ENDOMORPHISMS OF BOUNDED HEIGHT AND RESULTANT

BRIAN STOUT AND ADAM TOWSLEY

Abstract. Let $K$ be an algebraic number field and $B \geq 1$. For an endomorphism $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ defined over $K$ of degree $d$ let $\mathfrak{R}_\varphi \subset \mathcal{O}_K$ denote its minimal resultant ideal. For a fixed height function $h_{\mathcal{M}_d^n}$ on the moduli space of dynamical systems this paper shows that all such morphisms $\varphi$ of bounded resultant $N_{K/Q}(\mathfrak{R}_\varphi) \leq B$ and bounded height $h_{\mathcal{M}_d^n}([\varphi]) \leq B$ are contained in finitely many $\text{PGL}_{n+1}(K)$-equivalence classes. This answers a question of Silverman in the affirmative.

1. Introduction

In [2] Silverman asked the following question: given a rational map $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $d$ defined over $K$ are there only finitely many $K$-isomorphism classes of $\varphi$ of bounded height and bounded resultant? We prove the following $n$-dimensional generalization of Silverman’s question:

Theorem 1. Let $K$ be a number field and let $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ be a morphism of degree $d \geq 2$ defined over $K$. Let $\mathfrak{R}_\varphi$ denote the minimal resultant ideal of $\varphi$. Fix an embedding of $\mathcal{M}_d^n$ into projective space and denote the associated height function by $h$. If $B \geq 1$ then the set

$$
\Gamma_{K,B} = \{ \varphi \in \text{Hom}_d^n(K) : N_{K/Q}(\mathfrak{R}_\varphi) \leq B \text{ and } h([\varphi]) \leq B \}
$$

is contained in only finitely many $\text{PGL}_{n+1}(K)$-conjugacy classes of morphisms.

The minimal resultant ideal is a way of encoding information about the primes of bad reduction for $\varphi$ across its conjugacy class. For every non-archimedean place $v$ for which $\mathfrak{R}_\varphi$ has positive valuation, some conjugate $\varphi^f$ for $f \in \text{PGL}_{n+1}(K)$ has bad reduction.

One can consider the height $h([\varphi])$ as a measure of the arithmetic complexity of the conjugacy class of $\varphi$ and the norm of the resultant as

2010 Mathematics Subject Classification. Primary: 37P45; Secondary: 14D22.

Key words and phrases. Arithmetic dynamics, bounded height, bounded resultant.

Date of last revision: May 8, 2014.
a measure of the amount of bad reduction. As we will see in Section 3, bounding the norm of the minimal resultant ideal bounds the primes for which \( \varphi \) has bad reduction.

Bounding both the height of the conjugacy class and the norm of the minimal resultant ideal are needed to obtain a finiteness result. If only the norm \( N_{K/Q}(R_{\varphi}) \) is bounded, then one can still find infinitely many distinct PGL\(_{n+1}(K)\)-conjugacy classes of endomorphisms defined over \( K \). This can be accomplished, for example, by considering monic polynomials defined over \( \mathcal{O}_K \). Monic polynomials have everywhere good reduction and hence their minimal resultant ideal is the unit ideal, which has norm 1. It is easy to show that there are infinitely many distinct PGL\(_{n+1}(\overline{K})\)-conjugacy classes of such maps, and therefore infinitely many distinct PGL\(_{n+1}(K)\)-conjugacy classes.

Conversely, if one bounds only the height \( h(\langle \varphi \rangle) \) one gets a finite set of points in \( \mathcal{M}_d^2(K) \). Points in \( \mathcal{M}_d^2(K) \) are the same as PGL\(_{n+1}(K)\)-conjugacy classes of endomorphisms defined over \( K \); denote these classes by \([\varphi_1], \ldots, [\varphi_r]\) for endomorphisms \( \varphi_i \) of degree \( d \) on \( \mathbb{P}^n \) defined over \( K \). Each PGL\(_{n+1}(K)\)-conjugacy class which descends to some \([\varphi_i]\) is called a twist. A priori, it is not obvious how many twists over \( K \) descend to each \([\varphi_i]\). Indeed, if the automorphism group of \( \varphi_i \), which consists of the finite subgroup of PGL\(_{n+1}(\overline{K})\) that fixes \( \varphi_i \) under conjugation, is trivial, then there is only one twist. This need not be the case in general. For an example where there are infinitely many twists one can consider quadratic rational maps on \( \mathbb{P}^1 \) of the following form

\[
\varphi_b(z) = z + \frac{b}{z}
\]

where \( b \in K^* \). All \( \varphi_b \) are \( K \)-isomorphic and therefore descend to the point \([\varphi_1]\) in \( \mathcal{M}_2 \). However, \( \varphi_b \) and \( \varphi_c \) are \( K \)-isomorphic if and only if \( b/c \) is a square in \( K \). If we denote the set of twists of \( \varphi_1 \) by \( \text{Twist}(\varphi_1/K) \), then this gives an injective map \( K^*/K^{*2} \to \text{Twist}(\varphi_1/K) \) by \( b \mapsto [\varphi_b]_K \). See example 4.71 in [2] for more details. For a number field \( K^*/K^{*2} \) is infinite (for example, over \( \mathbb{Q} \) this set contains all the primes), so it follows that bounding the height \( h(\langle \varphi \rangle) \) is not enough to guarantee a finiteness result.

Acknowledgements Both authors would like to thank Tom Tucker for reading this paper and his helpful comments, and the referee for several helpful comments.

2. Preliminaries

2.1. The spaces \( \text{Hom}_d^2 \) and \( \mathcal{M}_d^2 \). Let \( K \) be a number field and \( \overline{K} \) be a fixed algebraic closure. By assumption, varieties and morphisms
will be defined over $\overline{K}$. When we wish to emphasize a special field of definition, we will use the notation $\mathbb{P}^n(K)$. Let
\[ \text{Hom}_d^n = \{ \varphi : \mathbb{P}^n \to \mathbb{P}^n \text{ is a degree } d \text{ morphism} \} . \]

By degree we mean algebraic degree. We will see that $\text{Hom}_d^n$ is a variety over $\overline{K}$ and that $K$-rational points correspond to morphisms of degree $d$ on $\mathbb{P}^n$ defined over $K$. Equivalently, points of $\text{Hom}_d^n(K)$ correspond to endomorphism $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ of algebraic degree $d$ defined over $\overline{K}$.

After fixing a basis $X_0, \ldots, X_n$ of $\mathbb{P}^n$, any morphism $\varphi \in \text{Hom}_d^n$ can be written as $\varphi = [\varphi_0, \ldots, \varphi_n]$, where each $\varphi_i$ is a degree $d$ homogeneous polynomial in the $X_i$, and $\varphi_0, \ldots, \varphi_n$ have no non-trivial common zeros over the algebraic closure $\overline{K}$. Each $\varphi_i$ can be written as
\[ \varphi_i = \sum_I a_I X^I \]
with multi-index $I$. Here, $I = (i_0, \ldots, i_n)$ and $i_0 + \cdots + i_n = d$ and $X^I = X_0^{i_0} \cdots X_n^{i_n}$. We order these monomials using the lexicographic ordering. Thus, if $N = \binom{n+d}{n} (n+1)-1$ is the number of monomials $X^I$ then we can identify any $\varphi \in \text{Hom}_d^n$ with a point in $\mathbb{P}^N$ via the association $\varphi \mapsto [a_I] \in \mathbb{P}^N$. It follows that $\text{Hom}_d^n(K) \subseteq \mathbb{P}^N(K)$.

**Theorem 2** (Theorem 1.8 in [3]). There exists a geometrically irreducible polynomial $\text{Res} \in \mathbb{Z}[a_i]$ in the coefficients of $\varphi$ such that
\[ \varphi \in \text{Hom}_d^n \iff \text{Res}(\varphi) \neq 0. \]

The polynomial $\text{Res}$ is called the Macaulay resultant of $\varphi$. We remark that we abuse notation above. Let $\Phi$ be an choice of the coordinates of the projective point defined by $\varphi$. If $\Psi$ is another choice, then $\Phi = \lambda \Psi$ some $\lambda \in \overline{K}$. It follows from elementary properties of Macaulay resultant that $\text{Res}(\Phi) = \lambda^{(n+1)d} \text{Res}(\Psi)$. Therefore, only the vanishing of $\text{Res}$ on $\mathbb{P}^N$ is well defined. It is multi-homogeneous in the coefficients of the $\varphi_i$. This implies that $\text{Hom}_d^n$ is an affine variety. Specifically, $\text{Hom}_d^n = \mathbb{P}^N - V(\text{Res})$. For further discussion and proof of these facts regarding the Macaulay resultant see [1].

The automorphism group $\text{Aut}(\mathbb{P}^n) = \text{PGL}_{n+1}(\overline{K})$ acts on $\text{Hom}_d^n$, and on $\text{Rat}_d^n$ (the set of rational functions from $\mathbb{P}^n$ to itself) via the action of conjugation, indeed it acts on the entire space $\mathbb{P}^N$; for $\varphi \in \text{Hom}_d^n$ and $f \in \text{PGL}_{n+1}(\overline{K})$, $\varphi' = f^{-1} \circ \varphi \circ f$. It follows from the properties of the resultant that $\varphi \in \text{Hom}_d^n \iff \varphi' \in \text{Hom}_d^n$, so $\text{Hom}_d^n$ is a $\text{PGL}_{n+1}(\overline{K})$-stable subset for the action of this group on $\mathbb{P}^N$. We then define the moduli space $M_d^n$ to be the set of all conjugacy classes of endomorphisms of $\mathbb{P}^n$, that is
\[ M_d^n = \text{Hom}_d^n / \text{PGL}_{n+1}(\overline{K}) . \]
For any $\varphi \in \text{Hom}^n_d$ we denote its image in $\mathcal{M}^n_d$ by $\langle \varphi \rangle$. It follows from Geometric Invariant Theory that $\mathcal{M}^n_d$ exists as an affine variety (see section 2.3 in [3]).

By picking an appropriate $M$ the moduli space $\mathcal{M}^n_d$ can be embedded into $\mathbb{P}^M$. It follows from Theorems 2.24 and 2.26 in [3] that there exists a projective variety $\mathcal{M}^n_{d,ss}$, the moduli space of semi-stable dynamical systems on $\mathbb{P}^n$. The variety $\mathcal{M}^n_{d,ss}$ exists as the quotient of the semi-stable locus for the $\text{PGL}_{n+1}(\bar{K})$ action on $\mathbb{P}^N$ and it follows that $\mathcal{M}^n_d \subset \mathcal{M}^n_{d,ss}$ is a dense open subset. As $\mathcal{M}^n_{d,ss}$ is projective, it embeds into some $\mathbb{P}^M$ as does $\mathcal{M}^n_d$ by the inclusion $\mathcal{M}^n_d \hookrightarrow \mathcal{M}^n_{d,ss} \hookrightarrow \mathbb{P}^M$. We can therefore define a height function $h_{\mathcal{M}^n_d}$ on $\mathcal{M}^n_d$ by taking the height of the image of $\langle \varphi \rangle$ in $\mathbb{P}^M$. We will denote this height function by $h$.

2.2. Minimal Resultants. Following [3] we now use the Macaulay resultant to define the minimal resultant of an endomorphism.

Let $R$ be a discrete valuation ring with discrete valuation $v$ and field of fractions $F$. If $\varphi = [\varphi_1, \ldots, \varphi_n] \in \text{Hom}^n_d(F)$ then we define

$$e_v(\varphi) = v(\text{Res}(\varphi)) - (n + 1) d^n \min_{0 \leq i \leq n} v(\varphi_i).$$

Where $v(\varphi_i)$ is taken to be the minimal valuation of the coefficients of $\varphi_i$. We remark that $e_v(\varphi)$ is well defined. Let $\Phi, \Psi$ be affine models of $\varphi$ and $\lambda \in F^\times$ such that $\Phi = \lambda \Psi$. Then $v(\text{Res}(\Phi)) = v(\text{Res}(\lambda \Psi) = v(\lambda^{(n+1)d^n} \text{Res}(\Psi)) = (n + 1)d^n v(\lambda) + v(\text{Res}(\Psi))$ Similarly,

$$\min_{0 \leq i \leq n} v(\Phi_i) = \min_{0 \leq i \leq n} v(\lambda \Psi_i) = v(\lambda) + \min_{0 \leq i \leq n} v(\Psi_i)$$

It follows that $e_v(\varphi)$ is independent of choice of affine model used to compute it.

The quantity $e_v(\varphi)$ is then used to define the exponent of the minimal discriminant of $\varphi$ by:

**Definition 3.**

$$\varepsilon_v(\varphi) = \min_{f \in \text{PGL}_{n+1}(K)} e_v(\varphi^f).$$

A fact that will be important in our proof of Theorem 1 is the following:

**Proposition 4.** $\varphi$ has good reduction if and only if $\varepsilon_v(\varphi) = 0$.

**Proof.** See proposition 3.11 in [3].

Now let $R$ be a Dedekind domain with field of fractions $K$. If $v$ is a discrete valuation on $R$ then we denote the prime ideal associated to $v$ by $p_v$.  

Definition 5. For an endomorphism \( \varphi \in \text{Hom}_d^n(K) \) the \textit{minimal resultant} of \( \varphi \) is

\[
\mathfrak{R}_\varphi = \prod_v \mathfrak{p}_v^{\varepsilon_v(\varphi)}.
\]

Where the product is taken over all of the inequivalent valuations on \( R \).

It is clear that this is an ideal of \( R \) as any morphism \( \varphi \) has only finitely many primes of bad reduction. It follows from Proposition 4 that \( \varepsilon_v(\varphi) = 0 \) for all but finitely many \( v \).

2.3. Twists. Two morphisms \( \varphi, \psi \in \text{Hom}_d^n(K) \) are \( \bar{K} \)-isomorphic if there is an \( f \in \text{PGL}_{n+1}(\bar{K}) \) such that \( \varphi = \psi^f \), that is if \( \langle \varphi \rangle = \langle \psi \rangle \). We denote this set of \( \bar{K} \)-isomorphic morphisms as

\[
[\varphi] = \{ \psi \in \text{Hom}_d^n(K) : \psi = \varphi^f \text{ for some } f \in \text{PGL}_{n+1}(\bar{K}) \}.
\]

If we restrict our automorphisms to those defined over \( K \) we get a second set

\[
[\varphi]_K = \{ \psi \in \text{Hom}_d^n(K) : \psi = \varphi^f \text{ for some } f \in \text{PGL}_{n+1}(K) \}.
\]

The twists of \( \varphi \) are the \( K \)-isomorphism classes of \( \varphi \) which are \( \bar{K} \)-isomorphic.

\[
\text{Twist}_K(\varphi) = \{ [\psi]_K : \psi \in \text{Hom}_d^n(K) \text{ and } [\psi] = [\varphi] \}.
\]

One can interpret twists in terms of moduli spaces. A \( \bar{K} \)-isomorphism class for \( \varphi \) defined over \( K \) corresponds to a \( K \)-rational point of \( \mathcal{M}_d^n \). One can also consider the quotient variety

\[
\mathcal{M}_{d,K}^n = \text{Hom}_d^n(K)/\text{PGL}_{n+1}(K)
\]

and a \( K \)-isomorphism class \([\varphi]_K\) corresponds to a \( K \)-rational point of this space. The natural inclusion \( \text{PGL}_{n+1}(K) \hookrightarrow \text{PGL}_{n+1}(\bar{K}) \) induces a map on the quotients \( \mathcal{M}_{d,K}^n \to \mathcal{M}_d^n \). Fibers of this morphism over the \( K \)-rational point \([\varphi]\) are twists.

In [4], the first author proved the following theorem which is central in our proof of [1].

Theorem 6. Let \( \varphi \in \text{Hom}_d^n(K) \) for \( d \geq 2 \), and let \( S \) be a finite set of places containing the archimedean places. If

\[
\mathcal{V}(S) = \{ [\psi]_K \in \text{Twist}_K(\varphi) : [\psi]_K \text{ has good reduction outside } S \},
\]

then \( \mathcal{V}(S) \) is finite.
3. Bounded height and resultant

Let $h$ denote a fixed height on $\mathcal{M}_d^n$ corresponding to some embedding $\mathcal{M}_d^n \to \mathbb{P}^M$. Let $K$ denote a fixed number field; we assume all $\varphi$ are defined over $K$.

**Lemma 7.** Let $d \geq 1$ be an integer and $B \geq 1$. The set

$$\mathcal{W} = \{\langle \varphi \rangle | \varphi \in \text{Hom}_d^n(K) \text{ and } h(\langle \varphi \rangle) \leq B \} \subset \mathcal{M}_d^n$$

is finite.

**Proof.** We claim that this set is a set of bounded height and degree in $\mathcal{M}_d^n$. First, every $\varphi \in \mathcal{W}$ is a $K$-rational point of $\mathcal{M}_d^n$. This follows from the assumption that $\varphi$ is defined over $K$. Therefore, it is a $K$-rational point of $\text{Hom}_d^n$. It follows via the quotient map $\text{Hom}_d^n \to \mathcal{M}_d^n$ that $\varphi$ corresponds to a $K$-rational point of $\mathcal{M}_d^n$. Hence, $\mathcal{W}$ is a set of bounded degree. By the assumption that each $\varphi \in \mathcal{W}$ satisfies $h(\langle \varphi \rangle) \leq B$ we have that $\mathcal{W}$ is a set of bounded height. By the theorem of Northcott (Theorem 3.7 of [2]), such sets of bounded degree and height are finite. \qed

We remark that this does not prove our main theorem, as this shows that $\Gamma$ is contained in finitely many $\text{PGL}_{n+1}(\overline{K})$ conjugacy classes. We make the following definition based on the requirement that the resultant is bounded.

**Definition 8.** Let $B \geq 1$. We define the set of primes $S_B$ of $K$ in the following way

$$S_B = \{ p | N_{K/Q}(p) \leq B \}$$

**Lemma 9.** Let $B \geq 1$. Then the set $S_B$ of primes of $K$ is finite.

**Proof.** There are only finitely many primes $p$ of $\mathbb{Z}$ such that $p \leq B$. It follows from the property of the norm that

$$N_{K/Q}(p) = \prod_{p|p} p^{[K/Q]}$$

and the fact that only finitely many primes $p$ lie over $p$ that $S_B$ is finite. \qed

**Lemma 10.** Let $\Gamma_{K,B}$ be the set from Theorem 7. If $\varphi \in \Gamma_{K,B}$, then $\varphi$ has good reduction at all primes $p \notin S_B$.

**Proof.** Let $\varphi \in \Gamma_{K,B}$ and $p \notin S_B$. By definition of the set $S_B$, we have that $N_{K/Q}(p) > B$. By Proposition 4 $\varphi$ has bad reduction at $p$ if and only if $p | R_{\varphi}$. If $\varphi$ has bad reduction at $p$, then $R_{\varphi} = pa$ and hence

$$N_{K/Q}(R_{\varphi}) = N_{K/Q}(p)N_{K/Q}(a) > BN_{K/Q}(a) > B.$$ 

This is contrary to
the assumption that $\varphi \in \Gamma_{K,B}$. It follows that $\varphi$ has good reduction at $p$. □

**Remark 1.** $S_B$ may contain some primes at which $\varphi$ has good reduction. Consider, for example, an endomorphism defined over $\mathbb{Q}$ with minimal resultant $R_\varphi = (2)^3$. Then $S_B = \{2, 3, 5, 7\}$ even though $\varphi$ has bad reduction only at 2.

We now prove theorem 1.

**Proof.** It follows from Lemma 7 that $\Gamma$ descends to only finitely many point in $\mathcal{M}_d^n(K)$, i.e. that $W = \pi(\Gamma)$ is finite under the image of the quotient map $\pi : \text{Hom}_d^n(K) \to \mathcal{M}_d^n(K)$.

Let $V$ be the set of $K$-conjugacy classes of maps in $\Gamma$. It follows that $V \subset \mathcal{M}_d^n,K$ and that under $\theta : \mathcal{M}_d^n,K \to \mathcal{M}_d^n \hat{\to} \mathcal{W}$. By definition, the $K$-conjugacy classes of $V$ consist of all twists lying over the finitely many $\hat{K}$-conjugacy classes in $\mathcal{W}$. If $V$ is infinite, then by the pigeonhole principle there is at least one $\hat{K}$-conjugacy class which contains infinitely many $K$-conjugacy classes. Denote this $\hat{K}$-conjugacy class by $[\psi]$ and the infinitely many distinct $K$-conjugacy classes by $[\psi_i]_{K}$ for $i = 0, 1, \ldots$ where $[\psi_i] = [\psi]$ for all $i$. It follows that each $[\psi_i]_K$ is a twist of $[\psi]$.

By Lemma 9 the set $S_B$ is finite and by Lemma 10 we see that each $[\psi_i]_K$ must have good reduction outside of $S_B$. Thus we have constructed an infinite set of twists $[\psi_i]_K$ of $[\psi]$ with good reduction outside of $S_B$ which contradicts Theorem 6. This concludes the proof of the main theorem. □

**References**

[1] David A. Cox, John B. Little, and Don O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, NY, 2nd edition, 1996. 536 pages.

[2] Joseph H. Silverman. *The Arithmetic of Dynamical Systems*, volume 241 of Graduate Texts in Mathematics. Springer, New York, 2007.

[3] Joseph H. Silverman. *Moduli spaces and arithmetic dynamics*, volume 30 of CRM Monograph Series. American Mathematical Society, Providence, RI, 2012.

[4] Brian Stout. A dynamical Shafarevich theorem for twists of rational morphisms. *arXiv:1308.4992 [math.NT]*, 2013.

BRIAN STOUT; DEPARTMENT OF MATHEMATICS; UNITED STATES NAVAL ACADEMY; ANNAPOLIS, MD 21401 U.S.A.

E-mail address: stout@usna.edu

ADAM TOWSELY; DEPARTMENT OF MATHEMATICS; THE CITY UNIVERSITY OF NEW YORK GRADUATE CENTER; NEW YORK, NY 10016 U.S.A.

E-mail address: atowsley@gc.cuny.edu