THE SIZE OF SEMIGROUP ORBITS MODULO PRIMES

WADE HINDES AND JOSEPH H. SILVERMAN
Let $V$ be a projective variety defined over a number field $K$, let $S$ be a polarized set of endomorphisms of $V$ all defined over $K$, and let $P \in V(K)$. For each prime $p$ of $K$, let $m_p(S, P)$ denote the number of points in the orbit of $P$ mod $p$ for the semigroup of maps generated by $S$. Under suitable hypotheses on $S$ and $P$, we prove an analytic estimate for $m_p(S, P)$ and use it to show that the set of primes for which $m_p(S, P)$ grows subexponentially as a function of $N_{K/Q}p$ is a set of density zero. For $V = \mathbb{P}^1$ we show that this holds for a generic set of maps $S$ provided that at least two of the maps in $S$ have degree at least four.

1. Introduction

A general expectation in arithmetic dynamics over number fields is that the dynamical systems generated by “unrelated” self-maps $f_1, f_2 : V \to V$ should not be too similar. For example, they should not have identical canonical heights [16], they should not have infinitely many common preperiodic points [2; 8; 11], their orbits should not have infinite intersection [10], and arithmetically their orbits should not have unexpectedly large common divisors [15]. It is not always clear what “unrelated” should mean, but in any case it includes the assumption that $f_1$ and $f_2$ do not share a common iterate.

Similarly, we expect that the points in semigroup orbits generated by all finite compositions of “unrelated” maps $f_1$ and $f_2$ should be asymptotically large [4; 13] when ordered by height, where now unrelated means that the semigroup is not unexpectedly small. For example, the semigroup is small if it contains no free
infinite subsemigroups requiring at least 2 generators; cf. [3].

In this note, we study the size of semigroup orbits over finite fields. In particular, we show that, under suitable hypotheses, a free semigroup of maps defined over a number field generates many large orbits when reduced modulo primes. See [1; 6; 7; 21] for additional results in this vein.

Definition 1. We set notation that will remain in effect throughout this note.

- \( K/\mathbb{Q} \) a number field
- \( V/K \) a smooth projective variety defined over \( K \)
- \( r \geq 1 \) an integer
- \( S = \{f_1, \ldots, f_r\} \) a set of morphisms \( f_i : V \to V \) defined over \( K \)
- \( d_1, \ldots, d_r \) real numbers satisfying \( d_i > 1 \) for \( i = 1, \ldots, r \)
- \( \mathcal{L} \in \text{Pic}_K(V) \otimes \mathbb{R} \) line bundles satisfying \( f_i^* \mathcal{L} \cong \mathcal{L} \otimes d_i \)
- \( M_S \) the semigroup generated by \( S \) under composition
- \( \text{Orb}_S(P) \) the orbit \( \{f(P) : f \in M_S\} \) of a point \( P \in V \)

The following property will play a crucial role in some of our results.

Definition 2. A point \( P \in V \) is called strongly \( S \)-wandering if the evaluation map

\[
M_S \to V, \quad f \mapsto f(P),
\]

is injective.

Remark 3. If \( V = \mathbb{P}^1 \) and \( S \) is any sufficiently generic set of maps as described in Section 3, then the set of points that fail to be strongly \( S \)-wandering is a set of bounded height. In particular, it follows in this case that all infinite orbits contain strongly wandering points, and this weaker condition is sufficient for our orbit bounds.

Our goal is to study the number of points in the reduction of \( \text{Orb}_S(P) \) modulo primes. We set some additional notation, briefly recall a standard definition, and then define our principal object of study.

\[
\begin{align*}
R_K & \quad \text{the ring of integers of } K \\
\text{Spec}(R_K) & \quad \text{the set of prime ideals of } R_K \\
N_p & \quad \text{the norm of } p \in \text{Spec}(R_K), \text{ that is, } N_p := \#R_K/p.
\end{align*}
\]

Definition 4. Let \( p \in \text{Spec}(R_K) \), and let \( R_p \) denote the localization of \( R_K \) at \( p \), and let \( k_p = R_p/pR_p \) denote the residue field. A finite \( K \)-morphism \( f : V \to V \) has good reduction at \( p \) if there is a scheme \( \mathcal{V}_p/R_p \) that is proper and smooth over \( R_p \), and there is an \( R_p \)-morphism \( F_p : \mathcal{V}_p \to \mathcal{V}_p \) whose generic fiber is \( f : V \to V \).

\footnote{Intuitively, this means that we can find equations for \( V \) and for \( f \) that have coefficients in \( R_K \), and so that when we reduce the equations modulo \( p \), the reduced variety \( \tilde{V} \mod p \) is non-singular and the reduced map \( \tilde{f} : \tilde{V} \to \tilde{V} \) is a morphism having the same degree as \( f \). Of course, when we say “find equations”, this needs to be done locally on an appropriately fine cover by affine neighborhoods.}
We write \( \tilde{V}_p = V_p \times_{R_p} k_p \) for the special fiber of \( V_p \). Properness implies that each point \( Q \in V(K) \) extends to a section \( Q_p \in V_p(R_p) \), and the reduction \( \tilde{Q}_p \in \tilde{V}_p(k_p) \) of \( Q \) modulo \( p \) is the intersection of the image of \( Q_p \) with the fiber \( \tilde{V}_p \), i.e.,
\[
\{ \tilde{Q}_p \} = Q_p(\text{Spec } R_p) \cap V_p.
\]
Similarly, the reduction \( \tilde{f}_p \) of \( f \) modulo \( p \) is the restriction of \( F_p \) to the special fiber \( \tilde{V}_p \).

**Remark 5.** Continuing with notation from **Definition 4**, we note that if \( f \) has good reduction at \( p \), then reduction modulo \( p \) commutes with evaluation,
\[
\tilde{f}(\tilde{Q}_p) = f_p(\tilde{Q}_p).
\]
Further, composition commutes with reduction for good reduction maps. In other words, if \( f \) and \( g \) have good reduction at \( p \), then
\[
(f \circ g)_p = \tilde{f}_p \circ \tilde{g}_p.
\]

**Definition 6.** Let \( p \in \text{Spec}(R_K) \). Continuing with notation from **Definition 4**, let \( f_1, \ldots, f_r : V \to V \) be maps that have good reduction modulo \( p \), and let \( P \in V(K) \). Then the reduction of the \( S \)-orbit of \( P \) modulo \( p \) is the set
\[
\text{Orb}_{\tilde{S}}(\tilde{P} \mod p) := \{ \tilde{f}_p(\tilde{P}_p) : f \in M_S \}.
\]
We define
\[
m_p := m_p(S, P) = \# \text{Orb}_{\tilde{S}}(\tilde{P} \mod p)
\]
to be the size of the mod \( p \) reduction of \( \text{Orb}_S(P) \). (If any of the maps \( f_1, \ldots, f_r \) has bad reduction at \( p \), then we formally set \( m_p = \infty \).)

Our main result is an analytic formula that implies that \( m_p \) is not too small on average.

**Theorem 7.** Assume that \( M_S \) is a free semigroup, that \( P \in V(K) \) is a strongly \( S \)-wandering point, and that \( r = \#S \geq 2 \). Then there exists a constant \( C_1 = C_1(K, V, S, P) \) such that, for all \( \epsilon > 0 \),
\[
\sum_{p \in \text{Spec}(R_K)} \frac{\log N_p}{N_p \cdot m_p(S, P)^\epsilon} \leq C_1 \epsilon^{-1}.
\]

**Remark 8.** The principal result of the paper [21] is an estimate exponentially weaker than (2) in the case that \( r = \#S = 1 \), while a principal result of the paper [17] is an estimate that exactly mirrors (2) with \( m_p \) equal to the number of points on the mod \( p \) reduction of the multiples of a point on an abelian variety. Thus the present
paper, as well as the papers [4; 13], suggest that the analogy

\[
(\text{arithmetic of points of an abelian variety}) \iff (\text{arithmetic of points in orbits of a dynamical system})
\]

described in [5] and [22, §6.5] may be more accurate when the dynamical system on the right-hand side is generated by at least two non-commuting maps, rather than using orbits coming from iteration of a single map.

Estimate (2) can be used to show that there are few primes \( p \) for which \( m_p(S, P) \) is subexponential compared to \( Np \). We quantify this assertion in the following corollary.

**Corollary 9.** Let \( S, M_S \) and \( P \) be as in Theorem 7, and let \( \delta \) and \( \delta \) denote the (upper) logarithmic analytic densities on sets of primes as described in Definition 12.

(a) There is a constant \( C_2 = C_2(K, V, S, P) \) such that

\[
\bar{\delta}(\{p \in \text{Spec}(R_K) : m_p(S, P) \leq Np^\gamma\}) \leq C_2\gamma
\]

holds for all \( 0 < \gamma < 1 \).

(b) Let \( L(t) \) be a subexponential function, i.e., a function with the property that

\[
\lim_{t \to \infty} \frac{L(t)}{t^\mu} = 0 \quad \text{for all } \mu > 0.
\]

Then

\[
\delta(\{p \in \text{Spec}(R_K) : m_p(S, P) \leq L(Np)\}) = 0.
\]

In the special case that \( V = \mathbb{P}^1 \), we show that the conclusions of Theorem 7 and Corollary 9 are true for generic sets of maps. In the statement of the next result, we write \( \text{Rat}_d \) for the space of rational maps of \( \mathbb{P}^1 \) of degree \( d \geq 2 \), so in particular \( \text{Rat}_d \) is an affine variety of dimension \( 2d + 1 \); see [20, §4.3] for details.

**Theorem 10.** Let \( r \geq 2 \), and let \( d_1, \ldots, d_r \) be integers satisfying

\[
d_1, d_2 \geq 4 \quad \text{and} \quad d_3, \ldots, d_r \geq 2.
\]

Then there is a Zariski dense subset

\[
U = U(d_1, \ldots, d_r) \subseteq \text{Rat}_{d_1} \times \cdots \times \text{Rat}_{d_r}
\]

such that the inequality (2) in Theorem 7 and the density estimates in Corollary 9 are true for all number fields \( K/\mathbb{Q} \), all \( S \in U(K) \), and all \( P \in \mathbb{P}^1(K) \) for which \( \text{Orb}_S(P) \) is infinite.

The contents of this paper are as follows. In Section 2 we build upon prior work [17; 21] of the second author to prove Theorem 7 and Corollary 9. Then in Section 3 we use results from [10; 13; 23] to construct many sets of maps on \( \mathbb{P}^1 \).
for which the bounds in Section 2 apply. The key step is to construct a point in every infinite orbit that is strongly wandering. The construction is explicit, and in particular, Theorem 15 describes an explicit set \( \mathcal{U} \) for which Theorem 10 is true.

2. The size of orbits modulo \( p \)

We start with a key estimate.

**Proposition 11.** Let \( S, M_S \) and \( P \) be as in Theorem 7. For each \( m \geq 2 \), we define an integral ideal

\[
\mathfrak{D}(m) = \mathfrak{D}(m; K, V, S, P) := \prod_{p \in \text{Spec}(R_K)} p.
\]

There are constants \( C_i = C_i(K, V, S, P) \) for \( i = 3, 4 \) such that the following hold:

(a) If \( r = \#S = 1 \), then

\[
\log \log N \mathfrak{D}(m) \leq C_3 m \quad \text{for all } m \geq 2.
\]

(b) Assume that \( S \) generates a free semigroup, that \( P \in V(K) \) is strongly \( S \)-wandering, and that \( r = \#S \geq 2 \). Then

\[
\log \log N \mathfrak{D}(m) \leq C_4 \log m \quad \text{for all } m \geq 2.
\]

**Proof.** (a) This is [21, Proposition 10].

(b) Next, since \( V \) and \( S \) are polarized with respect to some line bundle \( \mathcal{L} \), we may choose \( N \geq 1 \) and an embedding \( V \subseteq \mathbb{P}^N \) such that the \( f_i \) extend to self-morphisms of \( \mathbb{P}^N \). Next, for notational convenience, we write \( m_p \) for \( m_p(S, P) \) and use the standard combinatorics notation \( [r] = \{1, 2, \ldots, r\} \). Also to ease notation, we write

\[
f_i := f_{i_1} \circ f_{i_2} \circ \cdots \circ f_{i_k} \quad \text{for } i = (i_1, \ldots, i_k) \in [r]^k.
\]

Let

\[
m \geq 1 \quad \text{and} \quad k = k(m) := \left\lfloor \frac{\log(m + 1)}{\log r} \right\rfloor.
\]

For each good reduction prime \( p \), we consider the map that sends a function \( f_i \) to the image of \( P \) under reduction modulo \( p \),

\[
[r]^k \rightarrow \mathcal{O}_\tilde{S}(\tilde{P} \mod p), \quad i \mapsto f_i(P) \mod p.
\]

If

\[
m_p \leq m, \quad \text{then} \quad r^k > m_p \quad \text{by our choice of } k,
\]

so the map (4) cannot be injective (pigeonhole principle) and there exist

\[
i \neq j \text{ in } [r]^k \quad \text{satisfying} \quad f_i(P) \equiv f_j(P) \mod p.
\]
Sine we have assumed that $P$ is strongly wandering, i.e., that the map
\[ M_S \to V(K), \quad f \mapsto f(P), \]
is injective, it follows that the global points are distinct,
\[ f_i(P) \neq f_j(P), \]
so the ideals generated by their “differences” are non-zero.

More formally, [21, Lemma 9] says that there is an integral ideal $C = C_K \subseteq R_K$ with the property that every point $Q \in \mathbb{P}^N(K)$ can be written with homogeneous coordinates
\[ Q = [\alpha_0, \ldots, \alpha_N] \]
satisfying\footnote{If $R_K$ is a PID, then we can take $C = R_K$, so $\gcd(\alpha_0, \ldots, \alpha_N) = 1$. Thus [21, Lemma 9] provides a weaker version of this gcd result that holds for all $R_K$.}
\[ \alpha_0, \ldots, \alpha_N \in R_K \quad \text{and} \quad (\alpha_0 R_K + \cdots + \alpha_N R_K) \mid C_K. \]

Applying [21, Lemma 9] to our situation, for the given $P \in V(K)$, we can write
\[ f_i(P) = [A_0(i), \ldots, A_N(i)] \]
with $A_0(i), \ldots, A_N(i) \in R_K$ and such that the ideal
\[ \mathfrak{A}(i) := A_0(i)R_K + \cdots + A_N(i)R_K \]
divides the ideal $C$.

Then for $p \nmid C$ we have
\[ f_i(P) \equiv f_j(P) \pmod{p} \]
\[ \iff A_u(i)A_v(j) \equiv A_v(i)A_u(j) \pmod{p} \quad \text{for all } 0 \leq u, v \leq N. \]

We define a difference ideal
\[ \mathfrak{B}(i, j) := \sum_{0 \leq u, v \leq N} (A_u(i)A_v(j) - A_v(i)A_u(j))R_K, \]
and the product of the difference ideals
\[ \mathfrak{D}'(m) := \prod_{i, j \in [r]^k, i \neq j} \mathfrak{B}(i, j). \]

Then
\[ p \nmid C \text{ and } m_p \leq m \implies p \mid \mathfrak{D}'(m), \]
and hence
\[ \mathfrak{D}(m) \mid C \cdot \mathfrak{D}'(m). \]
Since $C$ depends only on $K$, it remains to estimate the norm of $\mathcal{D}'(m)$.

Let $h(\cdot)$ denote the logarithmic Weil height on $\mathbb{P}^N$, and let $\mathfrak{A}(i)$ for $i \in [r]^k$ be the ideals defined by (5). Then, using [21, Proposition 7], we find for all $i$ and $j$ that
\[
\frac{1}{[K : \mathbb{Q}]} \log \frac{N\mathfrak{A}(i, j)}{N\mathfrak{A}(i) \cdot N\mathfrak{A}(j)} \leq h(f_i(P)) + h(f_j(P)) + C_5,
\]
where $C_5$ is an absolute constant. Since $N\mathfrak{A}(i)$ and $N\mathfrak{A}(j)$ are smaller than $NC$, this implies that
\[
\frac{1}{[K : \mathbb{Q}]} \log N\mathfrak{A}(i, j) \leq h(f_i(P)) + h(f_j(P)) + C_6.
\]
Next we apply the height estimate
\[
h(f_i(P)) \leq C_7 \cdot \prod_{u=1}^{k} d_{iu},
\]
which is a weak form of [12, Lemma 2.1]. This yields
\[
\frac{1}{[K : \mathbb{Q}]} \log N\mathfrak{A}(i, j) \leq C_7 \cdot \prod_{u=1}^{k} d_{iu} + C_7 \cdot \prod_{u=1}^{k} d_{ju} + C_6.
\]
This gives
\[
\log \mathcal{D}'(m) = \sum_{i, j \in [r]^k, i \neq j} \log \mathfrak{A}(i, j)
\leq \sum_{i, j \in [r]^k, i \neq j} \left( C_7 \cdot \prod_{u=1}^{k} d_{iu} + C_7 \cdot \prod_{u=1}^{k} d_{ju} + C_6 \right)
\leq C_8 \cdot r^k \cdot \sum_{i \in [r]^k} \prod_{u=1}^{k} d_{iu}
= C_8 \cdot \left( r \cdot \sum_{i \in [r]} d_i \right)^k
\leq C_9 \cdot \left( r \cdot \sum_{i \in [r]} d_i \right)^{1 + \frac{\log(m+1)}{\log r}}.
\]
Hence
\[
\log \log \mathcal{D}'(m) \leq C_{10} \cdot \log(m+1) + C_{11}.
\]
Since $m \geq 2$, we can absorb $C_{11}$ into $C_{10}$, although we remark that if we leave in $C_{11}(K, V, S, P)$, then we can take $C_{10}$ to depend on only the degrees of the
maps in $S$,

$$C_{10} = C_{10}(d_1, \ldots, d_r) = 1 + \frac{\log(d_1 + \cdots + d_r)}{\log r}.$$ 

This completes the proof of Proposition 11. □

**Proof of Theorem 7.** To ease notation, we let

$$g(t) = \frac{\log t}{t} \quad \text{and} \quad G(t) = \frac{1}{t^\epsilon}.$$ 

We start with two elementary estimates. First, the mean value theorem gives

$$G(m) - G(m + 1) \leq \sup_{m \leq t \leq m+1} -G'(t) = \sup_{m \leq t \leq m+1} \frac{\epsilon}{t^{1+\epsilon}} = \frac{\epsilon}{m^{1+\epsilon}}.$$  

(6)

Second, an easy integral calculation gives

$$\sum_{m \geq 1} g(m)G(m) \leq \int_1^\infty \frac{\log x}{x^{1+\epsilon}} \, dx = \frac{1}{\epsilon^2}. $$  

(7)

We use these and our other calculations to estimate

$$\sum_{p \in \text{Spec}(R_K)} \frac{\log Np}{Np \cdot m_p^\epsilon}$$

$$= \sum_{p \in \text{Spec}(R_K)} g(Np) \cdot G(m_p) \quad \text{(by definition of $g$ and $G$)}$$

$$= \sum_{m \geq 1} G(m) \sum_{p \in \text{Spec}(R_K)} g(Np)$$

$$= \sum_{m \geq 1} (G(m) - G(m + 1)) \sum_{p \in \text{Spec}(R_K)} g(Np) \quad \text{(Abel summation)}$$

$$\leq \sum_{m \geq 1} \frac{\epsilon}{m^{1+\epsilon}} \sum_{p \in \text{Spec}(R_K)} g(Np) \quad \text{(from (6))}$$

$$= \sum_{m \geq 1} \frac{\epsilon}{m^{1+\epsilon}} \sum_{p \in \text{Spec}(R_K)} g(Np) \quad \text{(by definition (3) of $\mathcal{O}(m)$)}$$

$$\leq \sum_{m \geq 1} \frac{\epsilon}{m^{1+\epsilon}} \cdot (C_{12} \log \log \mathcal{O}(m) + C_{13}) \quad \text{(from [17, Corollary 2.3])}$$

$$\leq C_{14} \sum_{m \geq 1} \frac{\epsilon}{m^{1+\epsilon}} \cdot \log m \quad \text{(from Proposition 11(b))}$$

$$= C_{14} \cdot \epsilon \cdot \sum_{m \geq 1} g(m) \cdot G(m) \quad \text{(by definition of $g$ and $G$)}$$

$$\leq C_{15} \epsilon^{-1} \quad \text{(from (7))}. \quad \square$$
Definition 12. Let $\mathcal{P} \subset \text{Spec}(R_K)$ be a set of primes. The upper logarithmic analytic density of $\mathcal{P}$ is

$$\overline{\delta}(\mathcal{P}) := \limsup_{s \to 1^+} (s - 1) \sum_{p \in \mathcal{P}} \frac{\log Np}{Np^s}.$$ 

Similarly, the logarithmic analytic density of $\mathcal{P}$, denoted $\delta(\mathcal{P})$, is given by the same formula with a limit, instead of a lim sup.

Proof of Corollary 9. (a) For any $0 < \gamma < 1$, we let

$$\mathcal{P}_\gamma := \{ p \in \text{Spec}(R_K) : m_p \leq Np^\gamma \}.$$

Then

$$\frac{C_1}{\epsilon} \geq \sum_{p \in \text{Spec}(R_K)} \frac{\log Np}{Np \cdot m_p^\epsilon} \quad (\text{from Theorem 7})$$

$$\geq \sum_{p \in \mathcal{P}_\gamma} \frac{\log Np}{Np \cdot m_p^\epsilon} \quad (\text{summing over a smaller set})$$

$$(8) \geq \sum_{p \in \mathcal{P}_\gamma} \frac{\log Np}{Np^{1+\gamma \epsilon}} \quad (by \text{definition of } \mathcal{P}_\gamma).$$

This allows us to estimate the upper logarithmic density of $\mathcal{P}_\gamma$ by

$$\overline{\delta}(\mathcal{P}_\gamma) = \limsup_{s \to 1^+} (s - 1) \sum_{p \in \mathcal{P}_\gamma} \frac{\log Np}{Np^s}$$

$$= \limsup_{\epsilon \to 0^+} \gamma \epsilon \sum_{p \in \mathcal{P}_\gamma} \frac{\log Np}{Np^{1+\gamma \epsilon}} \quad (setting \ s = 1 + \gamma \epsilon)$$

$$\leq \limsup_{\epsilon \to 0^+} \gamma \epsilon \cdot \frac{C_1}{\epsilon} \quad (from \ (8))$$

$$= C_1 \gamma.$$ 

This completes the proof of Corollary 9(a).

(b) We let

$$\mathcal{P}_L := \{ p \in \text{Spec}(R_K) : m_p \leq L(Np) \}.$$

The assumption that $L$ is subexponential means that for all $\mu > 0$ there exists a constant $C_{16}(L, \mu)$ depending only on $L$ and $\mu$ such that

$$L(t) \leq t^\mu \quad \text{for all } t > C_{16}(L, \mu).$$
We also note that
\[ p \in \mathcal{P}_L \iff m_p \leq L(Np) \]
(9) \[ \implies m_p \leq (Np)^\mu \quad \text{for all } Np > C_16(L, \mu). \]

We now fix a \( \mu > 0 \) and estimate
\[
\bar{\delta}(\mathcal{P}_L) = \limsup_{\lambda \to 0^+} \lambda \sum_{p \in \mathcal{P}_L} \frac{\log Np}{Np^{1+\lambda}}
\]
\[
= \limsup_{\lambda \to 0^+} \lambda \sum_{p \in \mathcal{P}_L, Np \geq C_{16}(L, \mu)} \frac{\log Np}{Np^{1+\lambda}} \quad \text{(since } \mu \text{ is fixed, so we can discard finitely many terms)}
\]
\[
\leq \limsup_{\lambda \to 0^+} \lambda \sum_{p \in \mathcal{P}_L, Np \geq C_{16}(L, \mu)} \frac{\log Np}{Np} \cdot \frac{1}{m_p^{\lambda/\mu}} \quad \text{(from (9))}
\]
\[
\leq \limsup_{\lambda \to 0^+} \lambda \sum_{p \in \text{Spec } R_K} \frac{\log Np}{Np} \cdot \frac{1}{m_p^{\lambda/\mu}}
\]
\[
\leq \limsup_{\lambda \to 0^+} \lambda \cdot C_1 \cdot \left( \frac{\lambda}{\mu} \right)^{-1} \quad \text{(from Theorem 7)}
\]
\[
= C_1 \mu.
\]

This estimate holds for all \( \mu > 0 \), so we find that
\[
\bar{\delta}(\mathcal{P}_L) \leq \inf_{\mu > 0} C_1 \cdot \mu = 0,
\]
which completes the proof that \( \delta(\mathcal{P}_L) = 0 \). \( \square \)

3. Orbits of generic families of maps of \( \mathbb{P}^1 \)

In this section, we show that there are many sets of endomorphisms of \( \mathbb{P}^1 \) for which Theorem 7 holds. To make this statement precise, we need some definitions.

**Definition 13.** Let \( f \) be a non-constant rational map of \( \mathbb{P}^1 \) defined over \( \overline{\mathbb{Q}} \). A point \( w \in \mathbb{P}^1(\overline{\mathbb{Q}}) \) is a **critical value** of \( f \) if \( f^{-1}(w) \) contains fewer than \( \deg(f) \) elements. It is a **simple critical value** if
\[
\# f^{-1}(w) = \deg(f) - 1.
\]
The map \( f \) is **critically simple** if all of its critical values are simple.

**Definition 14.** Let \( f \) and \( g \) be non-constant rational maps of \( \mathbb{P}^1 \) with respective critical value sets \( \text{CritVal}_f \) and \( \text{CritVal}_g \). We say that \( f \) and \( g \) are **critically separated** if
\[
\text{CritVal}_f \cap \text{CritVal}_g = \emptyset.
\]
Our first result says that the conclusions of Theorem 7 and Corollary 9 hold for certain sets \( S \) that contain a pair of critically simple and critically separated maps and initial points \( P \) with infinite orbit.

**Theorem 15.** Let \( K/\mathbb{Q} \) be a number field, let \( S \) be a set of endomorphisms of \( \mathbb{P}^1 \) defined over \( K \) containing a pair of critically simple and critically separated maps of degree at least 4, and let \( P \in \mathbb{P}^1(K) \) be a point with infinite \( S \)-orbit. Then there is a constant \( C_{17} = C_{17}(K, S, P) \) such that for all \( \epsilon > 0 \),

\[
\sum_{p \in \text{Spec}(R_K)} \frac{\log N_p}{N_p \cdot m_p(S, P)\epsilon} \leq C_{17} \cdot \epsilon^{-1}.
\]

**Remark 16.** In particular, there is a constant \( C_{18}(S) \) such that Theorem 15 holds for all \( P \in \mathbb{P}^1(K) \) satisfying \( h(P) > C_{18}(S) \); see Lemma 18.

We start with a definition and some basic height estimates. In what follows, we fix an embedding \( V \subseteq \mathbb{P}^N \) and extend the maps \( f_i \) to self-morphisms of \( \mathbb{P}^N \); here we use our assumption that \( S \) is polarizable with respect to some line bundle \( L \). Moreover, \( h(\cdot) \) denotes the logarithmic Weil height on \( \mathbb{P}^N \).

**Definition 17.** A point \( P \in V \) is moderately \( S \)-preperiodic if

\[
g \circ f(P) = f(P) \quad \text{for some } f, g \in M_S \text{ with } g \neq 1.
\]

**Lemma 18.** Let \( V/\mathbb{Q} \) be a variety, and let \( S = \{f_1, \ldots, f_r\} \) be a set of polarized endomorphisms as described in Definition 1. Then there exists a constant \( C_{19} = C_{19}(S, V, L) \) such that the following statements hold for all \( Q \in V(\overline{\mathbb{Q}}) \):

(a) If \( Q \) is moderately \( S \)-preperiodic as described in Definition 17, then \( h(Q) \leq C_{19} \).

(b) If \( h(Q) > C_{19} \), then

\[
h(f(Q)) \geq h(Q) \quad \text{for all } f \in M_S.
\]

**Proof.** These estimates are proven in [4, Lemma 2.11].

We combine Lemma 18 with the techniques in [13; 19] to obtain the following result for pairs of maps that are critically simple and critically separated.

**Proposition 19.** Let \( f_1 \) and \( f_2 \) be endomorphisms of \( \mathbb{P}^1 \) of degree at least 4, let \( S = \{f_1, f_2\} \), and suppose that \( f_1 \) and \( f_2 \) are critically simple and critically separated. Then the following statements hold:

(a) The semigroup \( M_S \) is free.

(b) Let \( P \in \mathbb{P}^1(\overline{\mathbb{Q}}) \) be a point whose \( S \)-orbit \( \text{Orb}_S(P) \) is infinite. Then there exists a point \( Q \in \text{Orb}_S(P) \) such that \( Q \) is strongly \( S \)-wandering as described in Definition 2.
Proof. (a) See [13, Proposition 4.1].

(b) We fix a number field \( K \) over which \( P, f_1, \) and \( f_2 \) are defined. Letting \( \Delta \subset \mathbb{P}^1 \times \mathbb{P}^1 \) be the diagonal, we define three curves

\[
\Gamma_i := (f_i \times f_i)^{-1}(\Delta) \quad \text{for } i = 1, 2,
\]

\[
\Gamma_{1,2} := (f_1 \times f_2)^{-1}(\Delta).
\]

Then the main results in [19] (see also [13, Proposition 4.6]) imply that the curves \( \Gamma_1 \) and \( \Gamma_2 \) are each the union of \( \Delta \) and an irreducible curve of geometric genus \( \geq 2 \), while \( \Gamma_{1,2} \) is itself an irreducible curve of geometric genus \( \geq 2 \).

More specifically, the assumption that \( f_1 \) and \( f_2 \) are critically simple implies from [19, Corollary 3.6] that \( C_1 \backslash \Delta \) and \( C_2 \backslash \Delta \) are irreducible, while the assumption that \( f_1 \) and \( f_2 \) are critically separated implies from [19, Proposition 3.1] that \( C_{1,2} \) is irreducible. It then follows from [19, pages 208 and 210] that the geometric genera of these curves are given by the formulas

\[
\text{genus}(\Gamma_i \backslash \Delta) = (\deg(f_i) - 2)^2 \quad \text{for } i = 1, 2,
\]

\[
\text{genus}(\Gamma_{1,2} \backslash \Delta) = (\deg(f_1) - 1)(\deg(f_2) - 1).
\]

In particular, the assumption that \( f_1 \) and \( f_2 \) have degree at least 4 ensures that these genera are at least 2.

We now invoke Faltings’s theorem [9], [14, Theorem E.0.1] to deduce that the set

\[
\Sigma := \Gamma_{1,2}(K) \cup (\Gamma_1 \backslash \Delta)(K) \cup (\Gamma_2 \backslash \Delta)(K)
\]

is finite. We note that the definition of \( \Sigma \) says that for all \( P, Q \in \mathbb{P}^1(K) \), we have

\[
\begin{cases}
P \neq Q \quad \text{and} \quad f_1(P) = f_1(Q) & \Rightarrow \quad (P, Q) \in \Sigma \\
P \neq Q \quad \text{and} \quad f_2(P) = f_2(Q) & \Rightarrow \quad (P, Q) \in \Sigma \\
f_1(P) = f_2(Q) & \Rightarrow \quad (P, Q) \in \Sigma
\end{cases}
\]

Let \( \pi_1, \pi_2 : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1 \) be the two projection maps, and let

\[
C_{20} := \max\{\{h(P) : P \in \pi_1(\Sigma)\} \cup \{h(P) : P \in \pi_2(\Sigma)\}\}
\]

be the maximum of the heights of the coordinates of the finitely many points in \( \Sigma \). We then set

\[
C_{21} := \max\{C_{19}, C_{20}\},
\]

where \( C_{19} \) is the constant that appears in Lemma 18.

The fact that \( \text{Orb}_S(P) \subseteq \mathbb{P}^1(K) \) is infinite, combined with Northcott’s theorem [18] saying that \( \mathbb{P}^1(K) \) has only finitely many points of bounded height,
implies that there exists a point $Q \in \text{Orb}_S(P)$ satisfying
\begin{equation}
   h(Q) > C_{21}.
\end{equation}

We claim that $Q$ is strongly wandering for $S$. To see this, suppose that
\begin{equation}
   f_{i_1} \circ \cdots \circ f_{i_n}(Q) = f_{j_1} \circ \cdots \circ f_{j_m}(Q),
\end{equation}
where without loss of generality we may assume that $n \geq m$. Our goal is to prove that $m = n$ and $i_k = j_k$ for all $1 \leq i \leq n$.

To ease notation, we let
\begin{equation}
   F = f_{i_2} \circ \cdots \circ f_{i_n} \quad \text{and} \quad G = f_{j_2} \circ \cdots \circ f_{j_m}
\end{equation}
be the compositions with the initial map omitted. Thus (12) and (13) say that
\begin{equation}
   f_{i_1}(F(Q)) = f_{j_1}(G(Q)).
\end{equation}

It follows from (14) and (10) that one of the following is true:
\begin{enumerate}
   \item $i_1 = j_1$ and $F(Q) = G(Q)$.
   \item $i_1 = j_1$ and $F(Q) \neq G(Q)$ and $(F(Q), G(Q)) \in \Sigma$.
   \item $i_1 \neq j_1$ and $(F(Q), G(Q)) \in \Sigma$.
\end{enumerate}

On the other hand, we know that
\begin{equation}
   (F(Q), G(Q)) \in \Sigma \implies h(F(Q)) \leq C_{21} < h(Q)
\end{equation}
by (11). But this contradicts Lemma 18. Hence (ii) and (iii) are false, so (i) is true.

We recall that $m \leq n$, so repeating this argument, we conclude that
\begin{equation}
   i_k = j_k \quad \text{for all } 1 \leq k \leq m.
\end{equation}

If $m < n$ is a strict inequality, then we see that
\begin{equation}
   f_{i_{m+1}} \circ \cdots \circ f_{i_n}(Q) = Q.
\end{equation}

But then Lemma 18 implies that $h(Q) \leq C_{19} \leq C_{21}$, and we obtain a contradiction of (11). Thus $m = n$ and $i_k = j_k$ for all $1 \leq k \leq n$, which completes the proof that $Q$ is a strongly $S$-wandering point.

We now have the tools in place to prove Theorem 15.

\textbf{Proof of Theorem 15.} Let $S$ be the given set of endomorphisms of $\mathbb{P}^1$, and let $f_1$ and $f_2$ be the given maps in $S$ that have degree at least 4 and that are critically simple and critically separated. We let
\begin{equation}
   S' = \{f_1, f_2\}.
\end{equation}
We are given that the point \( P \in \mathbb{P}^1(K) \) has infinite \( S \)-orbit, and hence by Northcott’s theorem \([18]\), there are points of arbitrarily large height in \( \text{Orb}_S(P) \). We choose a point 
\[
Q' \in \text{Orb}_S(P) \text{ satisfying } h(Q') > C_{19}(S'),
\]
where \( C_{19}(S') \) is the constant associated to the set \( S' \) appearing in Lemma 18. In particular, it follows from Lemma 18(b) and Northcott’s theorem that \( \text{Orb}_{S'}(Q') \) must be infinite. Then Proposition 19 implies that \( M_{S'} \) is free and that there is a point 
\[
Q \in \text{Orb}_{S'}(Q') \subseteq \text{Orb}_S(P)
\]
that is strongly \( S' \)-wandering. Applying Theorem 7 to the set \( S' \) and the point \( Q \), we deduce that 
\[
\sum_{p \in \text{Spec}(R_K)} \frac{\log N_p}{N_p \cdot m_p(S, P)^\epsilon} \leq \sum_{p \in \text{Spec}(R_K)} \frac{\log N_p}{N_p \cdot m_p(S', Q)^\epsilon} \leq C_{17} \epsilon^{-1}
\]
for some constant \( C_{17} \) depending on \( S, Q \) (and so \( P \)) and \( K \). For this last conclusion, we have also used the fact that 
\[
m_p(S', Q) \leq m_p(S, P),
\]
which is immediate from the inclusion \( \text{Orb}_{S'}(Q) \subseteq \text{Orb}_S(P) \). \( \square \)

**Proof of Theorem 10.** We recall that \( \text{Rat}_d \) denotes the space of rational maps of degree \( d \). Then it follows from Theorems 1.1–1.4 in \([19]\) that if \( d_1, d_2 \geq 4 \), then the set 
\[
\mathcal{V}_{d_1,d_2} := \left\{ (f_1, f_2) \in \text{Rat}_{d_1} \times \text{Rat}_{d_2} : f_1 \text{ and } f_2 \text{ are critically simple and critically separated} \right\}
\]
is Zariski dense in \( \text{Rat}_{d_1} \times \text{Rat}_{d_2} \). Then for any \( d_3, \ldots, d_r \geq 2 \), the set 
\[
\mathcal{U}(d_1, \ldots, d_r) := \mathcal{V}_{d_1,d_2} \times \text{Rat}_{d_3} \times \cdots \times \text{Rat}_{d_r}
\]
is Zariski dense in \( \text{Rat}_{d_1} \times \cdots \times \text{Rat}_{d_r} \), and Theorem 15 gives us that the desired inequality (2) for every \( S \) generated by a set of maps 
\[
(f_1, \ldots, f_r) \in \mathcal{U}(d_1, \ldots, d_r).
\]
\( \square \)

We conclude with a variant of Theorem 15 in which the maps are polynomials. We start with a definition.

**Definition 20.** A polynomial \( f(x) \in \overline{\mathbb{Q}}[x] \) is **power-like** if there exist polynomials \( R(x), C(x), L(x) \in \overline{\mathbb{Q}}[x] \) such that 
\[
f = R \circ C \circ L, \deg(L) = 1, \deg(C) \geq 2,
\]
\[
C(x) = \text{a power map or a Chebyshev polynomial}.
\]
Theorem 21. Let $K/\mathbb{Q}$ be a number field, let $S$ be a set of endomorphisms of $\mathbb{P}^1$ defined over $K$, and let $P \in \mathbb{P}^1(K)$ be a point such that $\text{Orb}_S(P)$ is infinite. Suppose further that $S$ contains polynomials $f_1(x), f_2(x) \in K[x]$ having the following properties:

1. Neither $f_1$ nor $f_2$ is power-like; see Definition 20.
2. For all $g \in \overline{\mathbb{Q}}[x]$ satisfying $\deg(g) \geq 2$, we have $f_1 \neq f_2 \circ g$ and $f_2 \neq f_1 \circ g$.

Then there is a constant $C_{22} = C_{22}(K, S, P)$ such that for all $\epsilon > 0$,

$$\sum_{p \in \text{Spec}(K)} \frac{\log N_p}{N_p \cdot m_p(S, P)} \leq C_{22} \cdot \epsilon^{-1}.$$

The proof of Theorem 21 is similar to the proof of Theorem 15, except that we use [10; 23] instead of [13; 19]. As a first step, we need the following result, which is a polynomial analogue of Proposition 19.

Proposition 22. Let $f_1$ and $f_2$ be polynomials satisfying the hypotheses of Theorem 21, and let $S = \{f_1, f_2\}$. Then the following statements hold:

(a) The semigroup $M_S$ is free.

(b) Let $P \in \mathbb{P}^1(\overline{\mathbb{Q}})$ be a point whose $S$-orbit $\text{Orb}_S(P)$ is infinite. Then there exists a strongly $S$-wandering point $Q \in \text{Orb}_S(P)$.

Proof. (a) See [13, Proposition 4.5].

(b) The proof is very similar to the proof of Proposition 19, so we just give a brief sketch, highlighting the differences. We note that we have picked a coordinate function $x$ on $\mathbb{P}^1$. We let $\infty \in \mathbb{P}^1$ be the pole of $x$ and let $\mathbb{A}^1 = \mathbb{P}^1 \setminus \{\infty\}$. Replacing $P$ with another point in $\text{Orb}_S(P)$ if necessary, we may assume that $P \neq \infty$ is not the point at infinity. We choose a set $\mathcal{G}$ of primes of $K$ so that the ring of $\mathcal{G}$-integers $R_{K, \mathcal{G}}$ satisfies

$$P \in \mathbb{A}^1(R_{K, \mathcal{G}}) \quad \text{and} \quad f_1(x), f_2(x) \in R_{K, \mathcal{G}}[x].$$

We use the map $f_1 \times f_2 : \mathbb{A}^2 \to \mathbb{A}^2$ to define three affine curves,

$$\Gamma_1 := (f_1 \times f_1)^{-1}(\Delta), \quad \Gamma_2 := (f_2 \times f_2)^{-1}(\Delta), \quad \Gamma_{1,2} := (f_1 \times f_2)^{-1}(\Delta).$$

Then [13, Proposition 4.5], itself a consequence of the main results of [10; 23], tells us that these are geometrically irreducible curves of geometric genus at least 1. (This is where we use the assumptions (1) and (2) of Theorem 21 on $f_1$ and $f_2$.)
The Siegel–Mahler theorem for integral points on affine curves [14, Theorem D.9.1] then implies that
\[ \Gamma_1(R_K, \mathcal{E}), \quad \Gamma_2(R_K, \mathcal{E}), \quad \text{and} \quad \Gamma_{1,2}(R_K, \mathcal{E}) \]
are finite sets, and hence that
\[ \Sigma := \Gamma_{1,2}(R_K, \mathcal{E}) \cup (\Gamma_1 \setminus \Delta)(R_K, \mathcal{E}) \cup (\Gamma_2 \setminus \Delta)(R_K, \mathcal{E}) \]
is finite.

The remainder of the proof of Proposition 22 follows the proof of Proposition 19, starting with the three possibilities described in (10).

Proof of Theorem 21. The proof of Theorem 21 is identical to that of Theorem 15. We first use Lemma 18, Proposition 22, and the fact that \( \text{Orb}_S(P) \) is infinite to find a point \( Q \in \text{Orb}_S(P) \) that is strongly wandering for \( S' = \{ f_1, f_2 \} \). We then apply Theorem 7 to the point \( Q \) and the set \( S' = \{ f_1, f_2 \} \) to deduce the desired result for \( P \) and \( S \).  

Acknowledgements

The authors thank the referee for their detailed and helpful report.

References


Received March 31, 2023. Revised September 1, 2023.

WADE HINDES
DEPARTMENT OF MATHEMATICS
TEXAS STATE UNIVERSITY
SAN MARCOS, TX
UNITED STATES
wmh33@txstate.edu

JOSEPH H. SILVERMAN
DEPARTMENT OF MATHEMATICS
BROWN UNIVERSITY
PROVIDENCE, RI
UNITED STATES
joseph_silverman@brown.edu
Totally geodesic hyperbolic 3-manifolds in hyperbolic link complements of tori in $S^4$

MICHELLE CHU and ALAN W. REID

 Infinite homotopy stable class for 4-manifolds with boundary

ANTHONY CONWAY, DIARMUID CROWLEY and MARK POWELL

Counterexamples to the nonsimply connected double soul conjecture

JASON DeVITO

The fundamental group of an extension in a Tannakian category and the unipotent radical of the Mumford–Tate group of an open curve

PAYMAN ESKANDARI and V. KUMAR MURTY

The size of semigroup orbits modulo primes

WADE HINDES and JOSEPH H. SILVERMAN

Tropical Lagrangian multisections and toric vector bundles

YAT-HIN SUEN

Some effectivity results for primitive divisors of elliptic divisibility sequences

MATTEO VERZOBIO

Poisson manifolds of strong compact type over 2-tori

LUKA ZWAAN