Counting reducible polynomials

Robert Grizzard

LAFAYETTE COLLEGE

AMS Special Session on Diophantine Approximation and Analytic Number Theory in Honor of Jeffrey Vaaler
JMM January 12, 2018

A tale of two height functions

If $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d \in \mathbb{Z}[z]$, $w_0 \neq 0$, which factors over $\mathbb{C}$ as $f(z) = w_0(z - \alpha_1) \cdots (z - \alpha_d)$, we'll consider two notions of the height of f:

A tale of two height functions

If $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d \in \mathbb{Z}[z]$, $w_0 \neq 0$, which factors over $\mathbb{C}$ as $f(z) = w_0(z - \alpha_1) \cdots (z - \alpha_d)$, we'll consider two notions of the height of f:

1. The naive height: $\|f\|_\infty := \max_{0 \leq i \leq d} |w_i|$.

A tale of two height functions

If $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d \in \mathbb{Z}[z]$, $w_0 \neq 0$, which factors over $\mathbb{C}$ as $f(z) = w_0(z - \alpha_1) \cdots (z - \alpha_d)$, we'll consider two notions of the height of f:

1. The naive height: $\|f\|_\infty := \max_{0 \leq i \leq d} |w_i|$.
2. The Mahler measure: $M(f) := |w_0| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$.

A tale of two height functions

If $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d \in \mathbb{Z}[z]$, $w_0 \neq 0$, which factors over $\mathbb{C}$ as $f(z) = w_0(z - \alpha_1) \cdots (z - \alpha_d)$, we'll consider two notions of the height of f:

1. The naive height: $\|f\|_\infty := \max_{0 \leq i \leq d} |w_i|$.
2. The Mahler measure: $M(f) := |w_0| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$.

Up to a constant depending on d, the two are comparable:

A tale of two height functions

If $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d \in \mathbb{Z}[z]$, $w_0 \neq 0$, which factors over $\mathbb{C}$ as $f(z) = w_0(z - \alpha_1)\cdots(z - \alpha_d)$, we'll consider two notions of the height of f:

1. The naive height: $\|f\|_\infty := \max_{0 \leq i \leq d} |w_i|$.
2. The Mahler measure: $M(f) := |w_0| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$.

Up to a constant depending on d, the two are comparable:

Proposition (Mahler)

$\binom{d}{\lfloor d/2 \rfloor} \|f\|_\infty \leq M(f) \leq \sqrt{d+1}\|f\|_\infty$.

A tale of two height functions

If $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d \in \mathbb{Z}[z]$, $w_0 \neq 0$, which factors over $\mathbb{C}$ as $f(z) = w_0(z - \alpha_1)\cdots(z - \alpha_d)$, we'll consider two notions of the height of f:

1. The naive height: $\|f\|_\infty := \max_{0 \leq i \leq d} |w_i|$.
2. The Mahler measure: $M(f) := |w_0| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$.

Up to a constant depending on d, the two are comparable:

Proposition (Mahler)

$$\binom{d}{\lfloor d/2 \rfloor} \|f\|_\infty \leq M(f) \leq \sqrt{d+1}\|f\|_\infty.$$

So, when d is fixed and we are counting polynomials of bounded height, these heights are basically interchangeable.

How many polynomials are reducible?

Setup:

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$
- Some subset of size $s \in \{1, \ldots, d+1\}$ of the coefficients are "free."

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$
- Some subset of size $s \in \{1, \ldots, d+1\}$ of the coefficients are "free."
- The other $d + 1 - s$ coefficients are fixed integers.

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$
- Some subset of size $s \in \{1, \ldots, d+1\}$ of the coefficients are "free."
- The other $d + 1 - s$ coefficients are fixed integers.

Question

How many polynomials of this form of height $\leq T$ are reducible?

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$
- Some subset of size $s \in \{1, \ldots, d+1\}$ of the coefficients are "free."
- The other $d + 1 - s$ coefficients are fixed integers.

Question

How many polynomials of this form of height $\leq T$ are reducible?
(We hope not very many!)

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$
- Some subset of size $s \in \{1, \ldots, d+1\}$ of the coefficients are "free."
- The other $d + 1 - s$ coefficients are fixed integers.

Question

How many polynomials of this form of height $\leq T$ are reducible? (We hope not very many!)(What height are you using?)

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$
- Some subset of size $s \in \{1, \ldots, d+1\}$ of the coefficients are "free."
- The other $d + 1 - s$ coefficients are fixed integers.

Question

How many polynomials of this form of height $\leq T$ are reducible? (We hope not very many!)(What height are you using?)

first answer:

How many polynomials are reducible?

Setup:

- Consider polynomials of the form $f(z) = w_0 z^d + w_1 z^{d-1} + \cdots + w_d$
- Some subset of size $s \in \{1, \ldots, d+1\}$ of the coefficients are "free."
- The other $d + 1 - s$ coefficients are fixed integers.

Question

How many polynomials of this form of height $\leq T$ are reducible? (We hope not very many!)(What height are you using?)

first answer:

Theorem (S. D. Cohen, '79 – Effective HIT, special case)

The number of such specializations with $\|f\|_\infty \leq T$ where f is reducible is $\ll_d T^{s-1/2} \log T$. (Constant apparently effective.)

Is 1/2 power savings best possible?

- If we look at polynomials of the form $z^2 - t$, where t is the only free coefficient (here $s = 1$), it's easy to see that $\gg T^{1/2}$ of these are reducible, so can't do better than 1/2 power savings here...

Is 1/2 power savings best possible?

- If we look at polynomials of the form $z^2 - t$, where t is the only free coefficient (here $s = 1$), it's easy to see that $\gg T^{1/2}$ of these are reducible, so can't do better than $1/2$ power savings here...
- Can we do better if s is large enough?

Proposition (Masser-Vaaler, G.-Gunther,...)

If $s = d + 1$ (so we're just looking at the number of degree d reducible polynomials), the number of reducible polynomials with Mahler measure at most T is

Is 1/2 power savings best possible?

- If we look at polynomials of the form $z^2 - t$, where t is the only free coefficient (here $s = 1$), it's easy to see that $\gg T^{1/2}$ of these are reducible, so can't do better than $1/2$ power savings here...
- Can we do better if s is large enough?

Proposition (Masser-Vaaler, G.-Gunther,...)

If $s = d + 1$ (so we're just looking at the number of degree d reducible polynomials), the number of reducible polynomials with Mahler measure at most T is

$$\leq \begin{cases} 1758 \cdot T^2 \log T, & \text{if } d = 2,\ T \geq 2, \text{ and} \\ 153 \cdot 4^d P(d-1) \cdot T^d, & \text{if } d \geq 3,\ T \geq 1. \end{cases} \tag{1}$$

Is 1/2 power savings best possible?

- If we look at polynomials of the form $z^2 - t$, where t is the only free coefficient (here $s = 1$), it's easy to see that $\gg T^{1/2}$ of these are reducible, so can't do better than $1/2$ power savings here...
- Can we do better if s is large enough?

Proposition (Masser-Vaaler, G.-Gunther,...)

If $s = d + 1$ (so we're just looking at the number of degree d reducible polynomials), the number of reducible polynomials with Mahler measure at most T is

$$\leq \begin{cases} 1758 \cdot T^2 \log T, & \text{if } d = 2,\ T \geq 2, \text{ and} \\ 153 \cdot 4^d P(d-1) \cdot T^d, & \text{if } d \geq 3,\ T \geq 1. \end{cases} \tag{1}$$

So we have reducibles $\ll T^{s-1}$ here, or full power savings (when $d \geq 3$).

Proof sketch, and why Mahler measure is nice

Proof sketch, and why Mahler measure is nice

- Mahler measure is multiplicative! That is, if $f = f_1 f_2$, then $M(f) = M(f_1)M(f_2)$.

Proof sketch, and why Mahler measure is nice

- Mahler measure is multiplicative! That is, if $f = f_1 f_2$, then $M(f) = M(f_1)M(f_2)$.
- This makes it feasible to win my counting all possible factorizations.

Proof sketch, and why Mahler measure is nice

- Mahler measure is multiplicative! That is, if $f = f_1 f_2$, then $M(f) = M(f_1)M(f_2)$.
- This makes it feasible to win my counting all possible factorizations.
- Suppose $f = f_1 f_2$, where f_i has degree d_i, $1 \leq d_2 \leq d_1 \leq d - 1$.

Proof sketch, and why Mahler measure is nice

- Mahler measure is multiplicative! That is, if $f = f_1 f_2$, then $M(f) = M(f_1)M(f_2)$.
- This makes it feasible to win my counting all possible factorizations.
- Suppose $f = f_1 f_2$, where f_i has degree d_i, $1 \leq d_2 \leq d_1 \leq d - 1$.
- Let k be the unique integer with $2^{k-1} \leq M(f_1) \leq 2^k$ (so k will run from 1 to $\lfloor \log_T / \log 2 \rfloor + 1$).

Proof sketch, and why Mahler measure is nice

- Mahler measure is multiplicative! That is, if $f = f_1 f_2$, then $M(f) = M(f_1)M(f_2)$.
- This makes it feasible to win my counting all possible factorizations.
- Suppose $f = f_1 f_2$, where f_i has degree d_i, $1 \leq d_2 \leq d_1 \leq d - 1$.
- Let k be the unique integer with $2^{k-1} \leq M(f_1) \leq 2^k$ (so k will run from 1 to $\lfloor \log_T / \log 2 \rfloor + 1$).
- If $M(f) \leq T$, then $M(f_2) \leq 2^{1-k} T$.

Proof sketch, and why Mahler measure is nice

- Mahler measure is multiplicative! That is, if $f = f_1 f_2$, then $M(f) = M(f_1)M(f_2)$.
- This makes it feasible to win my counting all possible factorizations.
- Suppose $f = f_1 f_2$, where f_i has degree d_i, $1 \leq d_2 \leq d_1 \leq d - 1$.
- Let k be the unique integer with $2^{k-1} \leq M(f_1) \leq 2^k$ (so k will run from 1 to $\lfloor \log_T / \log 2 \rfloor + 1$).
- If $M(f) \leq T$, then $M(f_2) \leq 2^{1-k} T$.
- Sum over all the possible k, d_1.... finish proof.

An example

Let's take $d = 8$ and count reducible polynomials of the form

$$f(z) = w_0 z^8 + az^7 + bz^6 + cz^5 + dz^4 + ez^3 + fz^2 + w_7 z + w_8$$

An example

Let's take $d = 8$ and count reducible polynomials of the form

$$f(z) = w_0 z^8 + az^7 + bz^6 + cz^5 + dz^4 + ez^3 + fz^2 + w_7 z + w_8$$

(here $s = 3$). Let's count factorizations into two quartics

An example

Let's take $d = 8$ and count reducible polynomials of the form

$$f(z) = w_0 z^8 + az^7 + bz^6 + cz^5 + dz^4 + ez^3 + fz^2 + w_7 z + w_8$$

(here $s = 3$). Let's count factorizations into two quartics

$$f(z) = (x_0 z^4 + x_1 z^3 + x_2 z^2 + x_3 z + x_4)(y_0 z^4 + y_1 z^3 + y_2 z^2 + y_3 z + y_4)$$

An example

Let's take $d = 8$ and count reducible polynomials of the form

$$f(z) = w_0 z^8 + az^7 + bz^6 + cz^5 + dz^4 + ez^3 + fz^2 + w_7 z + w_8$$

(here $s = 3$). Let's count factorizations into two quartics

$$f(z) = (x_0 z^4 + x_1 z^3 + x_2 z^2 + x_3 z + x_4)(y_0 z^4 + y_1 z^3 + y_2 z^2 + y_3 z + y_4)$$

We get a system of 6 equations in the 10 variables x_i, y_i:

An example

Let's take $d = 8$ and count reducible polynomials of the form

$$f(z) = w_0 z^8 + az^7 + bz^6 + cz^5 + dz^4 + ez^3 + fz^2 + w_7 z + w_8$$

(here $s = 3$). Let's count factorizations into two quartics

$$f(z) = (x_0 z^4 + x_1 z^3 + x_2 z^2 + x_3 z + x_4)(y_0 z^4 + y_1 z^3 + y_2 z^2 + y_3 z + y_4)$$

We get a system of 6 equations in the 10 variables x_i, y_i:

$$\begin{aligned}
a &= x_0 y_1 + x_1 y_0 \\
b &= x_0 y_2 + x_1 y_1 + x_2 y_0 \\
c &= x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 \\
d &= x_0 y_4 + x_1 y_3 + x_2 y_2 + x_3 y_1 + x_4 y_0 \\
e &= x_1 y_4 + x_2 y_3 + x_3 y_2 + x_4 y_1 \\
f &= x_2 y_4 + x_3 y_3 + x_4 y_2
\end{aligned}$$

An example (continued)

$$
\begin{aligned}
a &= x_0 y_1 + x_1 y_0 \\
b &= x_0 y_2 + x_1 y_1 + x_2 y_0 \\
c &= x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 \\
d &= x_0 y_4 + x_1 y_3 + x_2 y_2 + x_3 y_1 + x_4 y_0 \\
e &= x_1 y_4 + x_2 y_3 + x_3 y_2 + x_4 y_1 \\
f &= x_2 y_4 + x_3 y_3 + x_4 y_2
\end{aligned}
$$

- Fix x_0, x_2, y_1, y_3...

An example (continued)

$$
\begin{aligned}
a &= x_0 y_1 + x_1 y_0 \\
b &= x_0 y_2 + x_1 y_1 + x_2 y_0 \\
c &= x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0 \\
d &= x_0 y_4 + x_1 y_3 + x_2 y_2 + x_3 y_1 + x_4 y_0 \\
e &= x_1 y_4 + x_2 y_3 + x_3 y_2 + x_4 y_1 \\
f &= x_2 y_4 + x_3 y_3 + x_4 y_2
\end{aligned}
$$

- Fix x_0, x_2, y_1, y_3...
- Then there are finitely many choices for x_1, x_3, y_0, y_2

An example (continued)

$$a = x_0y_1 + x_1y_0$$
$$b = x_0y_2 + x_1y_1 + x_2y_0$$
$$c = x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0$$
$$d = x_0y_4 + x_1y_3 + x_2y_2 + x_3y_1 + x_4y_0$$
$$e = x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1$$
$$f = x_2y_4 + x_3y_3 + x_4y_2$$

- Fix x_0, x_2, y_1, y_3...
- Then there are finitely many choices for x_1, x_3, y_0, y_2...

An example (continued)

$$a = x_0y_1 + x_1y_0$$
$$b = x_0y_2 + x_1y_1 + x_2y_0$$
$$c = x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0$$
$$d = x_0y_4 + x_1y_3 + x_2y_2 + x_3y_1 + x_4y_0$$
$$e = x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1$$
$$f = x_2y_4 + x_3y_3 + x_4y_2$$

- Fix x_0, x_2, y_1, y_3...
- Then there are finitely many choices for x_1, x_3, y_0, y_2...
- and the remaining two variables x_4 and y_4 must satisfy an overdetermined system of 3 eqautions.

An example (continued)

$$a = x_0y_1 + x_1y_0$$
$$b = x_0y_2 + x_1y_1 + x_2y_0$$
$$c = x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0$$
$$d = x_0y_4 + x_1y_3 + x_2y_2 + x_3y_1 + x_4y_0$$
$$e = x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1$$
$$f = x_2y_4 + x_3y_3 + x_4y_2$$

- Fix x_0, x_2, y_1, y_3...
- Then there are finitely many choices for x_1, x_3, y_0, y_2...
- and the remaining two variables x_4 and y_4 must satisfy an overdetermined system of 3 eqautions.
- On the locus where this overdetermined system has a positive dimensional solution set, we must have $x_0 = x_1 = x_2$ and $y_0 = y_1 = y_2$, and so we find that on this set we may fix x_0, x_4, y_1, y_3 to determine the other variables up to finitely many choices.

An example (continued)

$$a = x_0y_1 + x_1y_0$$
$$b = x_0y_2 + x_1y_1 + x_2y_0$$
$$c = x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0$$
$$d = x_0y_4 + x_1y_3 + x_2y_2 + x_3y_1 + x_4y_0$$
$$e = x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1$$
$$f = x_2y_4 + x_3y_3 + x_4y_2$$

- Fix x_0, x_2, y_1, y_3...
- Then there are finitely many choices for x_1, x_3, y_0, y_2...
- and the remaining two variables x_4 and y_4 must satisfy an overdetermined system of 3 eqautions.
- On the locus where this overdetermined system has a positive dimensional solution set, we must have $x_0 = x_1 = x_2$ and $y_0 = y_1 = y_2$, and so we find that on this set we may fix x_0, x_4, y_1, y_3 to determine the other variables up to finitely many choices.
- So, partitioning the space into these two cases, we win.

Theorem (G.)

If $d \geq 3$ and $s \geq d/2$, then the number of degree d reducible polynomials f with $\|f\|_\infty \leq T$ and any $d+1-s$ of the coefficients fixed integers is $\ll T^{s-1}$.

Theorem-in-progress (G.)

If $d \geq 3$ and $s \geq 3$, then the number of degree d reducible polynomials f with $\|f\|_\infty \leq T$ and any $d+1-s$ of the coefficients fixed integers is $\ll T^{s-1}$.

It's over!

Thanks for your attention!