 Probability that $\mathcal{R}_p \cap \mathcal{C}_p = \emptyset$

To further check the accuracy of the predictions of Sect. 5.1.2, we randomly generated 50,000 degree 2 polynomial maps $\varphi : \mathbb{A}^d \to \mathbb{A}^d$ with integer coefficients and checked how often the forward orbit of $(0, \ldots, 0)$ had a periodic point on the ramification divisor modulo p; see Fig. 3. In both cases, the data shows that as p increases, the probability quickly goes to 0 in dimension 1, remains roughly constant in dimension 2

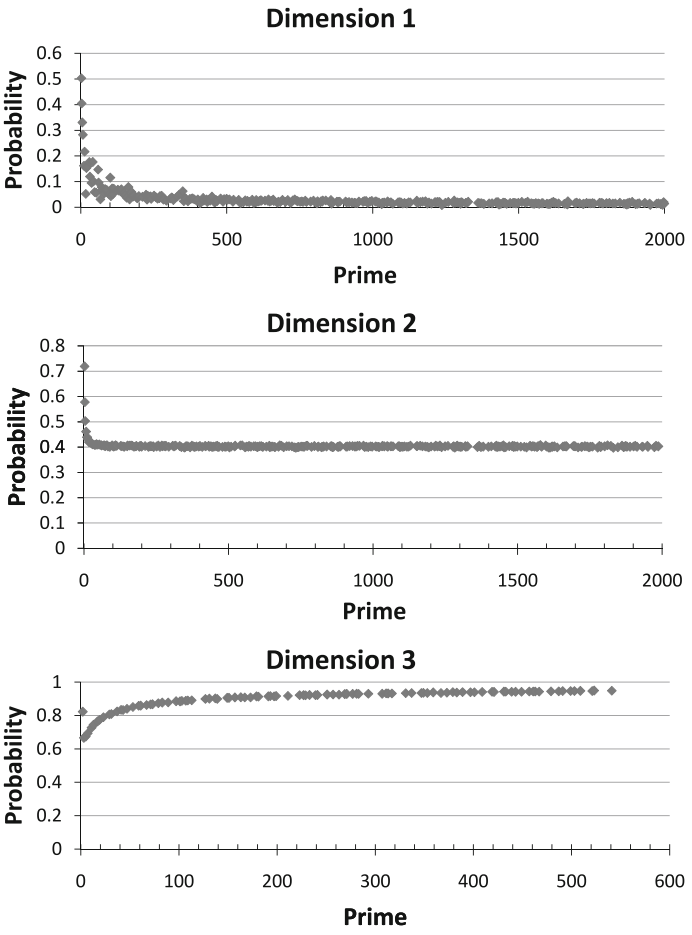

Fig. 3 Probability that the forward orbit of a point has a periodic point lying on the ramification divisor modulo p

(compare with Remark 2 and note that $1 - 0.598 \simeq 0.4$), and quickly goes to 1 in dimension 3, as suggested by our model.

For $d = 3$, we also compared the number of primes $p < N$ for which $\mathcal{C}_p \cap \mathcal{R}_p = \emptyset$ with the prediction given by the random map model. Thus, given p, let $X_p = 1$ if $\mathcal{C}_p \cap \mathcal{R}_p = \emptyset$, or $X_p = 0$ otherwise. According to Proposition 3, $\text{Prob}(X_p = 1)$ should be $\sqrt{\pi/(2p)} \cdot (1 + o(1))$. To test this prediction, Fig. 4 compares

$$S(N) := \sum_{p<N} X_p$$

with its expected value $\sum_{p<N} \sqrt{\pi/(2p)}$. For the first 5,000 primes p we estimated $\text{Prob}(X_p = 1)$ by taking a collection of 50 different polynomial maps of degree two, and for each p we computed the proportion of maps for which $\mathcal{C}_p \cap \mathcal{R}_p = \emptyset$. Once

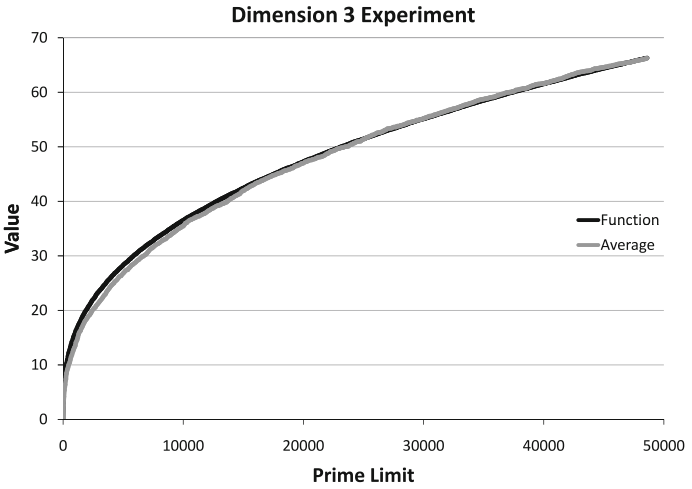

Fig. 4 $S(N)$ compared to $\sum_{p<N} \sqrt{\pi/(2p)}$

again, as Fig. 4 shows, the data agrees very closely with the predictions of the random map model.

6 Further questions

It is natural to ask whether Theorem 5 is true if we remove the restriction that at most one element of $\bigcup_{i=1}^{g} \mathcal{A}_i$ is not φ_i-preperiodic. Unfortunately, our method does not extend even to the case that $g = 1$ and $\mathcal{A}_1 = \{\alpha_1, \alpha_2\}$ if neither α_1 nor α_2 is φ_1-preperiodic. Indeed, the proof of Theorem 5 uses [4, Lemma 4.3], which relies on Roth's theorem and [19], and it is not at all clear how to extend those methods to the case of more than one wandering point.

Here is one particularly simple question that we have been unable to treat with our methods.

Question 1 Let K be a number field, let $\varphi : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ be a rational map of degree at least 2, and let $\gamma_1, \gamma_2 \in \mathbb{P}^1(K)$ be nonperiodic for φ. Are there infinitely primes $\mathfrak{p}$ of K such that neither γ_1 nor γ_2 is periodic modulo $\mathfrak{p}$? Is the density of such primes positive?

The answer to Question 1 is trivially "yes" if both γ_1 and γ_2 are preperiodic. In addition, Theorem 5 also gives a positive answer if only one of the points is preperiodic, or if $\phi^m(\gamma_1) = \gamma_2$ for some $m \geq 0$. Other than these special arrangements, however, we know of very few cases in which we can answer Question 1. One such case, again with a positive answer, is the case that $\gamma_1 = 0$ and $\varphi(x) = x^2 + c$, where c an integer other than 0 or -1. The proof is like that of Theorem 9: since the intersection of a set of positive density with a set of density 1 has positive density, the result follows by combining Theorem 5 with the results of [13].

In a different direction, one might also ask for a higher-dimensional version of Theorem 5 involving points rather than hypersurfaces.

Question 2 Let K be a number field, let $N > 1$, let $\Phi : \mathbb{P}^N_K \longrightarrow \mathbb{P}^N_K$ be a morphism of degree at least 2, and let $\gamma_1, \gamma_2 \in \mathbb{P}^N(K)$. Suppose that there is no $m \geq 0$ such that $\Phi^m(\gamma_1) = \gamma_2$. Are there infinitely many primes $\mathfrak{p}$ of K such that $\Phi^m(\gamma_1) \not\equiv \gamma_2 \pmod{\mathfrak{p}}$ for all m? Is the density of such primes positive?

In contrast to the case of orbits intersecting hypersurfaces as in Sect. 5, it appears to be *less* likely that the orbit of a point passes through another point modulo a prime in higher dimensions than in dimension 1. Indeed, the same orbit length heuristics suggest that at a given prime p of $\mathbb{Q}$, there is a $\frac{1}{p^{N/2}}$ chance that the orbit of γ_1 meets γ_2 modulo p. Because $\prod_p (1 - \frac{1}{p^{N/2}}) > 0$ for $N \geq 3$, the reasoning of Sect. 5 would suggest that there is a positive chance that in fact $\Phi^m(\gamma_1) \not\equiv \gamma_2 \pmod{p}$ for all m and all primes p.

It is not difficult to construct explicit examples where this happens if the orbit of γ_1 lies on a proper preperiodic subvariety of $\mathbb{P}^N$ that does not contain γ_2; it would be interesting to find examples where this happens when γ_1 has a Zariski dense forward orbit. Note also that Question 2 has a negative answer if Φ is not a morphism, or if it is a morphism of degree one.

By a result of Fakhruddin [6], a positive answer to Question 2 for maps $\Phi : \mathbb{P}^N_K \longrightarrow \mathbb{P}^N_K$ would give a positive answer for any polarizable self-map $f : X \longrightarrow X$ of projective varieties. (A map $f : X \longrightarrow X$ is said to be *polarizable* if there is an ample divisor L such that $f^*L \cong L^{\otimes d}$ for some $d > 1$; see [22].) In particular, one would have a reasonable dynamical generalization of [16]. However, proving that Question 2 has a positive answer may require new techniques. It is not clear to us how to modify the arguments in this paper to treat this higher-dimensional problem.

Acknowledgments R.B. gratefully acknowledges the support of NSF Grant DMS-0901494. D.G. was partially supported by NSERC. P.K. was supported in part by grants from the Göran Gustafsson Foundation, the Knut and Alice Wallenberg foundation, and the Swedish Research Council. T.S. was partially supported by NSF grants DMS-0854998 and DMS-1001550. T.T. was partially supported by NSF grants DMS-0801072 and DMS-0854839. Our computations in Sect. 5 were done with CPU time provided by the Research Computing Cluster at the CUNY Graduate Center. The authors thank the referee for his comments, thank Rafe Jones, Adam Towsley, and Michael Zieve for helpful conversations, and also thank the Centro di Ricerca Matematica Ennio De Giorgi for its hospitality in the summer of 2009 when this project was started.

References

1. Akbary, A., Ghioca, D.: Periods of orbits modulo primes. J. Number Theory **129**(11), 2831–2842 (2009)
2. Abramowitz, M., Stegun, I.A. (eds.): Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Dover Publications Inc., New York (1992). Reprint of the 1972 edition
3. Bach, E.: Toward a theory of Pollard's rho method. Inform. Comput. **90**(2), 139–155 (1991)
4. Benedetto, R.L., Ghioca, D., Kurlberg, P., Tucker, T.J.: A case of the dynamical Mordell–Lang conjecture, with an Appendix by U. Zannier. Math. Ann. (2011, in press)
5. Bell, J.P., Ghioca, D., Tucker, T.J.: The dynamical Mordell–Lang problem for étale maps. Am. J. Math. **132**(6), 1655–1675 (2010)
6. Fakhruddin, N.: Questions on self maps of algebraic varieties. J. Ramanujan Math. Soc. **18**(2), 109–122 (2003)

7. Faber, X.W.C., Voloch, J.F.: On the number of places of convergence of Newton's method over number fields. J. Théor. Nombres Bordeaux (2011, in press)
8. Ghioca, D., Tucker, T.J.: Periodic points, linearizing maps, and the dynamical Mordell–Lang problem. J. Number Theory **129**(6), 1392–1403 (2009)
9. Guralnick, R.M., Tucker, T.J., Zieve, M.E.: Exceptional covers and bijections on rational points. Int. Math. Res. Notes IMRN no. 1 (2007). art. ID rnm004, 20
10. Ghioca, D., Tucker, T.J., Zieve, M.E.: Intersections of polynomial orbits, and a dynamical Mordell–Lang conjecture. Invent. Math. **171**(2), 463–483 (2008)
11. Ghioca, D., Tucker, T.J., Zieve, M.E.: Linear relations between polynomial orbits (2011, submitted). arXiv:0807.3576
12. Ghioca, D., Tucker, T.J., Zieve, M.E.: The Mordell–Lang question for endomorphisms of semiabelian varieties. J. de Théor. Nombres Bordeaux (2011, in press)
13. Jones, R.: The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc. (2) **78**(2), 523–544 (2008)
14. Morton, P., Silverman, J.H.: Rational periodic points of rational functions. Internat. Math. Res. Notices **2**, 97–110 (1994)
15. Odoni, R.W.K.: The Galois theory of iterates and composites of polynomials. Proc. Lond. Math. Soc. (3) **51**(3), 385–414 (1985)
16. Pink, R.: On the order of the reduction of a point on an abelian variety. Math. Ann. **330**(2), 275–291 (2004)
17. Pollard, J.M.: A Monte Carlo method for factorization. Nordisk Tidskr. Informationsbehandling (BIT) **15**(3), 331–334 (1975)
18. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. Springer, New York (1986)
19. Silverman, J.H.: Integer points, Diophantine approximation, and iteration of rational maps. Duke Math. J. **71**(3), 793–829 (1993)
20. Silverman, J.H.: Variation of periods modulo p in arithmetic dynamics. NY J. Math. **14**, 601–616 (2008)
21. Stevenhagen, P., Lenstra, H.W. Jr.: Chebotarëv and his density theorem. Math. Intell. **18**(2), 26–37 (1996)
22. Zhang, S.: Distributions in Algebraic Dynamics. Survey in Differential Geometry, vol. 10, pp. 381–430. International Press, Somerville (2006)