A lower bound on the orbit growth of a regular self-map of affine space

Vesselin Dimitrov
vesselin.dimitrov@yale.edu

Abstract

We show that if \( f : \mathbb{A}^r_{\overline{\mathbb{Q}}} \to \mathbb{A}^r_{\overline{\mathbb{Q}}} \) is a regular self-map and \( P \in \mathbb{A}^r(\overline{\mathbb{Q}}) \) has \( \limsup_{n \in \mathbb{N}} \frac{\log h_{\text{aff}}(f^nP)}{\log n} < 1/r \), where \( h_{\text{aff}} \) is the affine logarithmic Weil height, then \( \mathbb{N} \) partitions into a finite set and finitely many full arithmetic progressions, on each of which the coordinates of \( f^nP \) are polynomials in \( n \).

In particular, if \( (f^nP)_{n \in \mathbb{N}} \) is a Zariski-dense orbit, then either \( r = 1 \) and \( f \) is of the shape \( t \mapsto \zeta t + c, \zeta \in \mu_\infty \), or else \( \limsup_{n \in \mathbb{N}} \frac{\log h_{\text{aff}}(f^nP)}{\log n} \geq 1/r \). This inequality is the exponential improvement of the trivial lower bound obtained from counting the points of bounded height in \( \mathbb{A}^r(K) \).

1. Introduction

1.1. In the appendix to our preprint [5] we formulated a precise conjectural criterion for the algebraicity of a formal function on a projective curve over a global field. For the case of the projective line, this criterion generalizes simultaneously the classical Pólya-Bertrandias criterion (cf. Amice [1], Ch. 5), on the one hand, and a conjecture of I. Ruzsa [7, 6, 10, 4], on the other hand. In [5] (3.2 in loc. cit.) we proved a weak variant of this conjecture with the purpose of applying it to a case of a generalization of the “Hadamard quotient theorem” to higher genus and positive equicharacteristic (Theorem 1.7 in loc. cit.). In the present note we prove another weak variant, and apply it to obtain a lower bound on the growth of an orbit under a regular iteration of affine space.
1.2. We need to settle some notation before we can state our result. In what follows we denote by $h(\cdot) : \overline{\mathbb{Q}}^\times \to \mathbb{R}^{\geq 0}$ the absolute logarithmic Weil height, whose definition we recall next. For $p$ a finite rational prime let $|\cdot|_p$ by the $p$-adic absolute value on $\mathbb{Q}$ normalized by $|p|_p = 1/p$, while for $p = \infty$ we consider the ordinary (archimedean) absolute value. For $v$ a place a number field $K$ lying over the place $p$ of $\mathbb{Q}$, and for $x \in K$, let $|x|_v := |N_{K_v/\mathbb{Q}_p}(x)|_p^{1/[K: \mathbb{Q}]}$. For $x = [x_0 : x_1 : \cdots : x_r] \in \mathbb{P}^r(\mathbb{K})$ we then have

$$h(x) := \sum_v \max_j \log |x_j|_v.$$  

This definition is independent of the choice of the number field $K$. Viewing $A^r(\overline{\mathbb{Q}})$ as the affine piece $[1 : x_1 : \cdots : x_r]$ in $\mathbb{P}^r(\overline{\mathbb{Q}})$, we consider the affine height $h_{\text{aff}}(\alpha_1, \ldots, \alpha_r) := h([1 : \alpha_1 : \cdots : \alpha_r])$. Finally, we write as usual $h(\alpha) = h_{\text{aff}}(\alpha)$ for $\alpha \in \overline{\mathbb{Q}} = A^1(\overline{\mathbb{Q}})$.

For a polynomial $F \in \mathbb{K}[x]$ in several variables over $\mathbb{K}$, we write $h(F)$ for the height of its set of coefficients, viewed as a point in a projective space.

1.3. To motivate our result we make the following trivial observation. If a point $P \in \mathbb{Z}^r$ has infinite orbit under a set-theoretic mapping $f : \mathbb{Z}^r \to \mathbb{Z}^r$, then $H := \max_{0 \leq i \leq n} \exp(h(f^i P))$ satisfies $(2H + 1)^r > n$, whence, in the limit,

$$\limsup_{n \to \infty} \frac{h_{\text{aff}}(f^n P)}{\log n} \geq 1/r.$$  

The result of this note is that when the mapping $f$ has an algebraic structure, and outside of a degenerate situation, this trivial inequality can be improved exponentially.

Theorem 1.4. Consider regular maps $f : A^r_\mathbb{K} \to A^r_\mathbb{K}$ and $\lambda : A^r_\mathbb{Q} \to A^1_\mathbb{Q}$. Let $P \in A^r(\overline{\mathbb{Q}})$ be a point such that

$$\limsup_{n \to \infty} \frac{\log h(\lambda(f^n P))}{\log n} < 1/r.$$  

Then there is a $d \in \mathbb{N}$ and polynomials $p_0, \ldots, p_{d-1} \in \overline{\mathbb{Q}}[x]$ such that $\lambda(f^{nd+i} P) = p_i(n)$ for all $i = 0, \ldots, d - 1$ and $n \gg 0$.

The following is an immediate corollary, obtained by taking $\lambda$ to be the coordinate projections.
Corollary 1.5. In the setup of Theorem 1.3, either the Zariski closure of the orbit \((f^n P)_{n \in \mathbb{N}}\) is a union of rational curves in \(\mathbb{A}^r\), or else 
\[
\limsup_{n \in \mathbb{N}} \frac{\log h_{\text{aff}}(f^n P)}{\log n} \geq 1/r.
\]

Another corollary arises in taking \(f\) to be a recurrence of the form 
\[(x_1, \ldots, x_{r-1}, x_r) \mapsto (x_2, \ldots, x_r, p(x_1, \ldots, x_r))\]
and \(\lambda\) the projection onto the last coordinate.

Corollary 1.6. Consider a sequence \(A : \mathbb{N} \to \mathbb{Z}\) satisfying a finite polynomial recurrence 
\[A(n + r) = p(A(n + r - 1), \ldots, A(n)),\]
where \(p \in \mathbb{Z}[T_1, \ldots, T_r]\). Then either 
\[
\limsup_{n \in \mathbb{N}} \frac{\log \log |A(n)|}{\log n} \geq 1/r,
\]
or else there is a \(d \in \mathbb{N}\) such that each of the sequences \((A(nd + i))_{n \geq 0}, 0 \leq i < d\), is a polynomial for \(n \gg 0\).

We will derive Theorem 1.4 from a criterion for the rationality of a formal function on the projective line, which we formulate and prove in the next section. Results of this type date back to the short paper [9] by U. Zannier.

2. A rationality criterion

In what follows, \(K\) is a number field and \(S\) a finite set of places of \(K\) including all archimedean places. The following is a particular case of the conjecture formulated in the appendix to [5].

Conjecture 2.1. Consider \(F \in O_{K,S}[[t]]\) a formal power series with \(S\)-integral coefficients which has a positive radius of convergence \(R_v > 0\) at each place \(v\) of \(K\). For each prime (closed point) \(s \in \text{Spec} O_K\) let \(h_s \in \mathbb{N}_0 \cup \{\infty\}\) be \(+\infty\) if either \(s \in S\) or the reduction \(F \mod s \in k(s)[[t]]\) is not in \(k(s)(t)\); and the degree of the rational function \(F \mod s\) otherwise. If 
\[
\sum_v \log R_v + \liminf_{n \in \mathbb{N}} \left\{ \frac{1}{n} \frac{1}{[K : Q]} \sum_{s:h_s < n} \log |k(s)| \right\} > 0,
\]

(1)
then the power series \( F \in K(t) \) is rational.

This conjecture is sharp, in the sense that there are uncountably many power series \( F \) for which the quantity on the left-hand side of (1) is zero. It extends an old conjecture of I. Ruzsa [7], and appears intractable to our current techniques. In this section we prove the following crude variant.

**Proposition 2.2.** Let \( \eta > 0 \). In the setup of Conjecture 2.1, assume instead that the inequality

\[
\frac{1}{[K : \mathbb{Q}]} \sum_{s : h_s < n/(2+\eta)} \log |k(s)| > \frac{3}{2} \log n + \left( 1 + \frac{1}{\eta} \right) h(F/n) + \frac{1}{2} \log |D_{K/\mathbb{Q}}| \tag{2}
\]

holds for all \( n \gg 0 \). Then \( F \in K(t) \) is rational.

**Proof.** The proof is a variant of that presented to the algebraicity criterion 3.2 in [5]. Without loss of generality we may assume \( \eta \) to be rational. Letting \( L \) be a large integer parameter such that \( \eta L \in \mathbb{Z} \), Siegel’s lemma (see 3.1 in [5] and the references therein) for \( M := L \) equations in \( N := (1 + \eta)L \) unknowns yields polynomials \( P \in K[t] \) and \( Q \in K[t] \setminus \{0\} \) of degrees less than \( (1 + \eta)L \) such that

\[
Q(t)F(t) - P(t) \equiv 0 \mod t^{(2+\eta)L} \tag{3}
\]

and

\[
h(Q) \leq \frac{1}{2} \log N + \frac{1}{2} \log |D_{K/\mathbb{Q}}| + \frac{1}{\eta} h\left(F/(2+\eta)L\right). \tag{4}
\]

It follows from (2) and (4) that there is an \( L < \infty \) such that all \( n \geq (2 + \eta)L \) satisfy

\[
\frac{1}{[K : \mathbb{Q}]} \sum_{s : h_s < n/(2+\eta)} \log |k(s)| > \log N + h(Q) + h(F/n). \tag{5}
\]

We claim that then \( F = P/Q \), hence \( F \) is rational. Assuming otherwise, let \( n \) be the minimum integer such that \( Q(t)F(t) - P(t) \not\equiv 0 \mod t^n \); by construction, \( n > (2 + \eta)L \). Consider a prime \( s \) of \( K \) with \( h_s < n/(2+\eta) \), and write \( F_s := A_s/B_s \) the reduction at \( s \), with \( A_s, B_s \in k(s)[t] \), \( \deg A_s, \deg B_s < n/(2+\eta) \). Then, denoting by a tilde the reduction at \( s \), we have \( A_s(t)\tilde{Q}(t) - B_s(t)\tilde{P}(t) \equiv 0 \mod t^{n-1} \). The degree of this polynomial is less than \( (1 + \eta)L + n/(2 + \eta) \), which by our assumption \( n > (2 + \eta)L \) does not exceed
It follows that the polynomial is identically zero, hence the coefficients of $Q(t)F(t) - P(t)$ all reduce to zero at $s$.

On the other hand, we have assumed that $t^n$ appears with a non-zero coefficient $c \in K \setminus \{0\}$ in $Q(t)F(t) - P(t)$. (This is just the coefficient of $t^n$ in $Q(t)F(t)$.) Thus the product formula yields

$$\sum_{v} - \log |c|_v = 0. \quad (6)$$

At the places corresponding to the primes $s$ with $h_s < n/(2+\eta)$, the previous paragraph shows that the contribution to $(6)$ is at least $\frac{1}{|K:Q|} \sum_{s: \eta} \log |k(s)|$. The absolute value of the sum of the remaining contributions does not exceed $h(c)$, and $(6)$ yields the lower bound

$$h(c) \geq \frac{1}{|K:Q|} \sum_{s: h_s < n/(2+\eta)} \log |k(s)|. \quad (7)$$

To estimate $h(c)$ from above, we use the easy bound

$$h(\alpha_1 + \cdots + \alpha_r) \leq \log r + \sum_{v} \max_j \log^+ |\alpha_j|_v,$$

applied to the sum defining $c$ as the coefficient of $t^n$ in $Q(t)F(t)$. We obtain:

$$h(c) \leq \log N + h(Q) + h(F/n). \quad (8)$$

Taken together with $(7)$ this contradicts $(5)$, thus forcing $F = P/Q$ as claimed.

3. Proof of Theorem 1.4

There is a number field $K$ and a finite set $S$ of its places, including all archimedean places, such that the triple $(f, \lambda, P)$ has a model over $O_{K,S}$. We will apply Proposition 2.2 to the formal power series $\Phi := \sum_{n \geq 0} \lambda(f^n P) t^n \in O_{K,S}[[t]]$. If the power series $\Phi$ is rational, the conclusion of Theorem 1.4 follows from the explicit descriptions of coefficients of rational power series as confluent power sums. If $\Phi$ is not rational, Proposition 2.2 with $\eta := 1$ implies the lower bound inequality

$$h(\Phi/n) \geq \frac{1}{2|K:Q|} \sum_{s: h_s(\Phi) < n/3} \log |k(s)| - O(\log n) \quad (9)$$

5
for infinitely many $n \in \mathbb{N}$. On the other hand, for $s \notin S$ a prime of $K$, the iteration $f : \mathbb{A}_{O_{K,S}}^r \to \mathbb{A}_{O_{K,S}}^r$ reduces mod $s$ to an iteration $f \mod s : \mathbb{A}_{k(s)}^r \to \mathbb{A}_{k(s)}^r$ over a set with $|k(s)|^r$ elements, hence $h_s(\Phi) \leq 2|k(s)|^r$. Consequently, by the prime number theorem, (9) yields

$$h(\Phi/n) \geq \frac{1}{3}(n/6)^{1/r} \quad \text{for arbitrarily large } n \in \mathbb{N}. \quad (10)$$

We have $h(\Phi/n) \leq |S| \max_{j \leq n} h(\lambda(f^jP))$, and the conclusion of the theorem follows from (10).

4. Two conjectures

We end this note by recording two conjectures related to the setup of Theorem 1.4. Problems of this type have been posed by J.H. Silverman in [8].

**Conjecture 4.1.** Let $X$ be a complex projective variety, $f : X \to X$ a rational self-map, $\lambda : X \to \mathbb{P}^1$ a non-constant rational function, and $P \in X(\mathbb{C})$ a point with well-defined forward orbit. Then the set $\{n \mid \lambda(f^nP) = 0\} \subset \mathbb{N}_0$ is the union of a finite set with finitely many full arithmetic progressions.

**Conjecture 4.2.** Let $A/\bar{\mathbb{Q}}$ be an abelian variety and $\lambda : A \to \mathbb{P}^1$ a non-constant rational function. Consider a point $P \in A(\bar{\mathbb{Q}})$. If $h(\lambda([n]P)) = o(n^2)$ then there is a surjective homomorphism $A \to B$ to an abelian variety mapping $P$ to a torsion point.

**References**

[1] Amice Y.: Les nombres $p$-adiques, *Collection SUP: Le Mathématicien*, vol. 14, Presses Universitaires de France, Paris, 1975.

[2] Bombieri E., W. Gubler: Heights in Diophantine Geometry, *Cambridge New Mathematical Monographs* (2006).

[3] Bombieri E., J. Vaaler: On Siegel’s lemma, *Invent. Math.* 73 (1983), pp. 11–32.
[4] Christol G.: Globally bounded solutions of differential equations, in *Analytic Number Theory Proc. Jap., Fr. Symp. Tokyo, 1988*, Lecture Notes in Math. vol. 1434 (1990), pp. 45–64.

[5] Dimitrov V.: A note on a generalization of the Hadamard quotient theorem. (Preprint.) arXiv:1309.1920

[6] Perelli A., U. Zannier: On recurrent mod $p$ sequences, *J. reine Angew. Math.*, vol. 348 (1984), pp. 135–146.

[7] Ruzsa I.: On congruence preserving functions (in Hungarian), *Mat. Lapok* 22 (1971), pp. 125–134.

[8] Silverman, J. H.: Dynamical degree, arithmetic entropy, and canonical heights for dominant rational self-maps of projective space, *Ergodic Theory and Dynamical Systems*, Available on CJO 2012 doi:10.1017/etds.2012.144. arXiv:1111.5664v2.

[9] Zannier U.: A note on recurrent mod $p$ sequences, *Acta Arithmetica*, vol. 41 (1982), pp. 277–280.

[10] Zannier U.: On periodic mod $p$ sequences and $G$-functions (On a conjecture of Ruzsa), *Manuscripta Math.*, vol. 90 (1996), pp. 391–402.