Effective Multiplicative Dependence in Orbits of Polynomial Functions

Ray Li
Joint with Prof. Igor Shparlinski

October 1, 2019

Definitions

- $\mathbb{K}$ denotes a number field, $\mathfrak{o}_{\mathbb{K}}$ the ring of integers.

Definitions

- $\mathbb{K}$ denotes a number field, $\mathfrak{o}_{\mathbb{K}}$ the ring of integers.
- $f^{(n)}$ will denote the function $\underbrace{f \circ \cdots \circ f}_{n \text{ times}}$ (where $f : \mathbb{K} \to \mathbb{K}$).

Definitions

- $\mathbb{K}$ denotes a number field, $\mathfrak{o}_{\mathbb{K}}$ the ring of integers.
- $f^{(n)}$ will denote the function $\underbrace{f \circ \cdots \circ f}_{n \text{ times}}$ (where $f : \mathbb{K} \to \mathbb{K}$).

Classification of points

- Periodic: There exists a $n \in \mathbb{Z}^+$ such that $f^{(n)}(\alpha) = \alpha$.

Definitions

- $\mathbb{K}$ denotes a number field, $\mathfrak{o}_{\mathbb{K}}$ the ring of integers.
- $f^{(n)}$ will denote the function $\underbrace{f \circ \cdots \circ f}_{n \text{ times}}$ (where $f : \mathbb{K} \to \mathbb{K}$).

Classification of points

- Periodic: There exists a $n \in \mathbb{Z}^{+}$ such that $f^{(n)}(\alpha) = \alpha$.
- Preperiodic: There exists $m > n \geq 0$ such that $f^{(m)}(\alpha) = f^{(n)}(\alpha)$.

Definitions

- $\mathbb{K}$ denotes a number field, $\mathfrak{o}_{\mathbb{K}}$ the ring of integers.
- $f^{(n)}$ will denote the function $\underbrace{f \circ \cdots \circ f}_{n \text{ times}}$ (where $f : \mathbb{K} \to \mathbb{K}$).

Classification of points

- Periodic: There exists a $n \in \mathbb{Z}^+$ such that $f^{(n)}(\alpha) = \alpha$.
- Preperiodic: There exists $m > n \geq 0$ such that $f^{(m)}(\alpha) = f^{(n)}(\alpha)$.
- Wandering: All values in the orbit are distinct. Denoted $\mathrm{Wander}_{\mathbb{K}}(f)$.

Definitions

- $\mathbb{K}$ denotes a number field, $\mathfrak{o}_{\mathbb{K}}$ the ring of integers.
- $f^{(n)}$ will denote the function $\underbrace{f \circ \cdots \circ f}_{n \text{ times}}$ (where $f : \mathbb{K} \to \mathbb{K}$).

Classification of points

- Periodic: There exists a $n \in \mathbb{Z}^{+}$ such that $f^{(n)}(\alpha) = \alpha$.
- Preperiodic: There exists $m > n \geq 0$ such that $f^{(m)}(\alpha) = f^{(n)}(\alpha)$.
- Wandering: All values in the orbit are distinct. Denoted $\mathrm{Wander}_{\mathbb{K}}(f)$.

Theorem (Northcott, (1950))

Let $f(X) \in \mathbb{K}(X)$ be a rational function of degree at least 2. Then the number of preperiodic points in $\mathbb{K}$ is finite. Furthermore, the size of this set can be effectively bounded.

Multiplicative Dependence

How about other kinds of dependence within an orbit?

Multiplicative Dependence

How about other kinds of dependence within an orbit?

Definition

Let Γ be a finitely generated subgroup of $\mathbb{K}^*$. We will say x and y are multiplicatively dependent modulo Γ if there exists $(r,s) \neq (0,0) \in \mathbb{Z}^2$ such that

$$x^r = uy^s$$

for some $u \in \Gamma$.

Multiplicative Dependence

How about other kinds of dependence within an orbit?

Definition

Let Γ be a finitely generated subgroup of $\mathbb{K}^*$. We will say x and y are multiplicatively dependent modulo Γ if there exists $(r, s) \neq (0, 0) \in \mathbb{Z}^2$ such that

$$x^r = uy^s$$

for some $u \in \Gamma$.

(slightly abbreviated form)

Theorem (Bérczes, Ostafe, Shparlinski, and Silverman, ())

Let $f \in \mathbb{K}[X]$ be a polynomial without multiple roots of degree $d \geq 3$ and for which 0 is not periodic. Let $\Gamma \subset \mathbb{K}^*$ be a finitely generated subgroup. Then, there are only finitely many elements $\alpha \in \mathbb{K}$ such that for some distinct integers $m, n \geq 0$ the values $f^{(m)}(\alpha)$ and $f^{(n)}(\alpha)$ are multiplicatively dependent modulo Γ.

Heights

Define:

- $M_{\mathbb{K}}$ for the set of places of $\mathbb{K}$. $M_{\mathbb{K}}^{\infty}$ for the infinite places, $M_{\mathbb{K}}^{0}$ for the finite places.

Heights

Define:

- $M_{\mathbb{K}}$ for the set of places of $\mathbb{K}$. $M_{\mathbb{K}}^{\infty}$ for the infinite places, $M_{\mathbb{K}}^{0}$ for the finite places.
- Height:

$$h(\alpha) := \sum_{v \in M_{\mathbb{K}}} \frac{l_v}{[\mathbb{K} : \mathbb{Q}]} \log^{+}(|\alpha|_v)$$

  where $|\alpha|_v$ is the valuation extending the one on $\mathbb{Q}$ and $l_v := e_v f_v$ denotes the local degree.

Heights

Define:

- $M_{\mathbb{K}}$ for the set of places of $\mathbb{K}$. $M_{\mathbb{K}}^{\infty}$ for the infinite places, $M_{\mathbb{K}}^{0}$ for the finite places.
- Height:

$$h(\alpha) := \sum_{v \in M_{\mathbb{K}}} \frac{l_v}{[\mathbb{K} : \mathbb{Q}]} \log^+(|\alpha|_v)$$

  where $|\alpha|_v$ is the valuation extending the one on $\mathbb{Q}$ and $l_v := e_v f_v$ denotes the local degree.
- E.g: $h(1/1000) = \log 1000$. Measures "complexity"

Heights

Define:

- $M_{\mathbb{K}}$ for the set of places of $\mathbb{K}$. $M_{\mathbb{K}}^{\infty}$ for the infinite places, $M_{\mathbb{K}}^{0}$ for the finite places.
- Height:

$$h(\alpha) := \sum_{v \in M_{\mathbb{K}}} \frac{l_v}{[\mathbb{K} : \mathbb{Q}]} \log^+(|\alpha|_v)$$

  where $|\alpha|_v$ is the valuation extending the one on $\mathbb{Q}$ and $l_v := e_v f_v$ denotes the local degree.
- E.g: $h(1/1000) = \log 1000$. Measures "complexity"

Properties:

- For any C, the set $\{x \in \mathbb{K} \mid h(x) < C\}$ is finite.
- There exists an effectively computable constant $C_1(f)$ independent of α such that

$$d \cdot h(\alpha) - C_1(f) \leq h(f(\alpha)) \leq d \cdot h(\alpha) + C_1(f)$$

- For all $n \in \mathbb{Z}$, $h(\alpha^n) = n \cdot h(\alpha)$. In particular, $h(\alpha^{-1}) = h(\alpha)$.

Canonical Height associated with f

$$\hat{h}_f(\alpha) := \lim_{n\to\infty} d^{-n} h(f^{(n)}(\alpha))$$

Canonical Height associated with f

$$\hat{h}_f(\alpha) := \lim_{n\to\infty} d^{-n} h(f^{(n)}(\alpha))$$

- $\hat{h}_f(f(\alpha)) = d\hat{h}_f(\alpha)$
- There exists an effectively computable constant $C_1(f)$ independent of α such that
$$|\hat{h}_f(\alpha) - h_f(\alpha)| < C_1(f)$$

T ideals and T heights

Define

- Let $T = \{\mathbf{p}_1, \ldots, \mathbf{p}_t\}$. Define

$$\langle \alpha \rangle_T := \prod_{\mathbf{p}_i \in T} \mathbf{p_i}^{\mathrm{ord}_{\mathbf{p_i}} \alpha}$$

T ideals and T heights

Define

- Let $T = \{\mathbf{p}_1, \ldots, \mathbf{p}_t\}$. Define

$$\langle \alpha \rangle_T := \prod_{\mathbf{p}_i \in T} \mathbf{p_i}^{\mathrm{ord}_{\mathbf{p_i}} \alpha}$$

- Hence, if $\langle \alpha \rangle = \mathbf{p_1}^{a_1} \cdots \mathbf{p_t}^{a_t} \mathbf{b}$, then $\langle \alpha \rangle_{M_{\mathbb{K}} \setminus T} = \mathbf{b}$.

T ideals and T heights

Define

- Let $T = \{\mathbf{p}_1, \ldots, \mathbf{p}_t\}$. Define

$$\langle \alpha \rangle_T := \prod_{\mathbf{p}_i \in T} \mathbf{p_i}^{\mathrm{ord}_{\mathbf{p_i}} \alpha}$$

- Hence, if $\langle \alpha \rangle = \mathbf{p_1}^{a_1} \cdots \mathbf{p_t}^{a_t} \mathbf{b}$, then $\langle \alpha \rangle_{M_{\mathbb{K}} \setminus T} = \mathbf{b}$.
- Let $T \subseteq M_{\mathbb{K}}$. Define the T-height

$$h_T(\alpha) := \sum_{v \in T} \frac{l_v}{[\mathbb{K} : \mathbb{Q}]} \log^+(|\alpha|_v)$$

Sketch of BOSS for $r = s = 1$

$$f^{(n+k)}(\alpha) = uf^{(k)}(\alpha), \quad u \in R_S^*$$

Sketch of BOSS for $r = s = 1$

$$f^{(n+k)}(\alpha) = uf^{(k)}(\alpha), \quad u \in R_S^*$$

implies

$$d^n \hat{h}_f(f^{(k)}(\alpha)) = \hat{h}_f(u \cdot f^{(k)}(\alpha))$$

Sketch of BOSS for $r = s = 1$

$$f^{(n+k)}(\alpha) = uf^{(k)}(\alpha), \quad u \in R_S^*$$

implies

$$d^n \hat{h}_f(f^{(k)}(\alpha)) = \hat{h}_f(u \cdot f^{(k)}(\alpha))$$

however

$$\begin{aligned} h_{M_{\mathbb{K}} \setminus S}(f^{(n+k)}(\alpha)) &= h_{M_{\mathbb{K}} \setminus S}(u \cdot f^{(k)}(\alpha)) \\ &= h_{M_{\mathbb{K}} \setminus S}(f^{(k)}(\alpha)) \end{aligned}$$

Sketch of BOSS for $r = s = 1$

$$f^{(n+k)}(\alpha) = uf^{(k)}(\alpha), \quad u \in R_S^*$$

implies

$$d^n \hat{h}_f(f^{(k)}(\alpha)) = \hat{h}_f(u \cdot f^{(k)}(\alpha))$$

however

$$\begin{aligned} h_{M_{\mathbb{K}} \setminus S}(f^{(n+k)}(\alpha)) &= h_{M_{\mathbb{K}} \setminus S}(u \cdot f^{(k)}(\alpha)) \\ &= h_{M_{\mathbb{K}} \setminus S}(f^{(k)}(\alpha)) \end{aligned}$$

and

$$\begin{aligned} h_{M_{\mathbb{K}} \setminus S}(f^{(n+k)}(\alpha)) &\leq h(f^{(k)}(\alpha)) \\ &\leq \frac{1}{d^n} h(f^{(n+k)}(\alpha)) + C \end{aligned}$$

as well as

$$h_S(f^{(n+k)}(\alpha)) \geq \frac{d^n - 1}{d^n} h(f^{(n+k)}(\alpha)) - C$$

Sketch of BOSS for $r = s = 1$

Look instead at

$$h_S(f^{(n+k)}(\alpha)^{-1})$$

If we were working in $\mathbb{Z}$ then

$$h_S(f^{(n+k)}(\alpha)^{-1}) \approx \log([f^{(n+k)}(\alpha)]_S)$$

Sketch of BOSS for $r = s = 1$

Look instead at

$$h_S(f^{(n+k)}(\alpha)^{-1})$$

If we were working in $\mathbb{Z}$ then

$$h_S(f^{(n+k)}(\alpha)^{-1}) \approx \log([f^{(n+k)}(\alpha)]_S)$$

Question

For a fixed $\varepsilon > 0$ is the set of α such that

$$h_S(f(\alpha)^{-1}) \geq \varepsilon h(f(\alpha))$$

finite?

Dynamical Diophantine result

Lemma (Hsia and Silverman, (2011))

Let $\alpha \in \mathrm{Wander}_{\mathbb{K}}(f)$*. Assume that* 0 *is not an exceptional point for* f*. Let* S *be a finite set of places of* $\mathbb{K}$*, and let* $1 \geq \varepsilon > 0$*. Then there is a constant* $C_3(\mathbb{K}, S, f, \varepsilon)$ *such that*

$$\max\left\{n \in \mathbb{Z}_{\geq 0} : h_S(f^{(n)}(\alpha)^{-1}) \geq \varepsilon \hat{h}_f(f^{(n)}(\alpha))\right\} \leq C_3(\mathbb{K}, S, f, \varepsilon)$$

Dynamical Diophantine result

Lemma (Hsia and Silverman, (2011))

Let $\alpha \in \mathrm{Wander}_{\mathbb{K}}(f)$. Assume that 0 is not an exceptional point for f. Let S be a finite set of places of $\mathbb{K}$, and let $1 \geq \varepsilon > 0$. Then there is a constant $C_3(\mathbb{K}, S, f, \varepsilon)$ such that

$$\max\left\{n \in \mathbb{Z}_{\geq 0} : h_S(f^{(n)}(\alpha)^{-1}) \geq \varepsilon \hat{h}_f(f^{(n)}(\alpha))\right\} \leq C_3(\mathbb{K}, S, f, \varepsilon)$$

So for $n + k$ sufficiently large and $\varepsilon = 1/3, d \geq 2$ we get

$$\begin{aligned} h(f^{(n+k)}(\alpha)) &= h_S(f^{(n+k)}(\alpha)^{-1}) + h_{M_{\mathbb{K}} \setminus S}(f^{(n+k)}(\alpha)^{-1}) \\ &\ll \varepsilon \hat{h}_f(f^{(n+k)}(\alpha)) + h(f^{(k)}(\alpha)) \\ &\ll \varepsilon h(f^{(n+k)}(\alpha)) + 1/d^n \hat{h}_f(f^{(n+k)}(\alpha)) + 1 \\ &\ll 5/6 \cdot h(f^{(n+k)}(\alpha)) + 1 \end{aligned}$$

Sketch of BOSS for $r = s = 1$

Now suppose $n + k$ is bounded, hence fixed. We get

$$f^{(n+k)}(\alpha)/f^{(k)}(\alpha) \in R_S^*$$

Sketch of BOSS for $r = s = 1$

Now suppose $n + k$ is bounded, hence fixed. We get

$$f^{(n+k)}(\alpha)/f^{(k)}(\alpha) \in R_S^*$$

Take a suff. large N. Then since $R_S^*/(R_S^*)^N$ is finite, there is some unit u for which there are infinite solutions to

$$r(\alpha) = uY^N$$

Contradicts Faltings's!

Theorem (Faltings, (1983))

For any curve of genus ≥ 2, there are finitely many points defined over $\mathbb{K}$.

Sketch of BOSS for $r = s = 1$

Now suppose $n + k$ is bounded, hence fixed. We get

$$f^{(n+k)}(\alpha)/f^{(k)}(\alpha) \in R_S^*$$

Take a suff. large N. Then since $R_S^*/(R_S^*)^N$ is finite, there is some unit u for which there are infinite solutions to

$$r(\alpha) = uY^N$$

Contradicts Faltings's!

Theorem (Faltings, (1983))

For any curve of genus ≥ 2, there are finitely many points defined over $\mathbb{K}$.

Problem: Entirely ineffective for getting a bound on $h(\alpha)$.

Effective Diophantine Approximation Result

Over $\mathbb{Z}$:

Lemma (Gross and Vincent, (2013))

Let $[n]_S$ denote the S part of n.
Let $f(x) \in \mathbb{Z}[x]$ have at least two distinct roots and S be a finite set of rational primes.
Then for all $n \in \mathbb{Z}$, $n \neq 0$, n not a root of $f(x)$, we have

$$[f(n)]_S < c_5 |n|^{\deg(f) - c_6}$$

where c_5, c_6 are positive, effectively computable constants depending only on f and S

Decomposable Forms

Lemma (Győry and Yu, (2006))

Let $F \in \mathbb{K}[X_1, \ldots, X_m]$ *be a triangularly connected decomposable form over* $\mathbb{K}$*. Let* $\beta \in \mathbb{K} \setminus \{0\}$*. Then all solutions* $\mathbf{x} = (x_1, \ldots, x_m) \in \mathfrak{o}_{\mathbb{K}}^m$ *of*

$$F(\mathbf{x}) = \beta$$

satisfy

$$h(x_1), \ldots, h(x_m) \ll_{\mathbb{K},F,S} 1 + h(\beta)$$

where the constant in $\ll_{\mathbb{K},F,S}$ *can be made explicit.*

For $m = 2$, if F has at least three pairwise non-proportional linear factors then F is triangularly connected.

Effective Diophantine Approximation Result

Lemma (Bugeaud, Evertse, and Györy, (2018))

Let $f(X) \in \mathbb{Z}[X]$ be a polynomial with at least three distinct roots and suppose that its splitting field has degree D over $\mathbb{Q}$. Let $S = \{p_1, \ldots, p_s\}$ be a finite set of primes. Then there exists an effectively computable positive constant $c(f)$ depending only on f such that for any integer n with $|n| > c(f)$ we have

$$[f(n)]_S \geq c(f)^{-1}|f(n)|^{\kappa}$$

where

$$\kappa = \frac{1}{c(f)^s(PQ)^D},$$

and

$$P = \max(p_1, \ldots, p_s) Q = \prod_{i=1}^{s} \log p_i.$$

Proof sketch of BEG

Proof.

Let $F(X,Y) := Y^n f(X)$, the homogenization.
Suppose $f(x) = F(x,1) = \beta = bp_1^{a_1} \cdots p_s^{a_s}$.
For all i, let $a_i := na_i' + a_i''$.

Proof sketch of BEG

Proof.

Let $F(X, Y) := Y^n f(X)$, the homogenization.
Suppose $f(x) = F(x, 1) = \beta = bp_1^{a_1} \cdots p_s^{a_s}$.
For all i, let $a_i := na_i' + a_i''$.
Then

$$F(x/p_1^{a_1'} \cdots p_s^{a_s'}, 1/p_1^{a_1'} \cdots p_s^{a_s'}) = bp_1^{a_1''} \cdots p_s^{a_s''}$$

Proof sketch of BEG

Proof.

Let $F(X, Y) := Y^n f(X)$, the homogenization.
Suppose $f(x) = F(x, 1) = \beta = bp_1^{a_1} \cdots p_s^{a_s}$.
For all i, let $a_i := na_i' + a_i''$.
Then

$$F(x/p_1^{a_1'} \cdots p_s^{a_s'}, 1/p_1^{a_1'} \cdots p_s^{a_s'}) = bp_1^{a_1''} \cdots p_s^{a_s''}$$

But

$$h(1/p_1^{a_1'} \cdots p_s^{a_s'}) \approx \frac{1}{n} \log[\beta]_S$$

while

$$h(bp_1^{a_1''} \cdots p_s^{a_s''}) \approx \log|b| = \log(|\beta|/[\beta]_S)$$

Proof sketch of BEG

Proof.

Let $F(X,Y) := Y^n f(X)$, the homogenization.
Suppose $f(x) = F(x,1) = \beta = bp_1^{a_1} \cdots p_s^{a_s}$.
For all i, let $a_i := na_i' + a_i''$.
Then

$$F(x/p_1^{a_1'} \cdots p_s^{a_s'}, 1/p_1^{a_1'} \cdots p_s^{a_s'}) = bp_1^{a_1''} \cdots p_s^{a_s''}$$

But

$$h(1/p_1^{a_1'} \cdots p_s^{a_s'}) \approx \frac{1}{n} \log[\beta]_S$$

while

$$h(bp_1^{a_1''} \cdots p_s^{a_s''}) \approx \log|b| = \log(|\beta|/[\beta]_S)$$

But F is decomposable. Hence, Győry and Yu, (2006) implies

$$[\beta]_S^{1/n} \ll C \cdot (|\beta|/[\beta]_S)^{C_2}$$

and simple rearranging concludes the proof. $\square$

Accounting for Archimedean places

Lemma

For every $\alpha \in \mathfrak{o}_K \setminus \{0\}$ *and for every integer* $n \geq 1$ *there exists an* $\varepsilon \in \mathfrak{o}_K^*$ *such that*

$$\left| \log(|\varepsilon^n \alpha|_{v_i}) - \frac{1}{d} \log(\mathrm{Nm}_{\mathbb{K}}(\alpha)) \right| \ll_{\mathbb{K}} n \tag{1}$$

for all $v_i \in M_K^\infty$.
Furthermore, the constant hidden by the $\ll_{\mathbb{K}}$ *notation can be made explicit.*

Accounting for Archimedean places

Lemma

For every $\alpha \in \mathfrak{o}_K \setminus \{0\}$ and for every integer $n \geq 1$ there exists an $\varepsilon \in \mathfrak{o}_K^*$ such that

$$\left| \log(|\varepsilon^n \alpha|_{v_i}) - \frac{1}{d} \log(\mathrm{Nm}_{\mathbb{K}}(\alpha)) \right| \ll_{\mathbb{K}} n \tag{1}$$

for all $v_i \in M_K^{\infty}$.
Furthermore, the constant hidden by the $\ll_{\mathbb{K}}$ notation can be made explicit.

Proof.

Let $\mathbf{v}$ be the column vector defined by

$$\mathbf{v}_i := \log(\mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}(\alpha)^{-l_{v_i}/d} |\alpha|_{v_i}^{l_{v_i}})$$

Accounting for Archimedean places

Lemma

For every $\alpha \in \mathfrak{o}_K \setminus \{0\}$ and for every integer $n \geq 1$ there exists an $\varepsilon \in \mathfrak{o}_K^*$ such that

$$\left| \log(|\varepsilon^n \alpha|_{v_i}) - \frac{1}{d} \log(\mathrm{Nm}_{\mathbb{K}}(\alpha)) \right| \ll_{\mathbb{K}} n \tag{1}$$

for all $v_i \in M_K^\infty$.
Furthermore, the constant hidden by the $\ll_{\mathbb{K}}$ notation can be made explicit.

Proof.

Let $\mathbf{v}$ be the column vector defined by

$$\mathbf{v}_i := \log(\mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}(\alpha)^{-l_{v_i}/d} |\alpha|_{v_i}^{l_{v_i}})$$

This vector sums up to 0. But by Dirichlet's Unit Theorem there is a unit with the same Archimedean valuations. □

Effective Diophantine Approximation over Number Fields

Theorem

Let $f(X) \in \mathfrak{o}_{\mathbb{K}}[X]$ be a polynomial with at least 3 distinct roots. Let S be a finite set of places of $\mathbb{K}$ containing all infinite places.
Then there exists effectively computable constants

$$0 < \varepsilon(f, \mathbb{K}, S) < 1$$

and

$$L(f, \mathbb{K}, S) > 0$$

dependent only on $f, \mathbb{K}, S$ such that

$$h_S(f(\alpha)^{-1}) < \varepsilon(f, \mathbb{K}, S) h(f(\alpha))$$

for all $\alpha \in \mathfrak{o}_{\mathbb{K}} \setminus \{0\}, h(\alpha) > L(f, \mathbb{K}, S)$.

Proof Sketch

Proof.

Define:

- We work in $\mathbb{L}$ a splitting field of f over $\mathbb{K}$.
- T the places of $\mathbb{L}$ lying over S.
- $F(X, Y) := Y^n f(X/Y)$, the homogenization of f.
- h the class number of $\mathbb{L}$.
- p_i be any generator of ${\mathbf{p_i}}^h$.

Proof Sketch

Proof.

Define:

- We work in $\mathbb{L}$ a splitting field of f over $\mathbb{K}$.
- T the places of $\mathbb{L}$ lying over S.
- $F(X, Y) := Y^n f(X/Y)$, the homogenization of f.
- h the class number of $\mathbb{L}$.
- p_i be any generator of ${\mathbf{p_i}}^h$.

Decomposition: If $\langle f(x)\rangle = \langle \beta \rangle = \mathbf{b}{\mathbf{p_1}}^{a_1} \cdots {\mathbf{p_t}}^{a_t}$ then letting $a_i = nha_i' + a_i''$ we have

$$\langle F(x/p_1^{a_i'} \cdots p_t^{a_t'}, 1/p_1^{a_1'} \cdots p_t^{a_t'})\rangle = \langle c \rangle := \mathbf{b}{\mathbf{p_1}}^{a_1''} \cdots {\mathbf{p_t}}^{a_t''}$$

Proof Sketch

Proof.

Define:

- We work in $\mathbb{L}$ a splitting field of f over $\mathbb{K}$.
- T the places of $\mathbb{L}$ lying over S.
- $F(X,Y) := Y^n f(X/Y)$, the homogenization of f.
- h the class number of $\mathbb{L}$.
- p_i be any generator of $\mathbf{p_i}^h$.

Decomposition: If $\langle f(x)\rangle = \langle\beta\rangle = \mathbf{b}\mathbf{p_1}^{a_1}\cdots\mathbf{p_t}^{a_t}$ then letting $a_i = nha'_i + a''_i$ we have

$$\langle F(x/p_1^{a'_i}\cdots p_t^{a'_t}, 1/p_1^{a'_1}\cdots p_t^{a'_t})\rangle = \langle c\rangle := \mathbf{b}\mathbf{p_1}^{a''_1}\cdots\mathbf{p_t}^{a''_t}$$

Finally, pick a $\varepsilon \in \mathfrak{o}_{\mathbb{K}}^*$ by earlier Lemma, so that $\varepsilon^n c$ has all its valuations close to $\mathrm{Nm}_{\mathbb{K}}(\beta)^{1/d}$.

Proof Sketch

Proof (Cont.)

We now consider

$$\langle F(\varepsilon x/p_1^{a_i'} \cdots p_t^{a_t'}, \varepsilon/p_1^{a_1'} \cdots p_t^{a_t'})\rangle = \langle \varepsilon^n c\rangle := \mathbf{b}\mathbf{p_1}^{a_1''} \cdots \mathbf{p_t}^{a_t''}$$

Proof Sketch

Proof (Cont.)

We now consider

$$\langle F(\varepsilon x/p_1^{a_i'} \cdots p_t^{a_t'}, \varepsilon/p_1^{a_1'} \cdots p_t^{a_t'})\rangle = \langle \varepsilon^n c\rangle := \mathbf{b}\mathbf{p_1}^{a_1''} \cdots \mathbf{p_t}^{a_t''}$$

By Györy and Yu, (2006)

$$h(\varepsilon/p_1^{a_1'} \ldots p_t^{a_t'}) \ll_{\mathbb{K},F,S} 1 + h(\varepsilon^n c) \tag{2}$$

Proof Sketch

Proof (Cont.)

We now consider

$$\langle F(\varepsilon x/p_1^{a_i'}\cdots p_t^{a_t'}, \varepsilon/p_1^{a_1'}\cdots p_t^{a_t'})\rangle = \langle \varepsilon^n c\rangle := \mathbf{b}\mathbf{p_1}^{a_1''}\cdots \mathbf{p_t}^{a_t''}$$

By Győry and Yu, (2006)

$$h(\varepsilon/p_1^{a_1'}\ldots p_t^{a_t'}) \ll_{\mathbb{K},F,S} 1 + h(\varepsilon^n c) \tag{2}$$

Rest of the proof is lower bounding LHS and upper bounding RHS.

Effective Result over integral points

Theorem

Let $f(X) \in \mathfrak{o}_{\mathbb{K}}[X]$ be a polynomial with at least 3 distinct roots and for which 0 is not periodic. Let S be a finite set of places of $\mathbb{K}$ containing all infinite places.
Suppose $\alpha \in \mathfrak{o}_K$ satisfies the equation

$$f^{(m)}(\alpha) = uf^{(n)}(\alpha) \tag{3}$$

where $m \neq n, u \in R_S^*$. Then

$$h(\alpha) < C(\mathbb{K}, S, f, \varepsilon)$$

where $C(\mathbb{K}, S, f, \varepsilon)$ is an effectively computable constant which depends only on $\mathbb{K}$, S, f and ε.

Bounding Multiplicative Dependence

$$f^{(n)}(f^{(k)}(\alpha)) = uf^{(k)}(\alpha), \quad u \in R_S^*, \alpha \in \mathfrak{o}_{\mathbb{K}}, f \in \mathfrak{o}_{\mathbb{K}}[X]$$

Above gives an upper bound on n.

Bounding Multiplicative Dependence

$$f^{(n)}(f^{(k)}(\alpha)) = uf^{(k)}(\alpha), \quad u \in R_S^*, \alpha \in \mathfrak{o}_{\mathbb{K}}, f \in \mathfrak{o}_{\mathbb{K}}[X]$$

Above gives an upper bound on n.
To lower bound n, let $\mathbf{b} := \langle f^{(n+k)}(\alpha) \rangle_{M_{\mathbb{K}} \setminus S}$. Then

$$\mathbf{b} \mid f^{(n+k)}(\alpha), f^{(k)}(\alpha) \implies \mathbf{b} \mid f^{(n)}(0)$$

Bounding Multiplicative Dependence

$$f^{(n)}(f^{(k)}(\alpha)) = uf^{(k)}(\alpha), \quad u \in R_S^*, \alpha \in \mathfrak{o}_{\mathbb{K}}, f \in \mathfrak{o}_{\mathbb{K}}[X]$$

Above gives an upper bound on n.
To lower bound n, let $\mathbf{b} := \langle f^{(n+k)}(\alpha) \rangle_{M_{\mathbb{K}} \setminus S}$. Then

$$\mathbf{b} \mid f^{(n+k)}(\alpha), f^{(k)}(\alpha) \implies \mathbf{b} \mid f^{(n)}(0)$$

And by our effective diophantine approximation result, we get

$$\begin{aligned}(1 - \varepsilon(f, \mathbb{K}, S))(d^{n+k}\hat{h}_f(\alpha) - C_1(f, \mathbb{K})) &\ll_{\mathbb{K},f,S} h_{M_{\mathbb{K}} \setminus S}(f^{(n+k)}(\alpha)^{-1}) \\ &\ll_{\mathbb{K},f,S} h_{M_{\mathbb{K}} \setminus S}(f^{(k)}(0)^{-1}) \\ &\ll_{\mathbb{K},f,S} d^k \hat{h}_f(0)\end{aligned}$$

and since $n > 0$ this effectively bounds $h(\alpha)$.

References I

Bérczes, A., A. Ostafe, I. E. Shparlinski, and J. H. Silverman (). "Multiplicative dependence among iterated values of rational functions modulo finitely generated groups". In: *Internat. Math. Res. Notices.*

Bugeaud, Y., J. H. Evertse, and K. Györy (2018). "S-parts of values of univariate polynomials, binary forms and decomposable forms at integral points". In: *Acta Arith.* 184, pp. 151–185.

Gross, S. S. and A. F. Vincent (2013). "On the factorization of $f(n)$ for $f(x)$ in $\mathbb{Z}[x]$". In: *Intern. J. Number Theory* 9, pp. 1225–1236.

Györy, K. and K. Yu (2006). "Bounds for the solutions of S-unit equations and decomposable form equations". In: *Acta Arith.* 123.1, pp. 9–41.

Hsia, L.C. and J. H. Silverman (2011). "A quantitative estimate for quasi-integral points in orbits". In: *Pacific J. Math.* 322, pp. 321–342.

Northcott, D. G. (1950). "Periodic points on an algebraic variety". In: *Ann. of Math.* 51, pp. 167–177.