Counting and Testing Dominant Polynomials

Artūras Dubickas\textsuperscript{a} \& Min Sha\textsuperscript{b}
\begin{itemize}
\item \textsuperscript{a} Department of Mathematics and Informatics, Vilnius University, Vilnius, Lithuania
\item \textsuperscript{b} School of Mathematics and Statistics, University of New South Wales, Sydney, Australia
\end{itemize}
Published online: 23 Jun 2015.

To cite this article: Artūras Dubickas \& Min Sha (2015) Counting and Testing Dominant Polynomials, Experimental Mathematics, 24:3, 312-325, DOI: 10.1080/10586458.2014.992080

To link to this article: http://dx.doi.org/10.1080/10586458.2014.992080
Counting and Testing Dominant Polynomials

Artūras Dubickas¹ and Min Sha²
¹Department of Mathematics and Informatics, Vilnius University, Vilnius, Lithuania
²School of Mathematics and Statistics, University of New South Wales, Sydney, Australia

CONTENTS

1. Introduction
2. Preliminaries
3. Counting Dominant Polynomials
4. Testing Dominant Polynomials
Acknowledgments
Funding
References

2000 AMS Subject Classification: Primary 11C08; Secondary 11B37, 11R06
Keywords: Dominant polynomial, linear recurrence sequence, Sturm’s theorem, Bistritz stability criterion

In this paper, we concentrate on counting and testing dominant polynomials with integer coefficients. A polynomial is called dominant if it has a simple root whose modulus is strictly greater than the moduli of its remaining roots. In particular, our results imply that the probability that what is known as the dominant root assumption holds for a random monic polynomial with integer coefficients tends to 1 in some setting. However, for arbitrary integer polynomials it does not tend to 1. For instance, the proportion of dominant quadratic integer polynomials of height $H$ among all quadratic integer polynomials tends to $(41 + 6 \log 2)/72$ as $H \to \infty$. Finally, we design some algorithms to test whether a given polynomial with integer coefficients is dominant without finding the polynomial’s roots.

1. INTRODUCTION

Consider

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{C}[X]$$

of degree $n \geq 2$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f$. If there exists a unique $\alpha_i$ such that $|\alpha_i| > |\alpha_j|$ for each $j \neq i$, we call $f$ dominant, and $\alpha_i$ is called the dominant root of $f$ (note that such an $\alpha_i$ must be real if $f(X) \in \mathbb{R}[X]$). Dominant polynomials arise in various contexts (see, for instance, the motivation and the results given in [Akiyama et al. 08, Akiyama and Pethő 14a, Akiyama and Pethő 14b]; one can also mention, e.g., linear recurrence sequences).

Recall that every linear recurrence sequence of complex numbers $s_0, s_1, s_2, \ldots$ of order $n \geq 2$ is defined by the linear relation

$$s_{k+n} = a_1s_{k+n-1} + \cdots + a_ns_k \quad (k = 0, 1, 2, \cdots), \quad (1)$$

where $a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, and $s_j \neq 0$ for at least one $j$ in the range $0 \leq j \leq n-1$. The characteristic polynomial of this linear recurrence sequence is

$$f(X) = X^n - a_1X^{n-1} - \cdots - a_n \in \mathbb{C}[X].$$

The linear recurrence sequences having dominant characteristic polynomial—the so-called dominant root assumption
—are often much easier to deal with, especially in considering Diophantine properties of linear recurrence sequences. Let us consider Pisot’s conjecture (Hadamard quotient theorem) as an example. That conjecture, which was proved in [Van der Poorten 88], asserts that if the quotient \( s_n/t_n \) of two linear recurrence sequences \( \{s_n\}_{n \in \mathbb{N}} \) and \( \{t_n\}_{n \in \mathbb{N}} \) is an integer for every \( n \in \mathbb{N} \), then \( \{s_n/t_n\}_{n \in \mathbb{N}} \) is also a linear recurrence sequence. In [Corvaja and Zannier 98, Theorem 1], the authors went further and generalized this conjecture to the case that \( s_n/t_n \) is an integer infinitely often in some setting using the subsequence theorem and under the dominant root assumption. Later, in [Corvaja and Zannier 02, Corollary 1], they removed the dominant root assumption.

In the first part of this paper, we consider how often the dominant root assumption holds for linear recurrence sequences. By counting dominant monic integer polynomials of fixed degree \( n \) and height bounded by \( H \), we find that for fixed \( n \), if in \((1–1)\) we choose \( a_1, \cdots, a_n \) as rational integers, the probability that the dominant root assumption holds tends to 1 as \( H \to \infty \). Combining this with [Dubickas and Sha 15, Theorem 1.1], we see that almost every randomly generated linear recurrence sequence is nondegenerate and has a dominant root; that is, it is exactly what we usually prefer it to be.

In a similar way, we also evaluate the number of dominant (not necessarily monic) integer polynomials of fixed degree and bounded height.

To state our results, we first define the set \( S_n(H) \) of dominant monic integer polynomials of degree \( n \geq 2 \) and height at most \( H \), that is,

\[
S_n(H) = \{ f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : \\
\text{f is dominant, } |a_i| \leq H, \ i = 1, \cdots, n \}.
\]

Similarly, we define

\[
S^*_n(H) = \{ f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : \\
\text{f is dominant, } a_0 \neq 0, \ |a_i| \leq H, \ i = 0, 1, \cdots, n \}.
\]

Then we put \( D_n(H) = |S_n(H)| \) and \( D^*_n(H) = |S^*_n(H)| \).

Below, we shall use the Landau symbol \( O \) and the Vinogradov symbol \( \ll \). Recall that the assertions \( U = O(V) \) and \( U \ll V \) are both equivalent to the inequality \( |U| \leq CV \) with some constant \( C > 0 \). In this paper, without special indication, the constants implied in the symbols \( O \), \( \ll \) depend only on the degree \( n \); moreover, all these constants, except for some constants in Section 4.3.4, can be effectively computed. In the sequel, we always assume that \( H \) is a positive integer (greater than 1 if there is the factor \( \log H \) in the corresponding formula) and that \( n \) is an integer greater than 1.

To determine how often dominant integer polynomials occur, we need to consider the asymptotic behavior of \( D_n(H) \) and that of \( D^*_n(H) \). First, we present a simple asymptotic formula for \( D_n(H) \).

**Theorem 1.1.** For every integer \( n \geq 2 \), we have

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

Theorem 1.1 says that the proportion of dominant monic integer polynomials of degree \( n \) and height at most \( H \) among all the monic integer polynomials of degree \( n \) and height at most \( H \) (there are \((2H+1)^n\) of these) tends to 1 as \( H \to \infty \). Roughly speaking, the dominant monic integer polynomials occur with a probability tending to 1. Moreover, the proof of Theorem 1.1 also implies an error term of the asymptotic formula.

We remark that the total number of real roots of a random polynomial of degree \( n \) (if the coefficients are independent standard normals) is only \( \frac{2}{\sqrt{n}} \log n + c \) as \( n \to \infty \), where \( c \) is an absolute constant (see, e.g., [Edelman and Kostlan 95]). That is, a random polynomial is expected to have many more nonreal roots than real ones. So Theorem 1.1 is a bit surprising. Moreover, for \( 0 < \varepsilon \leq 1 \), we define the set

\[
S_{n,\varepsilon}(H) = \{ f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : \\
\text{f is dominant, } 0 < |a_0| \leq H^{1-\varepsilon}, |a_i| \leq H, \ i = 1, \cdots, n \},
\]

and put \( D_{n,\varepsilon}(H) = |S_{n,\varepsilon}(H)| \). Then we can get a similar asymptotic result.

**Theorem 1.2.** For each \( \varepsilon \) satisfying \( 0 < \varepsilon \leq 1 \) and each integer \( n \geq 2 \), we have

\[
\lim_{H \to \infty} \frac{D_{n,\varepsilon}(H)}{2H^{1-\varepsilon}(2H)^n} = 1.
\]

Selecting \( \varepsilon = 1 \) in \( S_{n,\varepsilon}(H) \), we obtain \( a_0 \in \{-1, 1\} \). Hence \( D_{n,1}(H) = 2D_n(H) \), since half of the polynomials in \( S_{n,1}(H) \) have leading coefficient 1, and half have \(-1\). Thus, Theorem 1.2 with \( \varepsilon = 1 \) implies Theorem 1.1.

However, the situation for \( D^*_n(H) \) is quite different. We can get an explicit asymptotic formula for \( D^*_n(H) \), but for \( n \geq 3 \), we can get only lower and upper bounds.

**Theorem 1.3.** We have

\[
\lim_{H \to \infty} \frac{D^*_n(H)}{(2H)^n} = \frac{41 + 6 \log 2}{72} \approx 0.6272.
\]
2. PRELIMINARIES

Given a polynomial
\[ f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \]
in \( \mathbb{C}[X] \), \( a_0 \neq 0 \), its \textit{height} is defined by \( H(f) = \max_{0 \leq j \leq n} |a_j| \), and its \textit{Mahler measure} by
\[ M(f) = |a_0| \prod_{j=1}^{n} \max\{1, |a_j|\}. \]

For each \( f(X) \in \mathbb{C}[X] \) of degree \( n \), these quantities are related by the following well-known inequality:
\[ 2^{-n} H(f) \leq M(f) \leq \sqrt{n+1} H(f); \tag{2–1} \]
see, for instance, [Waldschmidt 00, (3.12)].

For an algebraic number \( \alpha \in \overline{\mathbb{Q}} \) of degree \( d \), its Mahler measure \( M(\alpha) \) is the Mahler measure of its minimal polynomial \( f \) over \( \mathbb{Z} \). Then for the \textit{(Weil) absolute logarithmic height} \( h(\alpha) \) of \( \alpha \), we have
\[ h(\alpha) = \frac{\log M(\alpha)}{d}. \tag{2–2} \]

Some special forms of polynomials will play an important role here. The one below is nontrivial. It was obtained in [Ferguson 97]; see also a previous result of [Boyd 94].

\[ \text{Lemma 2.1. If } f(X) \in \mathbb{Z}[X] \text{ is an irreducible polynomial that has exactly } m \text{ roots on a circle } |z| = c > 0 \text{ at least one of which is real, then one has } f(X) = g(X^m), \text{ where the polynomial } g(X) \in \mathbb{Z}[X] \text{ has at most one real root on every circle in the plane with center at the origin.} \]

The following lemma concerning the upper bound of the moduli of roots of polynomials is a classical result of [Cauchy 29] (see also [Mignotte and Ţeţeşcu 99, Theorem 2.5.1 and Proposition 2.5.9] or [Mishra 93, Corollary 8.3.2] or [Prasolov 10, Theorems 1.1.2 and 1.1.3]).

\[ \text{Lemma 2.2. All the roots of the polynomial } \]
\[ f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{C}[X] \]
of degree \( n \geq 1 \), where \( a_0 \neq 0 \) and \( (a_1, \ldots, a_n) \neq (0, \ldots, 0) \), are contained in the disk \( |X| = R \), where \( X = R \) is the unique positive solution of the equation
\[ |a_0|X^n - |a_1|X^{n-1} - \cdots - |a_{n-1}|X - |a_n| = 0. \]

In addition, for an arbitrary nonzero root \( x \) of \( f \), we have
\[ \min_{0 \leq i \leq n} |a_i| + \frac{1}{H(f)} + \min_{0 \leq i \leq n} |a_i| < |x| \tag{2–3} \]
\[ < 1 + \frac{1}{|a_0|} \max\{|a_1|, \ldots, |a_n|\}. \]

This lemma will assist us in constructing a family of dominant polynomials explicitly.

For bounding the distance between two distinct roots of a complex polynomial (especially an integer polynomial), the initial work is due to [Mahler 64], and since then, it has been studied extensively. See [Budarina and Gőetz, Bugeaud and Dujella 11, Bugeaud and Dujella 14, Bugeaud and Mignotte 11, Bugeaud and Mignotte 10, Dubickas 13, Evertse 04] for more recent progress, including some nontrivial constructions of polynomials with close roots. Usually, one needs to separate the roots of a polynomial by circles centered at those roots. For our purpose, however, we also need to use separations of roots by annuli centered at the origin. So we need to study the distance between two distinct moduli of roots of an integer polynomial. For this, there are two main tools that we use.

The first is Mahler’s inequality [Mahler 64], asserting that if \( \gamma \) and \( \gamma' \) are two distinct roots of a separable polynomial \( g(X) \in \mathbb{Z}[X] \) of degree \( m \geq 2 \), then
\[ |\gamma - \gamma'| > \sqrt{3} m^{-m/2-1} M(g)^{1-m}. \tag{2–4} \]
Lemma 2.3. Let \( f(X) \in \mathbb{Z}[X] \) be a polynomial of degree \( n \geq 2 \), and let \( \alpha \) and \( \beta \) be two distinct roots of \( f \). Then we have
\[
|\alpha - \beta| > \sqrt[3]{3(n + 1)^{-n/2}}|H(f)|^{1-n}.
\]
(2–5)

The second tool is a Liouville-type inequality. See, e.g., [Waldschmidt 00, Lemma 3.14]. We use the following version, given in [Fel’daman 81]: if \( \gamma_1, \ldots, \gamma_r \) are algebraic numbers with degrees \( d_1, \ldots, d_r \) over \( \mathbb{Q} \), and \( P(z_1, \ldots, z_r) \) is a polynomial with integer coefficients of degree \( N_1, \ldots, N_r \) in the variables \( z_1, \ldots, z_r \), respectively, then either \( P(\gamma_1, \ldots, \gamma_r) = 0 \) or
\[
|P(\gamma_1, \ldots, \gamma_r)| \geq L(P)^{1-kd} \prod_{1 \leq d \leq d_r} M(\gamma_r)^{-N_r/d},
\]
(2–6)
where \( L(P) \) is the sum of the moduli of the coefficients of \( P \), \( d = [Q(\gamma_1, \ldots, \gamma_r) : \mathbb{Q}] \), and \( \delta = 1 \) if the field \( Q(\gamma_1, \ldots, \gamma_r) \) is real, and \( \delta = 1/2 \) if it is complex.

We first consider quadratic integer polynomials.

Lemma 2.4. Let \( f(X) \in \mathbb{Z}[X] \) be a quadratic polynomial. Suppose that \( f \) has two real roots \( \alpha \) and \( \beta \) such that \( |\alpha| \neq |\beta| \). Then we have
\[
|\alpha| - |\beta| \geq |H(f)|^{-1}.
\]

Proof. Let \( f(X) = aX^2 + bX + c = a(X - \alpha)(X - \beta) \). Since \( \alpha \) and \( \beta \) are real, we have \( |\alpha| - |\beta| = |\alpha - \beta| \) or \( |\alpha + \beta| \). In the first case, we obtain
\[
|H(f)^2| |\alpha - \beta|^2 \geq |\alpha|^2 |\alpha - \beta|^2 = |b^2 - 4ac| \geq 1,
\]
which implies the desired result. In the second case, \( \alpha \neq -\beta \), so \( b \neq 0 \). Thus,
\[
|\alpha + \beta| = \frac{|b|}{|a|} \geq \frac{1}{|a|} \geq \frac{1}{H(f)}
\]
again. \( \square \)

Now we consider the general case.

Lemma 2.5. Let \( f(X) \in \mathbb{Z}[X] \) be a polynomial of degree \( n \geq 2 \), and let \( \alpha \) and \( \beta \) be two roots of \( f \) satisfying \( |\alpha| \neq |\beta| \). Then
\[
|\alpha| - |\beta| > 2^{n(n-1)/4}(n + 1)^{-n/4 + n^2/4 + 1/2} H(f)^{-n/2 + n^2/4 + 1/2 - 2}.
\]
if both \( \alpha \) and \( \beta \) are complex (nonreal). If, furthermore, \( \alpha \) is real and \( \beta \) is complex (nonreal), then
\[
|\alpha| - |\beta| \geq 2^{-n(n-1)(n-2)/2}(n + 1)^{-n(n-1)/2} H(f)^{-2n(n-1) - 1}.
\]
(2–7)

Finally, if both \( \alpha \) and \( \beta \) are real, then
\[
|\alpha| - |\beta| > (2n + 1)^{-3n} H(f)^{2-4n}.
\]
(2–8)

Proof. Let us begin with the case that both \( \alpha \) and \( \beta \) are real. If \( \alpha \) and \( \beta \) both have the same sign, then \( |\alpha| - |\beta| = |\alpha - \beta| \). If \( \alpha \) and \( \beta \) have different signs, then \( |\alpha| - |\beta| = |\alpha + \beta| = |\alpha - (-\beta)| \). In both cases, \( \alpha \) and \( \beta \) (or \( -\beta \)) are the roots of the polynomial \( f(X)f(-X) \in \mathbb{Z}[X] \). Its separable part \( g(X) \) (which is the product of the factors of \( f(X)f(-X) \) that are irreducible over \( \mathbb{Q} \) ) has degree at most \( 2n \) and Mahler measure \( M(g) \leq M(f)^2 \). Clearly, \( \alpha \), \( \beta \), and \( -\beta \) are the roots of \( g \).
Applying Mahler’s bound (2–4) and inequality (2–1) to the polynomial \( g \), we obtain
\[
|\alpha| - |\beta| > \sqrt[3]{3(2n)^{-n-1}} M(f)^{2-4n}
\]
\[
> (2n + 1)^{-n-1} \left(\frac{\sqrt{2n + 1} H(f)^2}{2}\right)^{2-4n}
\]
\[
= (2n + 1)^{-3n} H(f)^{2-4n},
\]
as claimed.

Now assume that \( \alpha \) and \( \beta \) are both complex (nonreal). Then \( n \geq 4 \) and
\[
2M(f)|\alpha| - |\beta| \geq 2 \max(|\alpha|, |\beta|)|\alpha| - |\beta|
\]
\[
\geq (|\alpha|^2 - |\beta|^2) = |\alpha \bar{\alpha} - \beta \bar{\beta}|,
\]
so
\[
|\alpha| - |\beta| \geq \frac{|\alpha \bar{\alpha} - \beta \bar{\beta}|}{2M(f)}.
\]
Take a separable polynomial
\[
f_i(X) = c_0(X - \gamma_1) \cdots (X - \gamma_l) \in \mathbb{Z}[X]
\]
dividing \( f(X) \) whose roots contain \( \alpha \) and \( \beta \). Observe that \( \bar{\alpha} \) and \( \bar{\beta} \) are also roots of \( f_i \). Clearly, \( l = \deg f_i \leq n \) and \( M(f_i) \leq M(f) \). Consider a separable polynomial \( g(X) \in \mathbb{Z}[X] \) whose roots contain \( \alpha \bar{\alpha} \) and \( \beta \bar{\beta} \) (which is either the minimal polynomial of \( \alpha \bar{\alpha} \) in \( \mathbb{Z}[X] \), if \( \beta \bar{\beta} \) is conjugate to \( a \bar{\alpha} \), or else it is the product of the minimal polynomial of \( a \bar{\alpha} \in \mathbb{Z}[X] \) and that of \( \beta \bar{\beta} \in \mathbb{Z}[X] \)). It is clear that \( g(X) \) divides the polynomial \( c_0^{l-1} \prod_{1 \leq i < j \leq l} (X - \gamma_i \gamma_j) \in \mathbb{Z}[X] \), so \( \deg g \leq l(l - 1)/2 \leq n(n - 1)/2 \) and
\[
M(g) \leq |c_0|^{l-1} \prod_{1 \leq i < j \leq l} \max(1, |\gamma_i \gamma_j|)
\]
\[
\leq |c_0|^{l-1} \prod_{1 \leq i < j \leq l} \max(1, |\gamma_i|) \max(1, |\gamma_j|)
\]
\[
= |c_0|^{l-1} \prod_{k=1}^l \max(1, |\gamma_k|)^{l-1} = M(f_i)^{l-1}
\]
\[
\leq M(f)^{n-1}.
\]
Now as above, applying Mahler’s bound (2–4) to the pair of roots \(a\alpha, b\beta\) of \(g\) and then inequality (2–1) to the polynomial \(g\), we obtain
\[
\|\alpha - \beta\| \geq \frac{|a\alpha - b\beta|}{2M(f)} > \frac{\sqrt{3}}{2M(f)} \left( \frac{n(n-1)}{2} \right)^{-n(n-1)/4-1} 
\times M(f)^{(n-1)(1-n(n-1)/2)} > 2\left(\sqrt{n + 1}H(f)\right)^{-n(n-1)/2} 
\times 2^{3(n-1)/4(n+1)} - 1)^{-n(n-1)/2 + n/2 - 2} = 2^{n(n-1)/4(n+1)} - 1)^{-n(n-1)/2 + n/2 - 2} \times H(f)^{-n(n-1)/2 + n/2 - 2}.
\]

It remains to consider the case that \(\alpha\) is real and \(\beta\) is complex. By Lemma 2.4, (2–7) is true when \(n = 2\). In the sequel, we assume that \(n \geq 3\).

As above, we obtain
\[
\|\alpha - \beta\| \geq \frac{|a^2 - b\beta|}{2M(f)}.
\]

In order to estimate \(|a^2 - b\beta|\) from below, we shall apply (2–6) to the polynomial \(P(z_1, z_2, z_3) = z_1^2 - z_2z_3\) at the point \((z_1, z_2, z_3) = (\alpha, \beta, \beta)\). We then have \(N_1 = 2, N_2 = N_3 = 1, L(P) = 2, \delta = 1/2,\) and \(d = [Q(\alpha, \beta, \beta) : Q] \leq n(n-1)(n-2)\). Also,
\[
d = \frac{[Q(\alpha, \beta, \beta) : Q]}{[Q(\alpha) : Q]} = [Q(\alpha, \beta, \beta) : Q(\alpha)] 
\leq [Q(\beta, \beta) : Q] \leq n(n-1),
\]

and similarly, \(d/d_2 = d/d_3 \leq n(n-1)\). Thus, applying (2–6), we find in view of \(M(\beta) = M(\beta)\) that
\[
|a^2 - b\beta| \geq 2^{1-n(n-1)(n-2)/2}M(\alpha)^{-n(n-1)/2}M(\beta)^{-n(n-1)/2}.
\]

Now from \(M(\alpha) \leq M(f)\), \(M(\beta) \leq M(f)\), and (2–9), we deduce
\[
\|\alpha - \beta\| \geq 2^{n(n-1)(n-2)/2}M(f)^{-2n(n-1)-1}.
\]

By (2–1), we have
\[
M(f)^{2n(n-1)+1} \leq (n + 1)^{n(n-1)+1/2}H(f)^{2n(n-1)+1}.
\]

Hence
\[
\|\alpha - \beta\| \geq 2^{n(n-1)(n-2)/2}M(f)^{-2n(n-1)-1} \times H(f)^{-2n(n-1)-1}.
\]

This completes the proof of the lemma.

In Lemma 2.5, if \(f(X)\) is irreducible and \(n \geq 3\), then (2–7) can be replaced by the following:
\[
\|\alpha - \beta\| \geq 2^{n(n-1)(n-2)/2}(n + 1)^{(n-1)(n-2)/2}H(f)^{-2(n-1)(n-2)-1},
\]

because \(d/d_i \leq (n-1)(n-2)\) for \(i = 1, 2, 3\). This will make sense for computations.

We conclude this section with the following lemma, which gives a lower bound better than (2–8) for irreducible polynomials of lower degrees (for example, of degree \(n\) with \(2 \leq n \leq 11\) and arbitrary height).

**Lemma 2.6.** Let \(f \in \mathbb{Z}[X]\) be an irreducible polynomial of degree \(n \geq 2\), \(\alpha\) and \(\beta\) two real roots of \(f\). If \(|\alpha| \neq |\beta|\), then we have
\[
\|\alpha - \beta\| \geq \exp(-[Q(|\alpha| - |\beta|) : Q]h(|\alpha| - |\beta|)).
\]

**Proof:** By Liouville’s inequality (see [Waldschmidt 00, (3.13)]), we have
\[
\|\alpha - \beta\| \geq \exp\left(-\frac{[Q(|\alpha| - |\beta|) : Q]}{[Q(\alpha) : Q]}h(|\alpha| - |\beta|)\right).
\]

Note that \(\alpha\) and \(\beta\) are two real algebraic numbers, and we have
\[
[Q(|\alpha| - |\beta|) : Q] \leq [Q(\alpha, \beta) : Q] \leq n(n-1).
\]

In addition, combining some basic properties of the height function with (2–1) and (2–2), we have
\[
h(|\alpha| - |\beta|) \leq h(|\alpha|) + h(|\beta|) + \log 2 
\leq h(|\alpha|) + h(|\beta|) + \log 2 
= \frac{2\log M(f)}{n} + \log 2 
\leq \frac{2}{n} \log H(f) + \frac{1}{n} \log(n + 1) + \log 2.
\]

Collecting the above inequalities, we derive the desired result.

\[\Box\]

### 3. COUNTING DOMINANT POLYNOMIALS

We first give several families of dominant polynomials.

**Lemma 3.1.** Let \(f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]\). Suppose that \(f\) is irreducible. If either \(a_0 > 0\) and \(a_i < 0\) for \(1 \leq i \leq n\) or \(a_0 < 0\) and \(a_i > 0\) for \(1 \leq i \leq n\), then \(f\) is dominant.

**Proof:** Since either \(a_0 > 0\) and \(a_1, \cdots, a_n < 0\) or \(a_0 < 0\) and \(a_1, \cdots, a_n > 0\), it follows by Lemma 2.2 that \(f\) has a unique positive root \(R\) such that all the other
Lemma 3.2. Let \( f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{C}[X] \). If \(|a_1| > n(n+1)^{1/4}|a_0|^{1/2} H(f)^{1/2}\), then \( f \) is dominant.

Proof. Let \( R \) be the largest modulus of the roots of \( f \). Suppose that \( f \) is not dominant, that is, that it has at least two roots on the circle \(|z| = R\). Then by the definition of the Mahler measure, we must have \( R^2 \leq M(f)/|a_0| \). Noting that \(|a_1| \leq nR|a_0| \) and applying (2–1), we obtain

\[
|a_1| \leq n(n+1)^{1/4}|a_0|^{1/2} H(f)^{1/2},
\]

which contradicts our assumption. 

Lemma 3.3. Let

\[
f(X) = (X-a)(a_0X^{n-1} + a_1X^{n-2} + \cdots + a_{n-1}) \in \mathbb{C}[X]
\]

be of degree \( n \geq 2 \). If either \(|a| \geq 2 \) and \(|a_0| \geq |a_i| \) for \( 1 \leq i \leq n-1 \), or \(|a| \geq \sqrt{H(f)} + n - 1 \) and \(|a_0| \geq 1 \), then \( f \) is dominant.

Proof. First, suppose that \(|a| \geq 2 \) and \(|a_0| \geq |a_i| \) for \( 1 \leq i \leq n-1 \). Then by (2–3), the roots of \( a_0X^{n-1} + a_1X^{n-2} + \cdots + a_{n-1} \) are strictly inside the circle

\[
|z| = 1 + \frac{1}{|a_0|} \max(|a_1|, \cdots, |a_{n-1}|) \leq 2.
\]

So \( a \) is a dominant root of \( f \), and thus \( f \) is dominant.

Next, suppose that \(|a_0| \geq 1 \) and \(|a| \geq \sqrt{H(f)} + n - 1 \). Note that

\[
f(X) = a_0X^n + (a_1 - a_0a)X^{n-1} + \cdots + (a_{n-1} - aa_{n-2})X - a_{n-1}.
\]

Since \(|a| > \sqrt{H(f)} \) and \( H(f) \geq 1 \), we obtain \(|a_i| < \sqrt{H(f)} + n - 1 - i \) for \( 0 \leq i \leq n - 1 \). By (2–3), the moduli of the roots of \( a_0X^{n-1} + a_1X^{n-2} + \cdots + a_{n-1} \) are less than

\[
1 + \frac{1}{|a_0|} \max(|a_1|, \cdots, |a_{n-1}|) < \sqrt{H(f)} + n - 1,
\]

where the inequality comes from \(|a_0| \geq 1 \). So \( a \) is a dominant root of \( f \), and thus \( f \) is a dominant polynomial. 

Here we also give two families of nondominant polynomials, which can help us to prove Theorem 1.4.

Lemma 3.4. For \( n \geq 2 \) an even integer, let \( f(X) = a_0X^n - a_1X^{n-1} + a_2X^{n-2} + \cdots + a_n \in \mathbb{R}[X] \) with \( a_i > 0 \) for each

\[0 \leq i \leq n, \text{ and } a_0 \geq a_1, a_2 \geq a_3, \cdots, a_{n-2} \geq a_{n-1}, a_n \geq a_0.\]

Then \( f \) is nondominant.

Proof. Let \( x \) be any positive real root of \( f \). Then

\[0 = f(x) > a_0x^n - a_1x^{n-1} = x^{n-1}(a_0x - a_1),\]

which yields \( x < a_1/a_0 \leq 1 \).

Set \( g(X) = f(-X) \). Then the negative real roots of \( f(X) \) are exactly the positive real roots of \( g(X) \). Since

\[g(X) = a_0X^n + a_1X^{n-1} + a_2X^{n-2} - a_3X^{n-3} + \cdots + a_{n-2}X^2 - a_{n-1}X + a_n,
\]

it is easy to see that \( g(x) > 0 \) for every real \( x \geq 1 \) (clearly, for \( n = 2 \) the polynomial \( g(X) \) has no positive roots). Thus, all the real roots of \( f(X) \) lie in the interval \((-1, 1)\).

Moreover, writing \( f(X) \) as \( f(X) = a_0\prod_{i=1}^n (X-a_i) \), we obtain \( a_n = (-1)^na_0\prod_{i=1}^n a_i = a_0\prod_{i=1}^n a_i \). Since \( a_n \geq a_0 > 0 \), we see that \(|a_i| \geq 1 \) for at least one index \( i \). So not all the roots of \( f(X) \) lie strictly inside the unit circle. It follows that the largest in modulus root of \( f \) is complex (nonreal); thus \( f(X) \) is nondominant.

Lemma 3.5. For \( n \) an odd integer, let \( f(X) = a_0X^n - a_1X^{n-1} + a_2X^{n-2} + \cdots + a_n \in \mathbb{R}[X] \) with \( a_i > 0 \) for \( 0 \leq i \leq n \), and \( a_0 \geq a_1, a_2 \geq a_3, \cdots, a_{n-1} \geq a_n, a_n \geq a_0. \) Then \( f \) is nondominant.

Proof. The proof is the same as that of Lemma 3.4, the sole difference being that here, one should consider \( g(X) = -f(-X) \).

Using some of the above polynomial families, we will now prove the theorems stated in Section 1.

Proof of Theorem 1.1. Consider the polynomial

\[f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X],\]

where \( H(f) \leq H \) and \(|a_1| > n(n+1)^{1/4}H^{1/2}\). By Lemma 3.2, we have \( f \in S_0(H) \). Note that for each sufficiently large \( H \), the number of such polynomials \( f \) is at least

\[(2H + 1)^{n-1/2} (H - n(n+1)^{1/4}H^{1/2})\],

which implies the desired result. 

Proof of Theorem 1.2. Clearly,

\[D_{n,\alpha}(H) \leq 2H^{1-\alpha}(2H + 1)^\alpha.\]

For the lower bound, consider the polynomials

\[f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]\]
Proof of Theorem 1.3. It is easy to see that the quadratic polynomials satisfying

\[ f, \quad 0 < |a_0| \leq H^{1-\epsilon}, \]
\[ |a_1| > n(n+1)^{1/4}|a_0|^{1/2}H^{1/2}. \]

Lemma 3.2 implies that \( f \in S_{n,e}(H) \). Observe that the number of such polynomials \( f \) is asymptotic to

\[ (2H)^{n-1} \cdot 4 \sum_{a_0=1}^{[H^{1-\epsilon}]} (H - \left\lfloor cH^{1/2}a_0^{1/2} \right\rfloor) \]

as \( H \to \infty \), where \( c = n(n+1)^{1/4} \), which is asymptotic to

\[ 4(2H)^{n-1} \int_1^{H^{1-\epsilon}} (H - cH^{1/2}x^{1/2}) \, dx \]

as \( H \to \infty \). Since the above integral is equal to

\[ H^{2-\epsilon} - \frac{2}{3}cH^{2-3\epsilon/2} + \frac{2}{3}cH^{1/2} - H, \]

the main term approaches \( 4(2H)^{n-1}H^{2-\epsilon} = 2H^{1-\epsilon}(2H)^n \) as \( H \to \infty \). This gives the desired result. \( \square \)

Proof of Theorem 1.4. Consider the polynomial

\[ f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X], \]

where \( H(f) \leq H \) and \( |a_1| > n(n+1)^{1/4}|a_0|^{1/2}H^{1/2} \). By Lemma 3.2, we have \( f \in S_n^e(H) \). Set \( c = n(n+1)^{1/4} \). The number of such polynomials \( f \) is asymptotic to

\[ (2H)^{n-1} \cdot 4 \sum_{a_0=1}^{[H^{1/2}]} (H - \left\lfloor cH^{1/2}a_0^{1/2} \right\rfloor) \]

as \( H \to \infty \), which is asymptotic to the following integral:

\[ 4(2H)^{n-1} \int_1^{H^{1/2}} (H - cH^{1/2}x^{1/2}) \, dx \]

as \( H \to \infty \). Note that the main term in the above integral is \( H^2/(3c^2) \) as \( H \to \infty \). The main term for the number of such polynomials \( f \) is thus \( (2H)^{n+1}/(3c^2) \), which gives the desired upper bound of the lower limit.

Now we want to derive the claimed upper bound for the upper limit. If \( n \) is even, we will count the polynomials \( f(X) \) with integer coefficients as in Lemma 3.4. Since \( a_n \geq a_0 \geq a_1 \) and \( a_{2i} \geq a_{2i+1} \) for each \( i = 1, \cdots, n/2 - 1 \), it is easy to find that the number of these polynomials \( f(X) \) is asymptotic to

\[ \frac{H^3}{6} \left( \frac{H^2}{2} \right)^{n/2-1} \]

as \( H \to \infty \). Note that \( f(-X), -f(X), \) and \( -f(-X) \) are also nondominant, and they are distinct polynomials. So as \( H \to \infty \), we get \( H^{n+1}/(3 \cdot 2^{n/2-2}) \) nondominant polynomials. Thus, we have

\[ \limsup_{H \to \infty} D_n^e(H)/(2H)^{n+1} \leq 1 - \frac{1}{3 \cdot 2^{3n/2-3}}, \]

where \( n \) is even.

If \( n \) is odd, then similarly, the number of polynomials \( f(X) \) with integer coefficients as in Lemma 3.5 (therefore satisfying \( a_{n-1} \geq a_0 \geq a_1 \) and \( a_{2i} \geq a_{2i+1} \) for \( i = 1, \cdots, (n-3)/2 \)) is asymptotic to

\[ \frac{H^4}{24} \left( \frac{H^2}{2} \right)^{(n-3)/2} \]

as \( H \to \infty \). As \( H \to \infty \), multiplying by 4 as above, we also get \( H^{n+1}/(3 \cdot 2^{(n-1)/2}) \) nondominant polynomials. Thus, for \( n \),

\[ \limsup_{H \to \infty} D_n^e(H)/(2H)^{n+1} \leq 1 - \frac{1}{3 \cdot 2^{3n/2-4}}, \]
odd, we obtain
\[
\limsup_{H \to \infty} D_x^e(H)/(2H)^{a+1} \leq 1 - \frac{1}{3 \cdot 2^{3(n+1)/2}},
\]
as claimed.

Consider cubic polynomials \( f(X) = a_0 X^3 + a_1 X^2 + a_2 X + a_3 \in \mathbb{Z}[X] \) with \( H(f) \leq H \). The number of these polynomials \( f \) with discriminant zero or \( a_1 a_2 a_3 \) zero is \( O(H^3) \), and the number of such reducible polynomials \( f \) is also \( O(H^3) \). It is well known that \( f \) has three distinct real roots if its discriminant \( \Delta \) is positive, and that it has two conjugate complex roots if \( \Delta < 0 \). So in particular, \( f \) is dominant if \( \Delta > 0 \). If \( f \) is irreducible, \( \Delta < 0 \), and \( a_1 a_2 a_3 \neq 0 \), then not all three roots of \( f \) lie on the same circle in view of Lemma 2.1; hence, either \( f(X) \) or its reciprocal polynomial \( X^3 f(X^{-1}) \) is dominant. Thus, at least half of all cubic integer polynomials \( f \) are dominant.

4. TESTING DOMINANT POLYNOMIALS

In this section, we will design some algorithms to test whether a given polynomial \( f \in \mathbb{Z}[X] \) is dominant without finding the polynomial roots. We first recall Sturm’s theorem and the Bistritz stability criterion.

4.1. Sturm’s Theorem

For an arbitrary real sequence \( a_0, a_1, \cdots, a_n \), its number of sign changes is determined as follows: one first deletes all the zero terms of the sequence. Then for the remaining nonzero terms, one counts the number of pairs of neighboring terms of opposite sign.

Given a polynomial \( f(X) \in \mathbb{R}[X] \), applying Euclid’s algorithm to \( f(X) \) and its derivative yields the following construction:

\[
\begin{align*}
p_0(X) &: = f(X), \\
p_1(X) &: = f'(X), \\
p_2(X) &: = \text{rem}(p_0(X), p_1(X)) = p_1(X)q_0(X) - p_0(X), \\
p_3(X) &: = \text{rem}(p_1(X), p_2(X)) = p_2(X)q_1(X) - p_1(X), \\
& \quad \vdots \\
0 &= \text{rem}(p_{m-1}(X), p_m(X)),
\end{align*}
\]

with \( p_m(X) \neq 0 \), where \( \text{rem}(p_1(X), p_2(X)) \) and \( q_i(X) \) are respectively the remainder and the quotient of the polynomial division of \( p_i(X) \) by \( p_j(X) \).

We now state Sturm’s theorem; see [Prasolov 10, Theorem 1.4.3].

**Theorem 4.1.** Let \( f(X), p_0(X), p_1(X), \cdots, p_m(X) \) be as above. For \( x \in \mathbb{R} \), let \( \sigma(x) \) be the number of sign changes of the sequence

\[
p_0(x), p_1(x), \cdots, p_m(x).
\]

Given real numbers \( a, b \) with \( a < b \), suppose that \( f(a) f(b) \neq 0 \). Then the number of distinct real roots of \( f(X) \) in the interval \((a, b)\) is equal to \( \sigma(a) - \sigma(b) \).

4.2. The Bistritz Stability Criterion

We say that a real polynomial is stable if all of its roots lie strictly inside the unit circle. The Bistritz stability criterion, arising from signal processing and control theory and developed by Yuval Bistritz, is a simple method to determine whether a given real polynomial is stable; see [Bistritz 84] for more details and also [Bistritz 86, Bistritz 02].

For a real polynomial \( f(X) \in \mathbb{R}[X] \) of degree \( n \geq 1 \), we denote by \( f^*(X) \) the reciprocal polynomial of \( f(X) \), that is, \( f^*(X) = X^n f(1/X) \).

Consider \( A_n(X) = a_0 X^n + \cdots + a_n \in \mathbb{R}[X] \), where \( n \geq 2 \), \( a_0 \neq 0 \), and \( A_n(1) \neq 0 \). (If \( A_n(1) = 0 \), the polynomial is not stable.) We assign to \( A_n(X) \) a sequence of symmetric polynomials \( T_m(X) = T_m^*(X), m = n, n-1, \cdots, 0 \), created by a three-term polynomial recurrence as follows.

**Initialization:**

\[
\begin{align*}
T_n(X) &= A_n(X) + A_n^*(X), \\
T_{n-1}(X) &= \frac{A_n(X) - A_n^*(X)}{X - 1}.
\end{align*}
\]

**Recurrence:** for \( k = n, n-1, \cdots, 2 \), define

\[
T_{k-2}(X) = \frac{\delta_k(X+1)T_{k-1}(X) - T_k(X)}{X},
\]

where \( \delta_k = T_k(0)/T_{k-1}(0) \). This recurrence requires the normal conditions

\[
T_{k-1}(0) \neq 0, \quad k = n, \cdots, 1,
\]

which mean that each polynomial \( T_{k-1}(X) \) is of degree \( k - 1 \). The recurrence is interrupted when \( T_{k-1}(0) = 0 \) occurs \( (k \geq 2) \), which corresponds to a singular case.

We divide the singular cases into the following two classes:

the case \( T_{k-1}(1) = 0 \) is called a first-type singularity, and the case \( T_{k-1}(0) = 0 \) but \( T_{k-2}(1) \neq 0 \) is called a second-type singularity. There is a necessary and sufficient condition for the occurrence of a first-type singularity.

**Theorem 4.2.** Let \( A_n(X) \in \mathbb{R}[X] \) be of degree \( n \geq 2 \). Then in the normal conditions for \( A_n(X) \), a first-type singularity occurs if and only if \( A_n(X) \) has roots on the unit circle or a reciprocal pair of roots \((x, x^{-1})\).
Based on Theorem 4.2, we will see later that for our purpose, essentially we do not need to be afraid of first-type singularities; see Lemma 4.4.

However, the appearance of a second-type singularity does not correspond to a special pattern of location of the roots, except that it implies an unstable polynomial. So here, we need not correspond to a special pattern of location of the roots, essentially we do not need to be afraid of first-type singularities. Proceeding from \( n \) to 1, if \( k \) is the first integer for which \( T_k(0) = 0 \) and \( T_{k-1}(X) \neq 0 \), we replace \( T_k(X) \) and \( T_{k-1}(X) \) by

\[
T_k(X) + (X - 1)T_{k-1}(X)(X^q - X^{-q})
\]

and

\[
T_{k-1}(X)(K + X^q + X^{-q}), \quad K > 2,
\]

where \( q \) is the multiplicity of \( T_{k-1}(X) \) at \( X = 0 \), and \( K \) is an arbitrary real constant greater than 2; after this replacement, we can see that \( T_{k-1}(0) \neq 0 \). Then we return to the recurrence (4–2). As soon as we encounter a second-type singularity, we apply the same treatment again. Finally, we will also obtain the sequence \( T_0(X) \), \( T_0(X) \), \( T_0(X) \), \( T_0(X) \),

**Theorem 4.3.** Let \( A_n(X), T_0(X), \ldots, T_n(X) \) be as above (including the situation that a second-type singularity occurs). Define \( v_n \) as the number of sign changes of the sequence

\[
T_n(1), \ldots, T_0(1).
\]

Then \( A_n(X) \) is stable if and only if the normal conditions hold and \( v_n = 0 \). Furthermore, if the normal conditions hold or only a second-type singularity occurs, then \( A_n(X) \) has \( v_n \) roots strictly outside the unit circle and \( n - v_n \) roots strictly inside the unit circle (counted with multiplicity).

### 4.3. Algorithms for Testing Dominant Polynomials

For a quadratic real polynomial \( f = aX^2 + bX + c \in \mathbb{R}[X] \), the testing problem is easy, because \( f \) is dominant if and only if \( b \neq 0 \) and \( b^2 - 4ac > 0 \). We shall now apply Sturm’s theorem and the Bistritz stability criterion to design general algorithms for testing dominant integer polynomials.

There are several ways to design such a general algorithm. We first present a simple algorithm (see Algorithm 1) as a comparison, and we then provide a more efficient one in practice (see Algorithm 3). Finally, we will give a slight improvement of Algorithm 3 in the case of irreducible polynomials; see Algorithm 4.

#### 4.3.1. The General Case

Following (2–5) and (2–7), for a polynomial \( f \in \mathbb{Z}[X] \) of degree \( n \geq 2 \), we define

\[
d_1(f) = 2^{-n(n-1)(n-2)/2(n + 1)}^{-n(n-1)-1/2} H(f)^{-2n(n-1)}
\]

and

\[
d_2(f) = \sqrt{3}(n + 1)^{-n/2} H(f)^{1-n}.
\]

Moreover, for \( f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] \), we define

\[
C_1(f) = \frac{1}{1 + H(f)}
\]

and

\[
C_2(f) = 1 + \frac{1}{\max(|a_1|, \ldots, |a_n|)}.
\]

Then by (2–3), every root of \( f \) is of modulus greater than \( C_1(f) \) and less than \( C_2(f) \).

Given a polynomial \( f(X) \in \mathbb{Z}[X] \) and a real root \( x \) of \( f \), if \( x \) is located in a small annulus \( r < |x| < R \) with \( R - r < d_1(f) \), then by (2–7), we can see that there are no roots of \( f \) located in this annulus with modulus not equal to \( |x| \).

**Lemma 4.4.** Let \( f(X) \in \mathbb{Z}[X] \) be of degree \( n \geq 2 \), and assume that there is a real root \( x \) of \( f \) lying in the annulus \( r < |x| < R \), where \( R - r \leq \frac{1}{2}d_1(f) \). We define \( g(X) = f(rX) \), and consider the normal conditions of \( g(X) \). If a first-type singularity occurs, then \( f \) has a root \( y \) such that \( |y| > |x| \).

**Proof.** Suppose that a first-type singularity occurs for \( g(X) \). By Theorem 4.2, we know that \( g(X) \) has roots on the unit circle or a reciprocal pair of roots.

If \( g(X) \) has a root \( \alpha \) on the unit circle, then \( r\alpha \) is a root of \( f \), and \( |r\alpha| = r \). But by the choice of \( r \) and \( R \), \( f \) has no roots on the circle \( |x| = r \). This is a contradiction, so \( g(X) \) has a reciprocal pair of roots.

In the sequel, we let \( (\alpha, \alpha^{-1}) \) be this reciprocal pair roots of \( g(X) \) with \( |\alpha| < 1 \). So \( f \) has roots \( r\alpha \) and \( r\alpha^{-1} \).

Assume that \( |r\alpha^{-1}| = |x| \). Since \( |r\alpha| < r < |x| \), we have

\[
0 < |x| - |r\alpha| = |x| - \frac{r^2}{|x|} < R - \frac{r^2}{R} \leq \left(1 + \frac{r}{R}\right) \cdot \frac{1}{2}d_1(f) < d_1(f). \tag{4–3}
\]

Note that both \( x \) and \( r\alpha \) are roots of \( f \), and \( x \) is real. Therefore, (4–3) contradicts (2–7).

Now assume that \( |r\alpha^{-1}| < |x| \). Since \( |\alpha^{-1}| > 1 \), we have

\[
0 < |x| - |r\alpha^{-1}| < |x| - r < R - r \leq \frac{1}{2}d_1(f).
\]

As above, this also yields a contradiction.
Thus, we must have $|ra^{-1}| > |x|$. So $ra^{-1}$ is exactly a root we need, and this completes the proof.

Now we will explain Algorithm 1 step by step.

Step 1: Let $R_+$ be the largest positive root of $f$ (if it exists), and let $R_-$ be the largest modulus of the negative roots of $f$ (if it exists). Suppose that $R_+$ exists. Applying Algorithm 2 to $f$ in the interval $(C_1(f), C_2(f))$ by setting $d = \frac{1}{2}d_1(f)$, we locate the positive root $R_+$ in an annulus $r_1 < |z| < R_1$ such that $R_1 - r_1 \leq \frac{1}{2}d_1(f)$. Then we apply a similar algorithm to $f$ in the interval $(-C_2(f), -R_1)$. Note that we might have $R_1 = C_2(f)$, but this case also can be excluded by Sturm’s theorem. If there are no roots located in this interval, then return $r = r_1, R = R_1$; otherwise, we can find an annulus $r_2 < |z| < R_2$ such that $r_2 < R_-. < R_2$ and $R_2 - r_2 \leq \frac{1}{2}d_1(f)$, in which case return $r = r_2, R = R_2$. If $R_+$ does not exist, we search for negative roots of $f$ in the interval $(-C_2(f), -C_1(f))$.

Step 2: Since $g(X)$ already has a real root strictly outside the unit circle, it is not stable. So the normal conditions of $g(X)$ may not hold. When a first-type singularity occurs, we see by Lemma 4.4 that $f$ is not dominant. If the normal conditions hold or only a second-type singularity occurs, then following the discussion in Section 4.2, we construct the sequence $T_n(X), \ldots, T_0(X)$ and compute the number of sign changes $\nu_n$ of the sequence $T_n(1), \ldots, T_0(1)$. Then by Theorem 4.3, $g(X)$ has $\nu_n$ roots strictly outside the unit circle.

Step 3: If $g(X)$ has only one root strictly outside the unit circle ($\nu_1 = 1$), then $f$ has only one root strictly outside the circle $|z| = R$. Since we already know that there exists one real root located in the annulus $r < |z| < R$, we can deduce that $f$ is dominant. Otherwise, $f$ is not dominant.

**Algorithm 1** Simple test of dominant polynomials

**Require:** polynomial $f(X) \in \mathbb{Z}[X]$ of degree $n \geq 2$.

**Ensure:** $1$ ($f$ is dominant) or $0$ ($f$ is not dominant).

1: Use Sturm’s theorem to locate a real root with the largest modulus among the real roots of $f$ in a small annulus $r < |z| < R$ such that $R - r \leq \frac{1}{2}d_1(f)$. If no nonzero real roots exist, return $0$.

2: Let $g(X) = f(rX)$, and apply the Bistritz stability criterion to calculate the number of roots of $g(X)$ strictly outside the unit circle.

3: If $g(X)$ has only one root strictly outside the unit circle, then return $1$; otherwise, return $0$.

4.3.2. The General Case II.

Since the lower bound $d_1(f)$ in (2–7) will become very small for large $n$, Algorithm 1 will be less efficient for polynomials of higher degrees. We will use here the lower bound $d_2(f)$ in (2–5) to design a more efficient algorithm; see Algorithm 3.

We explain now briefly Algorithm 3 step by step.

Step 1: the explanation is the same as for Step 1 of Algorithm 1, except that we apply Algorithm 2 by setting $d = d_2(f)$.

Step 2: if $g$ is not stable, then $f$ has roots on or strictly outside the circle $|z| = R$. Note that all the real roots of $f$ are strictly inside the circle $|z| = R$, so we can judge that $f$ is not dominant.

Step 3: if $g$ is stable, we have to narrow the annulus to ensure that it contains no complex (nonreal) roots.

Steps 4 and 5: the explanations are the same as for Steps 1 and 1 of Algorithm 1.

In Algorithm 3, we first apply the lower bound $d_2(f)$ to locate a real root with the largest modulus among all real roots. If $f$ is not dominant, then the process is likely to stop in Step 3; otherwise, we will use the lower bound $d_1(f)$ to narrow the small annulus $r < |z| < R$. Clearly, Algorithm 3 is more efficient than Algorithm 1, especially in testing a large number of polynomials at the same time, as in Section 4.4.
Algorithm 3 Efficient test of dominant polynomials

Require: polynomial \( f(X) \in \mathbb{Z}[X] \) of degree \( n \geq 2 \).
Ensure: 1 (\( f \) is dominant) or 0 (\( f \) is not dominant).

1: Use Sturm’s theorem to locate a real root with the largest modulus among the real roots of \( f \) in a small annulus \( r < |z| < R \) such that \( R - r \leq d_1(f) \). If no nonzero real roots exist, return 0.
2: Let \( g(X) = f(RX) \), and apply the Bistritz stability criterion to test whether \( g(X) \) is stable. If \( g \) is not stable, then return 0; otherwise, execute the following steps.
3: Similarly to Step 3, use Sturm’s theorem to narrow the annulus \( r < |z| < R \), and then obtain a new annulus \( r_1 < |z| < R_1 \) with \( R_1 - r_1 \leq \frac{1}{2}d_1(f) \), where the real root is located.
4: Let \( h(X) = f(r_1X) \), and apply the Bistritz stability criterion to calculate the number of roots of \( h(X) \) strictly outside the unit circle.
5: If \( h(X) \) has only one root strictly outside the unit circle, then return 1; otherwise, return 0.

4.3.3. Irreducible Polynomials

Algorithm 3 is applicable to all integer polynomials of degree at least 2. However, for irreducible integer polynomials, we can make a slight improvement in Algorithm 3; see Algorithm 4 below. In comparing it with Algorithm 3, we see that we need to explain only the following steps.

Step 1: we gather all the exponents of \( X \) in \( f \) whose coefficients are nonzero, then compute their greatest common divisor. If it is greater than 1, then \( f \) has such a form, and thus \( f \) is not dominant.

Step 4: we change the condition of Step 5 in Algorithm 2 to \( b - a \geq d_1(f) \), because here we do not need to use Lemma 4.4.

Step 6: if \( h(X) \) is stable, then all the roots of \( f \) are strictly inside the circle \( |z| = R_1 \). Note that \( f \) has a real root, say \( \alpha \), lying in the annulus \( r_1 < |z| < R_1 \). If there exists another root lying in this annulus, then it must have modulus \( |\alpha| \) by the choice of \( r_1 \) and \( R_1 \). Thus, by Lemma 2.1, \( f \) is a polynomial with respect to \( X^m \) for some integer \( m \geq 2 \); but this was excluded in Step 4. It follows that \( \alpha \) is the dominant root of \( f \), and so \( f \) is dominant.

In addition, if \( n \geq 3 \), then by the discussion below Lemma 2–5, we can let \( d_1(f) \) be the following:

\[
2^{-(n-1)(n-2)/2}(n+1)^{-(n-1)(n-2)-1/2} \times H(f)^{-(n-1)(n-2)-1}.
\]

We also would like to point out that an irreducible polynomial \( f \in \mathbb{Z}[X] \) has no roots in the rational numbers, and so we can drop Steps 2 and 2 in Algorithm 2.

Algorithm 4 Test of dominant irreducible polynomials

Require: irreducible polynomial \( f \in \mathbb{Z}[X] \) of degree \( n \geq 2 \).
Ensure: 1 (\( f \) is dominant) or 0 (\( f \) is not dominant).

1: Check whether \( f \) is a polynomial with respect to \( X^m \) for some integer \( m \geq 2 \). If yes, return 0; otherwise, execute the following steps.
2: Use Sturm’s theorem to locate a real root with the largest modulus among the real roots of \( f \) on a small annulus \( r < |z| < R \) such that \( R - r \leq d_2(f) \). If no nonzero real roots exist, return 0.
3: Let \( g(X) = f(RX) \), and apply the Bistritz stability criterion to test whether \( g(X) \) is stable. If \( g \) is not stable, then return 0; otherwise, execute the following steps.
4: Similarly to Step 4, use Sturm’s theorem to narrow the annulus \( r < |z| < R \), and then obtain a new annulus \( r_1 < |z| < R_1 \) with \( R_1 - r_1 \leq d_1(f) \), where the real root is located.
5: Let \( h(X) = f(R_1X) \), and apply the Bistritz stability criterion to test whether \( h(X) \) is stable.
6: If \( h(X) \) is stable, then return 1; otherwise, return 0.

4.3.4. Complexity.

Finally, we want to estimate the time complexity of Algorithms 1, 3, and 4.

Here, the time complexity means the total number of required arithmetic operations (multiplication and addition). We omit the running times for comparisons and decisions, because they can be ignored when compared to the time required for arithmetic operations.

In fact, we need to count only the running time that is devoted to applying Sturm’s theorem and the Bistritz stability criterion. According to [Bistritz 86, Section 4], testing the Bistritz stability criterion needs \( O(n^2) \) additions and multiplications.

For applying Sturm’s theorem to a given polynomial \( f \) of degree \( n \), we first need to compute the sequence \( p_0(X), p_1(X), \ldots, p_m(X) \) using polynomial long division. Note that for two polynomials \( g(X), h(X) \in \mathbb{Z}[X] \) with \( \deg g \geq \deg h \), polynomial long division of \( g \) by \( h \) needs at most \( 2 \deg h(\deg g - \deg h + 1) \) arithmetic operations. So computing the above sequence for \( f \) requires \( O(n^2) \) arithmetic operations.

For a given \( f(X) \in \mathbb{Z}[X] \) with \( \deg f = n \), we use Horner’s method (see [Mignotte and Ștefănescu 99, Section 1.2.2]) to compute the evaluation of \( f \) at a point \( X = a \). This requires \( 2n \) arithmetic operations. Thus, one call of Sturm’s theorem needs \( O(n^2) \) arithmetic operations. In view of Algorithm 2 and the
definitions of \( d_1(f) \), \( C_1(f) \), and \( C_2(f) \), there are about \( n^3 + n^2 \log H(f) \) (up to a constant time) calls of Sturm’s theorem.

Therefore, most of the running time is used in applying Sturm’s theorem repeatedly, and the time complexity of Algorithm 1 is \( O(n^5 + n^4 \log H(f)) \).

However, if \( f \) is not dominant, then the time complexity to test \( f \) using Algorithm 3 or 4 is likely to be \( O(n^3 \log n + n^3 \log H(f)) \). In general, the time complexity of each of Algorithms 3 and 4 is also \( O(n^5 + n^4 \log H(f)) \).

If we know beforehand that \( f \) has only real root, then in Algorithm 3, we can drop Step 3 and let \( h(X) = f(rX) \) in Step 3. In that case, the complexity will be \( O(n^3 \log n + n^3 \log H(f)) \).

**Remark 4.5.** According to Section 4.3.4, most of the running time is devoted to locating the real root with the largest modulus among all the real roots of the given polynomial. In view of Algorithms 1 and 3, our strategy is to apply Sturm’s theorem. Although our method is very simple, it might be not sufficiently efficient. One might, for example, adopt some root isolation methods based on Descartes’s rule of signs; see [Mehlhorn and Sagraloff 11, Sagraloff 14] and the references therein.

### 4.4. Numerical Results

In this section, we will present some numerical results concerning dominant integer polynomials. These were obtained by realizing the algorithms described in Section 4.3 in PARI/GP. Here we would like to indicate that because of limited computational resources, we have not made computations for polynomials of higher degrees.

In order to realize the algorithms successfully in PARI/GP, we should guarantee that all the polynomials arising in the process have rational coefficients. So, we replace the quantity \( d_1(f) \) by

\[
2^{1-n(n-1)(n-2)/2}(n+1)^{-n(n-1)-1}H(f)^{-2n(n-1)-1}
\]

or

\[
2^{1-n(n-1)(n-2)/2}(n+1)^{-n(n-1)(n-2)-1}H(f)^{-2(n-1)(n-2)-1},
\]

according to whether we are considering the general case or the case of irreducible polynomials and \( n \geq 3 \). We also replace \( d_2(f) \) with

\[
3H(f)^{1-n}(n+1)^{-n-1}.
\]

To speed up the computations, we apply Algorithm 3 if \( f \) is reducible, and otherwise, we apply Algorithm 4.

Moreover, one can reduce the computations using the fact that if \( f(X) \in \mathbb{Z}[X] \) is dominant, then \(-f(X), f(-X)\), and \(-f(-X)\) are also dominant. For example, if \( a_0 \in \mathbb{Z} \) is fixed,

\[
H \quad | \quad 10 \quad 30 \quad 50 \quad 70 \quad 90 \quad 110 \quad 130
\]

\[
M_2(H) \quad | \quad 0.7664 \quad 0.8707 \quad 0.9009 \quad 0.9169 \quad 0.9271 \quad 0.9343 \quad 0.9397
\]

\[
P_2(H) \quad | \quad 0.5923 \quad 0.6148 \quad 0.6195 \quad 0.6216 \quad 0.6228 \quad 0.6236 \quad 0.6241
\]

\[
Q_2(H) \quad | \quad 0.4508 \quad 0.5454 \quad 0.5722 \quad 0.5849 \quad 0.5926 \quad 0.5979 \quad 0.6016
\]

**TABLE 1.** Values of \( M_2(H) \), \( P_2(H) \), \( Q_2(H) \) for various \( H \)

then we have

\[
\begin{align*}
\{ & a_0X^n + a_1X^{n-1} + \cdots + a_n \in S_n^{C}(H) \\
= & \{ -a_0X^n + a_1X^{n-1} + \cdots + a_n \in S_n^{C}(H) \}
\end{align*}
\]

and

\[
\begin{align*}
\{ & a_0X^n + a_1X^{n-1} + \cdots + a_n \in S_n^{C}(H) : a_1 > 0 \\
= & \{ -a_0X^n + a_1X^{n-1} + \cdots + a_n \in S_n^{C}(H) : a_1 < 0 \}
\end{align*}
\]

In order to demonstrate that Algorithms 3 and 4 and their realizations are correct, we first perform some computations concerning quadratic integer polynomials and then compare the numerical results with Theorems 1.1 and 1.3. One can also test quadratic integer polynomials by checking their discriminants and coefficients. Furthermore, numerical results about cubic integer polynomials also can reflect the correctness of Algorithms 3 and 4 and their realizations.

For integers \( n \geq 2 \) and \( H \geq 1 \), let \( M_n(H) \) be the proportion of dominant monic integer polynomials of degree \( n \) and height at most \( H \) among all the monic integer polynomials of degree \( n \) and height at most \( H \), that is,

\[
M_n(H) = \frac{D_n(H)}{(2H+1)^n}.
\]

By Theorem 1.1, we have

\[
\lim_{H \to \infty} M_n(H) = \lim_{H \to \infty} \frac{D_n(H)}{(2H)^n} = 1.
\]

Similarly, we define

\[
P_n(H) = \frac{D_n^{C}(H)}{2H(2H+1)^n}
\]

**TABLE 2.** Values of \( M_3(H), P_3(H), Q_3(H) \) for various \( H \)

\[
\begin{array}{c|cccccccc}
H & 10 & 20 & 30 & 40 & 50 & 60 & 70 \\
\hline
M_3(H) & 0.7852 & 0.8502 & 0.8779 & 0.8944 & 0.9056 & 0.9139 & 0.9203 \\
P_3(H) & 0.5881 & 0.5993 & 0.6026 & 0.6043 & 0.6053 & 0.6059 & 0.6063 \\
Q_3(H) & 0.4962 & 0.5453 & 0.5640 & 0.5743 & 0.5807 & 0.5850 & 0.5883
\end{array}
\]
According to our numerical results (especially Table 4), we also can make the following conjecture, which roughly says that at least half of integer polynomials are dominant.

**Conjecture 4.7.** For every integer \( n \geq 2 \), we have
\[
\limsup_{H \to \infty} P_n(H) > \frac{1}{2}.
\]

**ACKNOWLEDGMENTS**

The authors would like to thank Igor E. Shparlinski for introducing them into this topic, and also for his valuable comments on an early version of this paper. M. S. also wants to thank the Katana team of UNSW and Xin Zhang for assisting him in the computations.

**FUNDING**

The research of A. D. was supported by Research Council of Lithuania Grant MIP-068/2013/LSS-110000-740. The research of M. S. was supported by Australian Research Council Grant DP130100237.

**REFERENCES**


<table>
<thead>
<tr>
<th>( H )</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>21</th>
<th>22</th>
<th>31</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P_3(H) )</td>
<td>0.5956</td>
<td>0.5978</td>
<td>0.5998</td>
<td>0.6099</td>
<td>0.6106</td>
<td>0.6152</td>
<td>0.6155</td>
</tr>
<tr>
<td>( P_4(H) )</td>
<td>0.5904</td>
<td>0.5919</td>
<td>0.5935</td>
<td>0.5997</td>
<td>0.6002</td>
<td>0.6029</td>
<td>0.6031</td>
</tr>
<tr>
<td>( P_5(H) )</td>
<td>0.5363</td>
<td>0.5376</td>
<td>0.5388</td>
<td>0.5443</td>
<td>0.5447</td>
<td>0.5472</td>
<td>0.5474</td>
</tr>
</tbody>
</table>

**TABLE 3.** Values of \( P_n(H) \) for \( n = 2, 3, 4 \) and various \( H \)

\[
Q_n(H) = \frac{|\{f \in S_n(H) : f \text{ is irreducible}\}|}{2H(2H + 1)^n}.
\]

By Theorem 1.3, we know that
\[
\lim_{H \to \infty} P_2(H) = \lim_{H \to \infty} D_n^*(H)/(2H)^3 = \frac{41 + 6 \log 2}{72} \approx 0.6272.
\]

Theorem 1.4 implies the rate of growth of the quantity \( D_n^*(H) \):
\[
H^{n+1} \ll D_n^*(H) \ll H^{n+1}.
\]

Noticing further the distribution of reducible polynomials [Kuba 09, Theorem 4], we find that
\[
\lim_{H \to \infty} Q_n(H) = 1,
\]

which implies that
\[
\lim_{H \to \infty} Q_2(H) = \lim_{H \to \infty} D_n^*(H)/(2H)^3 = \frac{41 + 6 \log 2}{72} \approx 0.6272.
\]

Table 1 gives the values of \( M_3(H) \), \( P_2(H) \), \( Q_2(H) \) for various \( H \), and it is highly consistent with the above limits. The table also suggests that the above limits can almost be achieved for small \( H \), which also can be seen from Table 2. This means that to investigate statistical properties of dominant integer polynomials, we might not need to consider polynomials of large height.

Based on Table 3, we can make the following conjecture.

**Conjecture 4.6.** For every integer \( n \geq 2 \), \( P_n(H) \) is an increasing function with respect to \( H \).

This conjecture implies that the limit \( \lim_{H \to \infty} P_n(H) \) exists for \( n \geq 3 \).

<table>
<thead>
<tr>
<th>( H )</th>
<th>( P_4(H) )</th>
<th>( P_5(H) )</th>
<th>( P_6(H) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.5155</td>
<td>0.5107</td>
<td>0.4947</td>
</tr>
<tr>
<td>10</td>
<td>0.5345</td>
<td>0.5272</td>
<td>0.5111</td>
</tr>
</tbody>
</table>

**TABLE 4.** Values of \( P_n(H) \) for \( n = 4, 5, 6 \) and \( H = 5, 10 \)


