# GRAND ORBITS OF INTEGER POLYNOMIALS

ARIEL SHNIDMAN AND MICHAEL E. ZIEVE

ABSTRACT. Let $K$ be a number field and set $R = \mathcal{O}_K$, the ring of integers in $K$. We determine all polynomials $f \in R[X]$ and all $\alpha \in R$ for which the grand orbit $\{\beta \in \overline{K} : f^n(\beta) = f^m(\alpha) \text{ for some } n, m \geq 0\}$ contains infinitely many elements of $R$ which are not in the forward orbit $\{f^n(\alpha) : n \geq 0\}$.

## 1. INTRODUCTION

Let $\phi : S \to S$ be a function from a set $S$ to itself. Two fundamental objects in dynamical systems are the forward and backwards orbit of an element $\alpha \in S$ under the map $\phi$, namely

$$\mathcal{O}_\phi^+(\alpha) := \{\phi^n(\alpha) : n \geq 0\} \quad \text{and}$$
$$\mathcal{O}_\phi^-(\alpha) := \{\beta \in S : \phi^n(\beta) = \alpha \text{ for some } n \geq 0\}.$$

These are joined together in the two-sided orbit

$$\mathcal{O}_\phi^\pm(\alpha) := \mathcal{O}_\phi^+(\alpha) \cup \mathcal{O}_\phi^-(\alpha).$$

The *grand orbit* of $\alpha$ is defined to be

$$\mathcal{GO}_\phi(\alpha) := \cup_{\beta \in \mathcal{O}_\phi^+(\alpha)} \mathcal{O}_\phi^-(\beta),$$

the set of all forward and backward images of any iterate of $\alpha$. In other words, $\mathcal{GO}_\phi(\alpha)$ is the connected component of the directed graph underlying the dynamical system $S$. In particular, the set of grand orbits comprises the equivalence classes under a natural dynamical equivalence relation (the same is not generally true of the set of all orbits of any of the other three types).

Intuitively, one might expect $\mathcal{O}_\phi^\pm(\alpha)$ to be much larger than $\mathcal{O}_\phi^+(\alpha)$ in general, since $\phi$ can be a many-to-one map. For the same reason, we

*Date*: July 30, 2010.

The authors thank Joe Silverman, Bjorn Poonen, and other participants of the 2010 Arizona Winter School for discussions which led us to pose the questions treated in this paper. The authors especially thank Bjorn Poonen for allowing us to include his proof of Proposition 2.3. The authors thank Brandon Seward for a stimulating collaboration resulting in the Appendix. The first author was partially supported by NSF grant DMS-0943832. The second author was partially supported by NSF grant DMS-0903420.

expect $\mathcal{GO}_\phi(\alpha)$ to be very much larger than $\mathcal{O}_\phi^\pm(\alpha)$. These intuitions can be formalized as rigorous theorems in the classical situation where $S$ is the Riemann sphere and $\phi$ is induced by a rational function of degree at least two [7].

We shall study the relationship between these various orbits in an arithmetic setting. Namely, $S$ will be the ring of integers $R = \mathcal{O}_K$ of a number field $K$, and $\phi$ will be the map $\beta \mapsto f(\beta)$ induced by a polynomial $f(X) \in R[X]$, $\deg(f) > 1$. In this situation, we find the opposite behavior to what occurs classically: grand orbits are typically not much larger than forward orbits. For most polynomials $f$, we show that the grand orbit of any element $\alpha \in R$ contains only finitely many elements outside the forward orbit. In this case, we say that the triple $(R, f, \alpha)$ has *finite branching*; otherwise $(R, f, \alpha)$ has *infinite branching*. We say that $(R, f)$ has finite branching if $(R, f, \alpha)$ has finite branching for every $\alpha \in R$. Our main result is a classification of the triples $(R, f, \alpha)$ which have infinite branching.

One can generate examples of triples $(R, f, \alpha)$ with infinite branching by choosing $f$ to be very structured. For example, suppose $G/R$ is a one dimensional algebraic group which can be identified with a dense subset of $\mathbb{P}^1$ via $\phi : G \hookrightarrow \mathbb{P}^1$. Any (affine) endomorphism $\tilde{f} : G \to G$ can be thought of as a rational map $f : \mathbb{P}^1 \to \mathbb{P}^1$. As long as $f(R) \subset R$, and as long as there are non-trivial points of $\ker \tilde{f}$ defined over $R$, then for any non-preperiodic $\alpha \in R$, the triple $(R, f, \alpha)$ has infinite branching. Moreover, if $f, g \in R[x]$ are two polynomials induced from $\tilde{f}, \tilde{g} : G \to G$, and if $\ker \tilde{f} \cap \ker \tilde{g}$ is non-trivial (over $R$), then $\tilde{f} + \tilde{g}$ also admits triples with infinite branching.

More generally, suppose $\Gamma$ is a finite subgroup of $\mathrm{Aut}(G)$ such that there is an inclusion $\phi : G/\Gamma \hookrightarrow \mathbb{P}^1$ and a commutative diagram:

$$\begin{array}{ccc} G & \xrightarrow{\tilde{f}} & G \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ G/\Gamma & & G/\Gamma \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ \mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1 \end{array}$$

Maps $f : \mathbb{P}^1 \to \mathbb{P}^1$ that arise in this way are called *dynamically affine* [9]. As before, a polynomial $f$ that arises in this way is likely to admit triples with infinite branching (assuming $\ker \tilde{f}$ is non-trivial over $R$).

A key difference, however, is that if $f$ and $g$ are two such maps and $(R, f, \alpha)$ and $(R, g, \alpha)$ have infinite branching, then it is not automatic that $(R, f+g, \alpha)$ has infinite branching even if $\ker \tilde{f} \cap \ker \tilde{g}$ is non-trivial. In fact, we will see that this is generally not the case.

Over an algebraic closure, $G$ is either $\mathbb{G}_a$, $\mathbb{G}_m$ or an elliptic curve. In the first case, $f$ is necessarily linear, so we get no interesting examples. Elliptic curves are also of no use, because any map $\mathbb{P}^1 \to \mathbb{P}^1$ induced by an endomorphism of an elliptic curve (a Latté map) is not polynomial. Thus, we might as well let $G$ be $\mathbb{G}_m$. The affine morphisms $z \mapsto az^n$ $(n \geq 2)$ on $\mathbb{G}_m$ give rise to power maps, which will have infinite branching as long as $1 \neq \zeta_n \in R$, for some $n$th root of unity $\zeta_n$. Similarly, any function of $x^d$ admits infinite branching, assuming $\zeta_n \in R$. The only non-trivial automorphism of $\mathbb{G}_m$ is $z \mapsto z^{-1}$, so the dynamically affine polynomials corresponding to $\mathbb{G}_m$ and the group $\Gamma = \mathrm{Aut}(\mathbb{G}_m)$ are the Chebychev polynomials $T_n \in \mathbb{Z}[x]$ defined by the equation

$$T_n(X + X^{-1}) = X^n + X^{-n}.$$

From the functional equation for $T_n$, we see that if $\zeta_n \in R$ and $z$ is a non-torsion unit in $R$, then $(R, T_n, z + 1/z)$ has infinite branching. While $T_n + T_m$ won't in general admit infinite branching, any conjugate of $T_n$ by a linear function in $\overline{K}[x]$ (i.e. a *twist* of $T_n$), will admit infinite branching, given the appropriate conditions on $R$.

Since these examples exhaust all maps induced from one-dimensional algebraic groups, it is natural to wonder if there are any other examples. It follows from our main result that these are indeed the only examples.

**Theorem 1.1.** *Let $K$ be a number field and let $R$ be the ring of integers in $K$. If $f \in R[x]$ and $(R, f)$ has infinite branching, then either $f$ is (up to translation) a polynomial in $x^d$ for some $d > 1$ or $f$ is a twist of $T_n$ for some $n > 1$.*

More specifically, we prove the following theorem which classifies integral polynomials $f$ which have grand orbits with infinite branching. Our main result is even stronger in that it classifies the triples $(R, f, \alpha)$ that gives rise to grand orbits with infinite branching; see Theorem 3.3.

**Theorem 1.2.** *Let $K$ be a number field with ring of integers $R$ and suppose $f(X) \in R[X]$ has degree $n > 1$. Let $\phi : R \to R$ be the map $\beta \mapsto f(\beta)$. Then there exists an $\alpha \in R$ such that $\mathcal{GO}_\phi(\alpha) \setminus \mathcal{O}_\phi^+(\alpha)$ is infinite if and only if either*

(1) *$f(X) = f(\zeta X + c)$ for some $c \in R$ and some root of unity $\zeta$ in $K$; or*

(2) $f = \ell \circ \pm T_n \circ \ell^{-1}$, *where* $\ell(X) = aX + b$ *with* $a^2, b \in K$ *and* $\ell^{-1}(X) = (X - b)/a$. *Moreover, there is an* $n$*-th root of unity* $\zeta \neq 1$ *in* $K$ *and the unit group* $R^\times$ *is infinite; or*
(3) $f = \ell \circ \pm T_n \circ \ell^{-1}$, *where* $\ell(X) = aX + b$ *with* $a^2, b \in K$. *Moreover, there is an* $n$*-th root of unity* $\zeta \neq 1$ *in* $\overline{K}$ *such that* $\zeta + \zeta^{-1} \in K$ *and* $K$ *is not totally real.*

The functional equation in the first case implies that $f$ is, up to translation, a function of $X^d$ for some $d|n$. Notice that when $K$ is totally real, $f$ is necessarily of the first type because $T_2$ is an even function. In the appendix, we give an elementary proof of this fact.

As stated, this theorem only applies to rings of integers, but this is mainly to keep the statement clean. For instance, Theorem 1.1 is true for the ring of $S$-integers of $K$, for any finite set $S$ of primes in $K$. Using the same method of proof, one obtains a slightly weaker analog of Theorem 1.2 for any finitely generated, commutative integral domain of characteristic zero. Although we won't state the general result, we will occasionally mention references needed to handle the case where $R$ is transcendental over $\mathbb{Z}$.

This result contributes to the rapidly advancing subject of arithmetic dynamical systems [9]. In particular, motivated by the well-established topic of arithmetic geometry, we are examining the interplay between arithmetic and dynamical structures.

Our proof begins with a height argument which shows that each backwards orbit contains only finitely many elements of $R$; in case $R$ is contained in $\overline{\mathbb{Q}}$ we can use the usual canonical height associated to $\phi$, but for more general $R$ we need a variant of Moriwaki's arithmetic height functions [8]. Thus, it suffices to classify the $f \in R[X]$ and $\alpha \in R$ for which $\mathcal{O}_\phi^+(\alpha)$ contains infinitely many elements that are $f$-images of an element of $R$ outside this orbit; in other words, $(f(X) - f(Y))/(X - Y)$ has infinitely many zeroes in $R \times \mathcal{O}_\phi^+(\alpha)$. By Siegel's theorem (as generalized by Lang), this hypothesis implies that $(f(X) - f(f(Y)))/(X - f(Y))$ has an irreducible factor in $K[X, Y]$ which is absolutely irreducible (i.e., irreducible over the algebraic closure $\overline{K}$ of $K$) and defines a curve of genus zero which has at most two places at infinity. We classify the polynomials $f$ with these properties.

Questions akin to ours have been studied previously. Avanzi and Zannier [1] determined the complex polynomials $f(X)$ for which $(f(X) - f(Y))/(X - Y)$ has an irreducible factor defining a genus-zero curve. Bilu [2] determined the polynomials $f, g$ over a field $K$ of characteristic zero for which $f(X) - g(Y)$ has a factor of degree at most 2; this result was generalized to arbitrary characteristic by Kulkarni, Müller

and Sury [6]. Bilu and Tichy [3, Thm. 9.3] describe the polynomials $f, g \in \mathbb{Q}[X]$ for which $f(X) = g(Y)$ has infinitely many rational solutions having bounded denominator (they also generalized this result to polynomials defined over a number field). Finally, Ghioca, Tucker and Zieve [4, 5] determined the complex polynomials $f, g$ such that $\mathcal{O}_f^+(\alpha) \cap \mathcal{O}_g^+(\alpha)$ is infinite for some $\alpha \in \mathbb{C}$; the present paper makes progress towards treating infinite intersections of grand orbits. It should be emphasized that these problems have a long history, and the papers mentioned above build on previous work of Cassels, Davenport, Feit, Fried, Lewis, Schinzel, Tverberg, and many others.

As far as we can tell, our results do not follow from the work of Bilu and Tichy cited earlier. One might use the results of [3] to obtain a classification of polynomials $f \in R[X]$ with the property that $f(X) - f(Y)/(X - Y)$ has infinitely many solutions in $R \times R$. But there are pairs $(R, f)$ with this property which do not have infinite branching. For example, take any $R$ which contains a third root of unity and a non-torsion unit, and take $f(x) = T_3(x) + T_{15}(x)$. Since

$$f(x + 1/x) = x^3 + x^{15} + 1/x^3 + 1/x^{15},$$

the map $f : R \to R$ is non-injective at infinitely many points in $R$. But $f$ is not linearly conjugate to any $T_n$, so by our result, $(R, f)$ has finite branching. The results of [3] narrow down the possible pairs $(R, f)$ with infinite branching, but not enough to obtain a complete classification. In any case, the proof in the present paper is much simpler than the proofs of the more general results in the papers quoted above.

In the Appendix (written jointly with Brandon Seward), we give an alternate proof of Theorem 1.2 for totally real $R$, which does not rely on Siegel's theorem. This approach is based on a elementary new method for effectively determining integral points on varieties, which we will develop in full generality in a subsequent paper.

In the next section we review the relevant facts about height functions, and give some applications. We prove Theorems 3.3 and 1.2 in Section 3, before concluding with the Appendix mentioned above.

## 2. Heights

The properties of height functions allow us to deduce basic structural properties of $f$-orbits in $R$. The following lemmas show that backwards orbits over $R$ are always finite.

**Lemma 2.1.** *Let $f \in \overline{\mathbb{Q}}(x)$ be of degree $n > 1$ and $\alpha \in \overline{\mathbb{Q}}$. Then the backwards orbit of $\alpha$ with respect to $f$ contains only finitely many elements $b$ with $[\mathbb{Q}(b) : \mathbb{Q}] < N$ for any fixed $N$.*

*Proof.* This follows from the theory of height functions [9]. Associated to $f$ is a canonical height function $h_f : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$ which satisfies

(1) $h_f(\alpha) = h(\alpha) + O(1)$
(2) $h_f(f(\alpha)) = nh_f(\alpha)$

for all $\alpha \in \overline{\mathbb{Q}}$. Here, $h$ is the usual (logarithmic) height function on $\overline{\mathbb{Q}}$ [9]. Since $h$ has the property that there are only finitely many $b \in \overline{\mathbb{Q}}$ with bounded degree (over $\mathbb{Q}$) and bounded height, (1) implies that $h_f$ has this property as well. Hence, (2) implies there are finitely many $b$ in the backwards orbit of $\alpha$. □

A result of Moriwaki allows us to extend this result to more general fields.

**Lemma 2.2.** *The previous lemma holds if we replace $\mathbb{Q}$ with a field $K$ of finite transcendence degree over $\mathbb{Q}$.*

*Proof.* We can mimic the proof of the previous lemma as long as there exists a height function $h$ on $\overline{K}$ which satisfies:

(1) $h$ admits only finitely many elements of bounded height and bounded degree over $K$
(2) $h(\alpha) = nh(\alpha) + O(1)$ for all $\alpha \in \overline{K}$.

Moriwaki has constructed such height functions [8]. □

Height functions also allow for a simple proof that there are infinitely many grand orbits in $R$ under $f$.

**Proposition 2.3** (Poonen)**.** *Let $R$ be a finitely generated ring of characteristic zero. If $f \in R[x]$ is a polynomial of degree $d > 1$, then there are infinitely many grand orbits (in $R$) under $f$.*

*Proof.* Let $h_f(x)$ be the canonical logarithmic height associated to $f$. Then we have $h_f(f(x)) = dh_f(x)$. Notice that

$$\frac{\log h_f(f(x))}{\log d} - \frac{\log h_f(x)}{\log d} = 1$$

for all $x$. Thus the quantity $\frac{\log h_f(x)}{\log d} \in \mathbb{R}/\mathbb{Z}$ is constant on any grand orbit. On the other hand, for $x \in \mathbb{Z}$, $h_f(x) = \log|x| + O(1)$ so that the image of

$$\frac{\log h_f(x)}{\log d} = \log\log|x| + o(1)$$

in $\mathbb{R}/\mathbb{Z}$ as $x$ ranges over $\mathbb{Z}$ is dense. Hence there must be infinitely many grand orbits. □

## 3. Proofs of main results

Our proof of Theorem 3.3 uses the following generalization of Siegel's finiteness result for integral points on affine curves [Lang].

**Theorem 3.1.** *Let $F$ be a field finitely generated over $\mathbb{Q}$ and let $R$ be a subring finitely generated over $\mathbb{Z}$. Let $V$ be an affine curve defined over $F$ and let $X$ be its projective normalization. If the genus of $X$ is positive or if there are at least three points in the complement of $V$ in $X$, then every set of $R$-integral points on $V$ is finite.*

We will apply Siegel's theorem to curves defined by absolutely irreducible factors of $(f(X) - f(Y))/(X - Y)$. It is simple to check that the number of points at infinity on such curves is equal to the degree of the factor. Furthermore, each point at infinity is non-singular. The theorem then implies that only linear or quadratic factors can have infinitely many integral points.

**Lemma 3.2.** *Let $L/K$ be a quadratic extension of number fields. Then the norm map $U(L) \to U(K)$ has finite kernel if and only if $K$ is totally real and $L$ is totally imaginary, i.e. $L/K$ is a CM extension.*

*Proof.* By Hilbert 90, every norm 1 element of $L$ is of the form $x/x^\sigma$, where $\sigma$ generates $\mathrm{Gal}(L/K)$. Thus, the kernel of the norm map $L^\times \to K^\times$ is isomorphic to $L^\times/K^\times$. If the rank of $U(L)$ is larger than that of $U(K)$, then $U(L)/U(K)$ is an infinite subgroup of $L^\times/K^\times$, which corresponds to units of norm 1. Since $U(L)$ and $U(K)$ have the same rank if and only if $L/K$ is CM, this implies one direction. Conversely, if $L/K$ is CM, then since complex conjugation commutes with every embedding of $L$, every unit of norm 1 (which we may write as $x/x^\sigma$), has absolute value 1 in every complex embedding. Thus, $x/x^\sigma$ is a root of unity and there are finitely many units of norm 1. □

Theorem 1.2 follows from the following more specific result together with the previous lemma.

**Theorem 3.3.** *Let $K$ be a number field with ring of integers $R$ and suppose $f(X) \in R[X]$ has degree $n > 1$. Let $\phi : R \to R$ be the map $\beta \mapsto f(\beta)$, and suppose $\alpha \in R$ is not pre-periodic under $\phi$. Then $\mathcal{GO}_\phi(\alpha) \setminus \mathcal{O}^+_\phi(\alpha)$ is infinite if and only if either*

1. *$f(X) = f(\zeta X + c)$ for some $c \in R$ and some root of unity $\zeta$ in $K$; or*
2. *$f = \ell \circ \pm T_n \circ \ell^{-1}$, where $\ell(X) = aX + b$ with $a^2, b \in K$ and $\ell^{-1}(X) = (X - b)/a$. Moreover, there is an $n$-th root of unity $\zeta \neq 1$ in $K$ and an element $\alpha' \in \mathcal{GO}_\phi(\alpha)$ such that $\alpha' = a(z/a+$*

*$a/z)+b$ for some $z \in K$ such that $z^2/a^2$ is a non-torsion unit in $R$; or*

(3) *$f = \ell \circ \pm T_n \circ \ell^{-1}$, where $\ell(X) = aX+b$ with $a^2, b \in K$. Moreover, there is an $n$-th root of unity $\zeta \neq 1$ in $\overline{K}$ such that $\zeta + \zeta^{-1} \in K$ and and element $\alpha' \in \mathcal{GO}_\phi(\alpha)$ such that $\alpha' = a(z/a + a/z) + b$ for some $z \in L = K(\zeta)$ such that $z^2/a^2$ is a non-torsion unit in $L$ satisfying $\mathrm{Nm}_{L/K}(z^2/a^2) = 1$.*

*Proof.* The hypotheses and Lemma 2.2 guarantee that

$$F(x,z) = \frac{f(x) - f(z)}{x - z} \in R[x]$$

has infinitely many solutions in $R \times f(\alpha)$. By Siegel's theorem, this polynomial must have an irreducible factor (with coefficients in $K$) of genus 0 with at most two points at infinity. Homogenizing with the variable $Y$ and setting $Y = 0$ shows that the number of points at infinity for such factors is exactly the degree. So we may assume that $F(x,z)$ has a linear or quadratic factor with infinitely many solutions in $R \times f(\alpha)$.

First suppose that $F(x,z)$ has a linear factor. This factor is necessarily of the form $(x - \zeta^{-1}z + b)$, where $1 \neq \zeta \in \mu_n$, $n = \deg(f)$ and $b \in K$. Since this factor has infinitely many $R$-solutions, its coefficients are in $K$, hence $\zeta \in K$. Since $R$ is integrally closed, we even have $\zeta \in R$, and hence $b \in R$ as well. We have $f(x) = f(\zeta x + c)$, where $c = b\zeta$. Polynomials satisfying this type of functional equation are polynomials in $x^d$ (where $d$ is the order of $\zeta$ in $\mu_n$) precomposed with a translation. Indeed, if $g(x) = f(x - \frac{c}{\zeta - 1})$, then $g(x) = g(\zeta x)$, and such a polynomial is clearly in $\mathbb{C}[x^d]$.

Next suppose that $F(x,z)$ has an irreducible quadratic factor

$$g(x,z) = x^2 + a(z)x + b(z),$$

where $a, b \in K[z]$ with $\deg(a) = 1$ and $\deg(b) = 2$. By setting $z = f(y)$, we see that $h(x,y) = x^2 + a(f(y))x + b(f(y))$ divides the polynomial

$$F_0(x,y) = \frac{f(x) - f^2(y)}{x - f(y)}.$$

First suppose that $h(x,y)$ is irreducible. Let $G$ be the curve corresponding to $g(x,z)$ and $H$ the curve corresponding to $h(x,y)$. Our assumption on the orbit of $\alpha$ guarantees that both $G$ and $H$ have infinitely many $R$-points. Siegel's theorem then implies that both have genus zero, i.e. they are isomorphic to $\mathbb{P}^1$. Consider the map $H \to G$ given by $f^* : (x,y) \mapsto (x, f(y))$. We have the following commutative

diagram:

$$\begin{array}{ccc} H & \longrightarrow & \mathbb{P}^1_y \\ {\scriptstyle f^*}\downarrow & & \downarrow{\scriptstyle f} \\ G & \longrightarrow & \mathbb{P}^1_z \end{array}$$

We choose a coordinate $u$ on $H$ so that the two points at infinity are at $u = 0$ and $u = \infty$. We pick an analogous coordinate, $v$, for the curve $G$ and we may assume that $u = 0$ is the unique preimage of $v = 0$ and similarly for infinity. Since $v = 0, \infty$ are both totally ramified under the map $f^*$, we find that $v = au^n$ where $n$ is the degree of $f$ and $a \in K$. Now $K(z)$ is a degree two extension of $K(v)$ with poles at 0 and infinity, so $z = bv + c + \frac{d}{v}$ for some $b, c, d \in K$. Similarly, $y = ru + s + \frac{t}{u}$ for some $r, s, t \in K$. Thus, $f$ satisfies

$$f\left(ru + s + \frac{t}{u}\right) = bau^n + c + \frac{d}{au^n}.$$

Applying translations, we may assume that $f$ satisfies $f(ru + t/u) = Cu^n + D/u^n$ for some $C, D \in K$. Then pre-composing with $x \mapsto x\sqrt{rt}$ (and post-composing with a similar map as well), we may assume that $f(au + 1/au) = bu^n + 1/bu^n$, where $a$ and $b$ may now lie in a quadratic extension of $K$. Since this holds for all $u$, we find that $f(du + 1/du) = u^n + u^{-n}$ for some $d$. But comparing high degree coefficients (in both $u$ and $u^{-1}$), we find that $d^n = \pm 1$. Thus, replacing $u$ with $u/d$, we conclude $f(u + 1/u) = \pm(u^n + u^{-n})$. This is the defining property of the Chebychev polynomials $\pm T_n$.

Thus, $f = l_1 \circ T_n \circ l_2$ for linears $l_1, l_2$ with coefficients in a quadratic extension of $K$. Mimicking our argument above, we can construct a curve which maps to $H$, and we find that $f \circ f = l_3 \circ T_{n^2} \circ l_4$ for linears $l_3, l_4$. Thus

$$T_{n^2} = l_3^{-1} \circ l_1 \circ T_n \circ l_2 \circ l_1 \circ T_n \circ l_2 \circ l_4^{-1}.$$

For any $m$, the maps $T_m$ are totally ramified at $\infty$ and otherwise only ramify at $\pm 2$. More precisely, each point in the preimage of $\pm 2$ has ramification index equal to 2, aside from the fixed points $\pm 2$ which have ramification index equal to 1. A simple ramification argument shows that $l_2 \circ l_4^{-1}$ must send the set $\{\pm 2\}$ to itself and similarly $l_2 \circ l_1$ fixes $\{\pm 2\}$. We conclude that $l_2 \circ l_1 = \pm x$, hence $f = l_1 \circ \pm T_n \circ l_1^{-1}$, i.e., $f$ is linearly conjugate to $\pm T_n$. If $l_1 = ax + b$, then a quick check of the coefficients shows that $a^2, b \in K$. In this case, we may assume $n$

is odd because $T_n(x) - T_n(y)$ has linear factors for even $n$. For odd $n$, the quadratic factors of $\frac{T_n(x)-T_n(y)}{x-y}$ are of the form

$$x^2 - \xi xy + y^2 + c$$

where $\xi = \zeta + \zeta^{-1}$ for some non-trivial $n$th root of unity $\zeta$ [B-Z]. Hence the quadratic factors of $\frac{f(x)-f(y)}{x-y}$ are of the form

$$\frac{1}{a^2}\left((x-b)^2 - \zeta(x-b)(y-b) + (y-b)\right) + c.$$

Since $a^2 \in K$, $\xi \in K$.

Now suppose that $\zeta \in K$. The functional equation for $f$ reads:

$$f\left(z + \frac{a^2}{z} + b\right) = a\left((z/a)^n + (a/z)^n\right) + b.$$

Write $\alpha = z + \frac{a^2}{z} + b$ for some $z$ which may only lie in a quadratic extension of $K$. We want to show that in fact $z \in K$ and that $z^2/a^2$ is a unit in $K$. By assumption, there are infinitely many positive integers $k$ such that

$$f^{(k)}(\alpha) = a\left((z/a)^{n^k} + (a/z)^{n^k}\right) + b$$

is in $R$. This shows that $z/a$ is a unit in some extension of $K$. Indeed, if it had some non-zero $w$-adic valuation for some prime $w$ lying above a prime $v$ of $K$, then clearly $f^{(k)}(\alpha)$ could not be $v$-adically integral for large $k$. Since $a^2 \in K$, it only remains to show that $z \in K$. But by replacing $\alpha$ with a forward iterate, we may assume that $\beta = \zeta z + \frac{a^2}{\zeta z} + b$ is in $K$ as well, and then the equation

$$z = \frac{a^2(\zeta - \zeta^{-1})}{(\alpha - b)\zeta - (\beta - b)}$$

shows that $z \in K$, as claimed.

Now suppose that $\xi = \zeta + \zeta^{-1} \in K$, but $\zeta \notin K$. Set $L = K(\zeta)$, and let $\mathrm{Gal}(L/K)$ be generated by $\sigma$. We choose $z$ as before, and by replacing $\alpha$ with a forward iterate, we may again assume that $\beta$ (as defined above) is in $K$. The above formula for $z$ shows that $z \in L$. We have $\sigma(z) = a^2/z$, by the very definition of $z$. Arguing as before, we find that $z^2/a^2$ is a (non-torsion) unit in $L$, and we also compute $\mathrm{Nm}_{L/K}(z^2/a^2) = 1$.

Lastly, we need to consider the case where $h(x, y)$ factors into a product of two polynomials linear in $x$. Then $G(x, y)$ must have a factor of the form $x - q(y)$ for some polynomial $q(y) \neq f(y)$ in $K[y]$. In other words, $f \circ q = f \circ f$. But this implies that $q = u \circ f$ for some (non-trivial) linear polynomial $u$ such that $f \circ u = f$. By the same

argument as before, we conclude that $f(x)$ is a function of $x^n \circ l(x)$ for some linear function $l(x)$.

The converse statements in the theorem all follow immediately from the functional equations for $f$. For instance, if $\zeta \in K$ is an $n$th root of unity and if $\alpha = z + 1/z$ for some non-torsion $z \in U(K)$, then the grand orbit minus the forward orbit of $\alpha$ under $T_n$ is infinite because it contains $\zeta z^{n^k} + 1/(\zeta z^{n^k})$ for each $k \geq 1$. The general cases (i.e. when $\ell(x) \neq x$ or when $\zeta \notin K$) work the same way. □

*Remark* 3.4. As it may be useful, we give precise conditions on the linear polynomial $\ell(x) = ax + b$ which guarantee that $f = \ell \circ T_n \circ \ell^{-1}$ lies in $R[x]$. If we let $A = 1/a$ and $B = -b/a$ (so $\ell^{-1}(x) = Ax + B$), then $f \in R[x]$ if and only if $A^2, B^2, AB$ and $A^{-1}(T_n(B) - B)$ all lie in $R$.

*Remark* 3.5. If $f \in R[x]$ is not of either type mentioned in Theorem 3.3 and also not a composition of a Chebychev by linears, then the proof implies that the curve

$$\frac{f(x) - f(f(y))}{x - f(y)}$$

has finitely points. Thus, all but finitely many grand orbits of $f$ are one-sided infinite rays (when viewed as a graph) except for some possible branching at the second vertex. Moreover, the finite number of remaining grand orbits are infinite one-sided rays after removing finitely many points.

*Example* 3.6. Let $R = \mathbb{Z}[\sqrt{-3}]$ and let $f(x) = (x+1)^3 + 1 = f(\zeta x + \zeta - 1)$, where $\zeta$ is a primitive third root of unity. Notice that $\zeta - 1 \notin R$ but if $\alpha \in \mathbb{Z}$ is odd, then $\mathcal{G}_f(\alpha) - \mathcal{O}_\phi^+(\alpha)$ is infinite. This is one example of how our main theorem (as stated) is false if one considers orders in number fields, or more generally, rings which are not integrally closed.

## Appendix: A different approach

In this Appendix, which describes joint work with Brandon Seward, we give a different proof of Theorem 1.2 for $R = \mathbb{Z}$, and discuss which rings $R$ can be treated in a similar manner.

**Proposition A.1.** *Pick $\alpha \in \mathbb{Z}$ and $f(X) \in \mathbb{Z}[X]$ of degree $n \geq 2$. Then $\mathcal{GO}_\phi(\alpha) \setminus \mathcal{O}_\phi^+(\alpha)$ contains infinitely many integers if and only if $f(X) = g(X^2 - aX)$ for some $a \in \mathbb{Z}$ and $g \in \mathbb{Z}[X]$.*

*Remark* A.2. The last condition is equivalent to asserting that $f$ satisfies $f(X) = f(-X + a)$. For, if $f \in \mathbb{Z}[X]$ satisfies this identity, then $f$ lies in the subfield of $\mathbb{Q}(X)$ fixed by the automorphism $X \mapsto -X + a$,

namely $\mathbb{Q}(X(-X+a))$. Thus $f = g(X^2 - aX)$ for some $g \in \mathbb{Q}(X)$, and since $f$ is a polynomial we must have $g \in \mathbb{Q}[X]$. By successively equating coefficients of $X^{2n}, X^{2n-2}, \ldots, X^2, X^0$ in $f$ and $g(X^2 - aX)$, we find that $g \in \mathbb{Z}[X]$.

*Proof.* Define $A := (\mathcal{G}\mathcal{O}_\phi(\alpha) \cap \mathbb{Z}) \setminus \mathcal{O}_\phi^+(\alpha)$. If $f(X) = f(-X+a)$ for some $a \in \mathbb{Z}$ then clearly $A$ is infinite. Now assume that $A$ is infinite. Viewing $f$ as a function from $\mathbb{Z}$ to itself, there are infinitely many integers with multiple (integer) preimages under $f$. We will use this information to construct an infinite set of $x_i \in \mathbb{Z}$ such that $f(x_i) = f(-x_i - a_i)$ for some $a_i \in \mathbb{Z}$ with $a_i$ bounded by some absolute constant (depending only on $f$).

Indeed, write $f(X) = b_d X^d + \cdots + b_0$ and note that $d$ must be even for the hypothesis to hold. It is easy to see that there exists a positive constant $c \in \mathbb{R}$ such that

$$b_0(x-c)^d \le f(x) \le b_0(x+c)^d$$

for positive $x$ large enough, and we get the reverse inequalities for negative $x$ with large enough absolute value. By assumption we can find infinitely many $x_i$ and $a_i$ (both integers) such that for all $i$ we have

- $f(x_i) = f(-x_i - a_i)$
- $x_i$ and $-x_i - a_i$ have opposite signs
- Both $|x_i|$ and $|-x_i - a_i|$ are greater than $c$.

The inequalities above holds for $x = x_i$ and we also have

$$b_0(-x_i - a_i - c)^d \ge f(x_i) \ge b_0(-x_i - a_i + c)^d.$$

Since $d$ is even, we can flip the signs inside the parentheses. Taking $d$th roots and combining the two inequalities yields $|a_i| \le 2c$.

Since the $a_i$ form a bounded sequence of integers, we may choose some $a_j$ such that $a_i = a_j$ for at least $d+1$ values of $i$. Then the polynomial $f(x) - f(-x - a_j)$ has at least $d+1$ roots but has degree less than $d$. Thus we must have $f(x) = f(-x - a_j)$ for all $x$, which is the desired conclusion. □

*Remark* A.3. Working one embedding at a time, the same argument shows that Proposition A.1 (and hence Theorem 1.2) is true with $R = \mathbb{Z}$ replaced by the ring of integers of any totally real number field. Aside from being more elementary than the proof which uses Siegel's theorem, this proof gives an effective way of computing bounds on the number of integral solutions to $(f(x) - f(y))/(x-y) = 0$. We will discuss generalizations of this method to other problems in a further paper.

## References


[1] R. M. Avanzi and U. M. Zannier, *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$*, Compositio Math. **139** (2003), 263–295.

[2] Y. F. Bilu, *Quadratic factors of $f(x) - g(y)$*, Acta Arith. **90** (1999), 341–355.

[3] Y. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

[4] D. Ghioca, T. J. Tucker and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math. **171** (2008), 463–483, arXiv:0705.1954v2.

[5] ———, *Linear relations between polynomial orbits*, submitted for publication, arXiv:0807.3576.

[6] M. Kulkarni, P. Müller and B. Sury, *Quadratic factors of $f(X) - g(Y)$*, Indag. Math. (N.S.) **18** (2007), 233–243.

[7] J. Milnor, Dynamics in One Complex Variable, 3rd ed., Princeton Univ. Press, Princeton, NJ, 2006.

[8] A. Moriwaki, *Arithmetic height functions over finitely generated fields*, Invent. Math. **140** (2000), 101–142.

[9] J. H. Silverman, The Arithmetic of Dymamical Systems, Springer-Verlag, New York, 2007.



Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109-1043 USA

*E-mail address*: shnidman@umich.edu

Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109-1043 USA

*E-mail address*: zieve@umich.edu

*URL*: http://www.math.lsa.umich.edu/∼zieve/