Counting integer polynomials with several roots of maximal modulus

Min Sha
South China Normal University
(Joint woth with Artūras Dubickas)

Number Theory Seminar, University of Debrecen
27/09/2024

Counting integer polynomials

- Counting integer polynomials with respect to some arithmetic properties and under some measures has a long history and is still active.

- Many mathematicians have done work in this topic.
  For example, the number theory research group in Debrecen.

Counting integer polynomials

- These arithmetic properties include:
  reducibility,

  decomposability $(f(x) = g(h(x)))$,

  signature of roots ($f(x)$ is of signature (r, s) if it has r real roots and $2s$ non-real roots),

  moduli of roots,

  degeneracy (a polynomial $f(x)$ is said to be degenerate if it has two roots whose quotient is a root of unity).

Height, Mahler measure, house

- For a polynomial of degree $n \geq 1$:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = a_n \prod_{i=1}^{n} (x - \alpha_i) \in \mathbb{C}[x],$$

its *height* is defined by

$$H(f) := \max_{0 \leq i \leq n} |a_i|,$$

its *Mahler measure* is defined by

$$M(f) := |a_n| \prod_{i=1}^{n} \max(1, |\alpha_i|),$$

and the *house* of f or the *inclusion radius* of f is defined by

$$r(f) := \max_{1 \leq i \leq n} |\alpha_i|,$$

A classical result

Let $\rho_n(m, H)$ be the number of monic polynomials

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x], \quad n \geq 2, \quad H(f) \leq H,$$

which are reducible in $\mathbb{Z}[x]$ with an irreducible factor of degree m.

van der Waerden proved:

Theorem (van der Waerden, 1936)

For integers $n \geq 2$ and $m \geq 1$, we have

$$H^{n-m} \ll \rho_m(n, H) \ll H^{n-m} \quad \textit{if} \quad 1 \leq m < n/2,$$

$$H^{n-m} \log H \ll \rho_m(n, H) \ll H^{n-m} \log H \quad \textit{if} \quad m = n/2.$$

In particular, when $n \geq 3$, the number of monic integer reducible polynomials of degree n and of height at most H is $\ll H^{n-1}$.

Motivation

- In this talk, we are interested in counting integer polynomials according to the moduli of their roots.
- The motivation is from the Skolem Problem of linear recurrence sequences.
- The Skolem Problem asks whether such a sequence has a zero term.

Linear recurrence sequences

- A *linear recurrence sequence* (LRS) over the rational numbers $\mathbb{Q}$, denoted by $\{s_m\}_{m\geq 0}$, of order $n \geq 2$:

  $$s_{m+n} = a_{n-1}s_{m+n-1} + \cdots + a_1 s_{m+1} + a_0 s_m, \quad m = 0, 1, 2, \ldots,$$

  where $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ and $a_0 \neq 0$. The *characteristic polynomial* of this sequence is

  $$f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathbb{Q}[x].$$

- The famous *Skolem-Mahler-Lech Theorem* states that the set $\{m : s_m = 0\}$ is the union of a finite set and finitely many arithmetic progressions. (the zero set)

- However, the corresponding algorithmic question, called the *Skolem Problem*, which asks to determine whether a given LRS has a zero term, is still widely open.

Linear recurrence sequences

- So far, the decidability of the Skolem Problem is only known in some special cases, based on the relative order of the absolute values of the characteristic roots.
- In 1984, Mignotte, Shorey and Tijdeman showed that the Skolem Problem is decidable if the characteristic polynomial $f(x)$ has **at most three** dominant roots (counted without multiplicity).
- However, the Skolem Problem for LRS of order at least 5 is still not decidable.

Linear recurrence sequences

- It is of interest to count polynomials according to the number of dominant roots.
- From this, one can see how often the Skolem Problem for a random LRS is decidable.

Some notation

- Recall that for $f \in \mathbb{C}[x]$, $r(f)$ is the largest modulus of the roots of f. Then, the roots of f with modulus $r(f)$ are said to be of *maximal modulus*. (Alteratively, *dominant root*)

- $D_n(k, H)$: the number of monic integer polynomials of degree n and height at most H with exactly k dominant roots (counted with multiplicity).

- $D_n^*(k, H)$: the number of integer polynomials of degree n and height at most H with exactly k dominant roots (counted with multiplicity).

Some symbols

- $U \ll V$ or, equivalently, $V \gg U$ for two positive quantities U, V (depending on k, n, H) means that $U \leq cV$ for some positive constant c which may depend on k and n but does not depend on H.
- $U \sim V$ means $\lim_{H\to\infty} U/V = 1$.

The case $k = 1$ about monic polynomials

Theorem (Dubickas and S., 2015)

For any integer $n \geq 2$, we have

$$D_n(1, H) \sim (2H)^n,$$

that is,

$$\lim_{H \to \infty} \frac{D_n(1, H)}{(2H)^n} = 1.$$

Recall that there are $(2H + 1)^n$ monic integer polynomials of degree n and with height at most H.

The case $k = 1$ about non-monic polynomials

Theorem (Dubickas and S., 2015)

For any integer $n \geq 2$, we have

$$0 < \limsup_{H \to \infty} \frac{D_n^*(1, H)}{(2H)^{n+1}} < 1.$$

This implies

$$H^{n+1} \ll D_n^*(1, H) \ll H^{n+1}.$$

Recall that there are $2H(2H+1)^n$ integer polynomials of degree n and with height at most H.

The case $k = 2$ about monic polynomials

Theorem (Dubickas and S., 2016)

For any integer $n \geq 2$, we have

$$H^{n-1/2} \ll D_n(2, H) \ll H^{n-1/2};$$

and

$$\sum_{k=3}^{n} D_n(k, H) \ll H^{n-1}.$$

The case $k = 2$ about non-monic polynomials

Theorem (Dubickas and S., 2016)

For any integer $n \geq 2$, we have

$$\lim_{H \to \infty} \frac{D_n^*(1, H) + D_n^*(2, H)}{(2H)^{n+1}} = 1,$$

and

$$\sum_{k=3}^{n} D_n^*(k, H) \ll H^n.$$

This implies

$$H^{n+1} \ll D_n^*(2, H) \ll H^{n+1},$$

Back to the motivation

- Recall that Mignotte, Shorey and Tijdeman showed that the Skolem Problem is decidable if the characteristic polynomial has **at most three** dominant roots (counted without multiplicity).

- Recall
$$\lim_{H\to\infty} \frac{D_n^*(1,H)+D_n^*(2,H)}{(2H)^{n+1}} = 1.$$

- So, roughly speaking, for almost all LRS over $\mathbb{Q}$, the Skolem Problem is decidable.

Question by Igor Shparlinski

- Igor: get a good bound on the number of integer polynomials of fixed degree and bounded height and with several dominant roots?
- Then, we come back to this topic.

This talk

- We are interested in the size of the quantity $D_n(k, H)$ when $k \geq 3$. (that is, focusing on monic polynomials)

- The case of non-monic polynomials is somehow easier, because one can enlarge the leading coefficient to control the moduli of roots.

The case $k \geq 3$

Theorem (Dubickas and S., 2024)

For any integers $n \geq k \geq 3$ and $H \geq 1$, we have

$$H^{\frac{n+1}{2}-k+\frac{5k^2-4k+7}{8n}} \ll D_n(k,H) \ll H^{n-\frac{k+1}{2}}$$

for k odd, and

$$H^{\frac{n+1}{2}-k+\frac{5k^2-2k+16}{8n}} \ll D_n(k,H) \ll H^{n-\frac{k-1}{2}}$$

for k even.

This implies

$$\sum_{k=3}^{n} D_n(k,H) \ll H^{n-3/2}. \qquad (\text{previously}, \ll H^{n-1})$$

How large are the lower bounds?

- Define

$$e(n,k) = \begin{cases} \frac{n+1}{2} - k + \frac{5k^2-4k+7}{8n} & \text{if } k \text{ is odd,} \\ \frac{n+1}{2} - k + \frac{5k^2-2k+16}{8n} & \text{if } k \text{ is even} \end{cases}$$

- Viewing the exponent $e(n,k)$ as a quadratic polynomial in k, we obtain

$$e(n,k) \geq \begin{cases} \frac{n+1}{10} + \frac{31}{40n} & \text{if } k \text{ is odd,} \\ \frac{n+3}{10} + \frac{79}{40n} & \text{if } k \text{ is even.} \end{cases}$$

Counting reducible and irreducible polynomials separately

- $I_n(k, H)$: the number of monic **irreducible** integer polynomials of degree n and height at most H and with exactly k dominant roots (counted with multiplicity).
- $R_n(k, H)$: the number of monic **reducible** integer polynomials of degree n and height at most H and with exactly k dominant roots (counted with multiplicity).
- Clearly,
$$D_n(k, H) = I_n(k, H) + R_n(k, H).$$

Counting irreducible polynomials

Theorem (Dubickas and S., 2024)

Let $n \geq 2$ and $H \geq 1$ be two integers. Then, for any odd integer k satisfying $1 \leq k \leq n$, we have

$$I_n(k, H) \begin{cases} \sim (2H)^{n/k} & \textit{if } k \mid n, \\ = 0 & \textit{if } k \nmid n; \end{cases}$$

for any integer k with $1 \leq k \leq n$, we have

$$I_n(k, H) \ll H^{n-(k-1)/2}.$$

Finally, for even $n \geq 2$, we have

$$I_n(n, H) \gg H^{\frac{n}{8}+\frac{2}{n}+\frac{1}{4}}.$$

Counting reducible polynomials

Theorem (Dubickas and S., 2024)

For any integers $n \geq 3$ and k with $1 \leq k \leq n$, we have

$$R_n(k, H) \ll H^{n-(k+1)/2},$$

and also in all those cases, except when $k = n$ is even,

$$R_n(k, H) \gg H^{e(n,k)}.$$

Finally, in the case when $k = n$ is even, we have

$$R_n(n, H) \gg H^{\frac{n}{8}+\frac{2}{n}-\frac{1}{4}}.$$

The case $k = 3$

When $k = 3$, we have $R_n(3, H) \ll H^{n-2}$, and

$$I_n(3, H) \begin{cases} \sim (2H)^{n/3} & \text{if } 3 \mid n, \\ = 0 & \text{if } 3 \nmid n. \end{cases}$$

From $D_n(3, H) = I_n(3, H) + R_n(3, H)$, we directly have:

Corollary

For any integer $H \geq 1$, we have

$$D_n(3, H) \ll H^{n-2}.$$

Question

- What is the correct size of $D_n(3, H)$ when n is large?
- The key point is to estimate $R_n(3, H)$.
- For $n = 3, 4$, we get:

Theorem (Dubickas and S., 2024)

For any integer $H \geq 1$, we have

$$H \ll D_3(3, H) \ll H, \qquad H \log H \ll D_4(3, H) \ll H \log H.$$

More general questions

- What is the correct size of $D_n(k, H)$ for any $k \geq 3$?
- Moreover, how about asymptotic formulas?

Counting irreducible polynomials when k is odd

Theorem (Dubickas and S., 2024)

Let $n \geq 2$ and $H \geq 1$ be two integers. Then, for any odd integer k satisfying $1 \leq k \leq n$, we have

$$I_n(k, H) \begin{cases} \sim (2H)^{n/k} & \text{if } k \mid n, \\ = 0 & \text{if } k \nmid n. \end{cases}$$

Counting irreducible polynomials when k is odd

- Let $f(x)$ be an irreducible polynomial contributing to $I_n(k, H)$. Since k is odd, f has a real dominant root.

- The following result proved by Ferguson, which is a generalization of Boyd's result.

Theorem (Ferguson, 1997)

Suppose that an irreducible integer polynomial $f(x) \in \mathbb{Z}[x]$ has k roots, at least one real, of equal modulus. Then, $f(x) = g(x^k)$, where $g(x)$ is an irreducible integer polynomial.

In particular, $k \mid \deg f$.

Counting irreducible polynomials when k is odd

- Conversely, we have:

Lemma

Let $g(x)$ be a monic irreducible integer polynomial of positive degree such that $|g(0)|^{1/m} \notin \mathbb{Q}$ for any integer $m > 1$. Then, $g(x^k)$ is also irreducible in $\mathbb{Z}[x]$ for any integer $k \geq 1$.

This is a corollary of Capelli's lemma about the irreducibility of compositions of polynomials.

Counting irreducible polynomials: the general case

Theorem (Dubickas and S., 2024)

Let $n \geq 2$ and $H \geq 1$ be two integers. Then, for any integer k with $1 \leq k \leq n$, we have

$$I_n(k, H) \ll H^{n-(k-1)/2}.$$

For even $n \geq 2$, we have

$$I_n(n, H) \gg H^{\frac{n}{8}+\frac{2}{n}+\frac{1}{4}}.$$

Counting irreducible polynomials: the general case

- Consider a monic integer polynomial contributing to $I_n(k, H)$

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

- By definition, we obtain

$$r(f)^k \leq M(f) \leq \sqrt{n+1}\rangle H(f) \leq \sqrt{n+1}H,$$

which gives

$$r(f) \ll H^{1/k}.$$

- From $|a_{n-i}| \leq \binom{n}{i} r(f)^i$ for any integer i with $1 \leq i \leq n$, we see that the vector

$$(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$$

can take at most $\ll r(f)^{1+2+\cdots+k} \ll r(f)^{k(k+1)/2} \ll H^{(k+1)/2}$ values.

Counting irreducible polynomials: the general case

- Since the vector

$$(a_{n-k-1}, a_{n-k-2}, \dots, a_0)$$

takes at most $(2H+1)^{n-k} \ll H^{n-k}$ values, there are at most

$$\ll H^{(k+1)/2+n-k} \ll H^{n-(k-1)/2}$$

suitable monic polynomials f.

- In fact, we obtain

$$D_n(k, H) \ll H^{n-(k-1)/2}.$$

Counting reducible polynomials

Theorem (Dubickas and S., 2024)

For any integers $n \geq 3$ and k with $1 \leq k \leq n$, we have

$$R_n(k, H) \ll H^{n-(k+1)/2},$$

and also in all those cases, except when $k = n$ is even,

$$R_n(k, H) \gg H^{e(n,k)}.$$

In the case when $k = n$ is even, we have $R_n(n, H) \gg H^{\frac{n}{8}+\frac{2}{n}-\frac{1}{4}}$.

$$e(n,k) = \begin{cases} \frac{n+1}{2} - k + \frac{5k^2-4k+7}{8n} & \text{if } k \text{ is odd,} \\ \frac{n+1}{2} - k + \frac{5k^2-2k+16}{8n} & \text{if } k \text{ is even} \end{cases}$$

Counting reducible polynomials: k is even

- Assume first that the integer k satisfying $2 \le k \le n$ is even. Set $\ell = k/2$. Fix an integer m in the range

$$\frac{H^{2/n}}{5} \le m \le \frac{H^{2/n}}{4}.$$

- Consider a monic integer irreducible polynomial

$$(x - \beta_1) \cdots (x - \beta_\ell)$$

  of degree ℓ with all ℓ real roots in the interval $[-2\sqrt{m}, 2\sqrt{m}]$.

- How many are these polynomials?

Counting reducible polynomials: k is even

Theorem (Akiyama and Pethő, 2014)

Let $s \geq 0$ and $n \geq 1$ be two integers satisfying $s \leq n/2$. Then, there are constants $v_1(s,n) > 0$ and $v_2(s,n) > 0$ such that for each $B > 0$ the number $J_n(s,B)$ of monic irreducible integer polynomials f of degree n with $r(f) \leq B$ and with exactly $2s$ non-real roots satisfies

$$\left| J_n(s,B) - v_1(s,n) B^{n(n+1)/2} \right| \leq v_2(s,n) B^{n(n+1)/2-1}.$$

- By the above theorem, there are $\gg m^{\ell(\ell+1)/4}$ of such polynomials $(x-\beta_1)\cdots(x-\beta_\ell)$.

Counting reducible polynomials: k is even

- For each of the above polynomials with all roots in the open interval $(-2\sqrt{m}, 2\sqrt{m})$, we set

$$g(x) = (x^2 - \beta_1 x + m) \cdots (x^2 - \beta_\ell x + m) \in \mathbb{Z}[x].$$

From $\beta_i^2 - 4m < 0$, we see that each such polynomial g has all its $2\ell = k$ roots of modulus $\sqrt{m}$.

- Consider monic polynomials f of the form

$$f(x) = g(x)h(x),$$

where g is as the above and $h \in \mathbb{Z}[x]$ is a monic polynomial of degree $n - k$ that has its all $n - k$ roots of modulus $\leq \sqrt{m}/2$.

Counting reducible polynomials: k is even

- $g(x)$ is irreducible.
- If $k < n$, such polynomials f contribute to $R_n(k, H)$.
- If $k = n$, then such polynomials f contribute to $I_n(n, H)$.
- If $k = n \geq 4$, set $\ell = (n-2)/2$, and then apply similar arguments, and obtain a lower bound for $R_n(n, H)$.

Counting reducible polynomials: k is odd

- Now, k is odd. Set $\ell = (k-1)/2$. This time we argue with integer m in the range

$$\frac{H^{1/n}}{3} \le m \le \frac{H^{1/n}}{2}.$$

- Consider a monic integer irreducible polynomial

$$(x-\beta_1)\cdots(x-\beta_\ell)$$

of degree ℓ with all ℓ real roots in the interval $(-2m, 2m)$.

Counting reducible polynomials: k is odd

- Set
$$g(x) = (x - m)(x^2 - \beta_1 x + m^2) \dots (x^2 - \beta_\ell x + m^2) \in \mathbb{Z}[x].$$
By $\beta_i^2 - 4m^2 < 0$, $i = 1, \dots, \ell$, we see that the polynomial g has all its $k = 2\ell + 1$ roots of modulus m, with m being the only real root among them. Note that if $k = 1$, we have $g(x) = x - m$.

- Consider monic polynomials f of the form
$$f(x) = g(x)h(x),$$
where g is as the above and $h \in \mathbb{Z}[x]$ is a monic polynomial of degree $n - k$ that has its all $n - k$ roots of modulus $\leq m/2$.

Counting reducible polynomials: k is odd

- $g(x)$ is reducible, $g(x)/(x-m)$ is irreducible.
- Such polynomials f contribute to $R_n(k,H)$. Counting these polynomals gives a lower bound for $R_n(k,H)$.

Thank you for your attention!